NTIA Special Publication 22-558


International Symposium on
Advanced Radio Technologies™

ISART 2020: Proceedings of the 18th International Symposium on Advanced Radio Technologies

# 5G Spectrum and a Zero Trust Network

August 10-13, 2020 • Fully virtual

NTIA Special Publication 22-558

Proceedings of the 18th
International Symposium on Advanced Radio Technologies™

# ISART 2020: 5G Spectrum and a Zero Trust Network

August 10–13, 2020 • Fully virtual


**U.S. DEPARTMENT OF COMMERCE**

February 2022

## ORGANIZING COMMITTEE

### General Chairs

Andrew Boedigheimer-Thiessen, NTIA/ITS

Melissa Midzor, NIST

### Vice Chair

Rebecca Dorch, NTIA/ITS

### Technical Advisory Committee

Dale Hatfield, University of Colorado, Boulder

Jean Pierre de Vries, University of Colorado Boulder

Keith Gremban, University of Colorado Boulder

### Conference Coordinators

Lilli Segre, NTIA/ITS

Amanda Hyman, NIST

Rachel Anderson, NTIA/ITS summer intern and CU Law Student

Gladys Arrisueno, NIST/PAO

### Proceedings Editors

Lilli Segre, NTIA/ITS

Rachel Anderson, NTIA/ITS summer intern and CU Law Student

## PREFACE

ISART™ 2020 was the 18th in a series of symposia hosted by the Institute for Telecommunication Sciences, ITS: the Nation's spectrum and communications lab, since 1998. Over the first decade of its life, the International Symposium on Advanced Radio Technologies™ evolved from a having an intensely technical focus to providing a neutral forum where business experts, technologists, scientists, and government regulators can share their points of view, debate issues, and engage in a holistic and expansive exploration of the future use of existing and emerging radio technologies.

ITS believes that promoting such expanded dialog and debate has greatly benefited the spectrum stakeholder community. Ideas first floated at ISART have found their way into breakthrough technologies and innovative regulation. ISART 2020, however, faced an unprecedented challenge: the Centers for Disease Control and Prevention (CDC) public health response to the COVID-19 pandemic led to cancellation of large in-person gatherings such as ISART. As a result, ISART 2020 took place as a fully virtual event.

ITS and the 2020 co-hosts, the University of Colorado and the National Institute of Standards and Technology, worked hard to ensure the virtual agenda included plenty of opportunity for the discussion and networking that had always been a hallmark of ISART, as well as the in-depth exploration of new and emerging technologies, the technical challenges they present, and the potential solutions that represent the future of radio technology. A benefit of the virtual format was that ISART 2020 drew 225 registrants, the most the symposium has ever had, and included many international participants as both speakers and registrants that might not have been able to attend an in-person event. Speakers and registrants included U.S. government, international, academic, and industry representatives involved in 5G developments in their countries, providing a broad range of perspectives on 5G spectrum security, standards, and deployments.

The text of these proceedings is taken from a transcription of the video record, which is available as a YouTube playlist on the NTIAgov channel. A best effort has been made to correct spellings of names and terms of art, but it is in no way an "edited" transcript. The figures referred to by various speakers are contained in the presentation files that have been posted in the Past Programs area of the ISART website.

Certain products, technologies, and corporations are mentioned in this report to describe aspects of the different current or potential future approaches to the topics covered in the symposium. The mention of such entities should not be construed as any endorsement, approval, recommendation, or prediction of success by the Department of Commerce or any of its agencies, nor as any inference that they are in any way superior to or more noteworthy than similar entities that were not mentioned.

## CONTENTS

## EXECUTIVE SUMMARY

The topic of the 2020 International Symposium on Advanced Radio Technologies™ (ISART 2020), "5G and a Zero Trust Network," was sparked by comments made by Dr. Lisa Porter, former Deputy Under Secretary of Defense for Research and Engineering, at the Silicon Flatirons "Saving Our Spectrum" conference in October of 2019. Dr. Porter said: "There is no such thing as a secure system—we can work to make things more secure, be more mindful of vulnerabilities, but ultimately, we must effectively use networks in which we have 'zero trust.'"

Future wireless systems (5G and beyond) will offer major economic benefit to countries and companies that can deploy those networks and services reliably, quickly, and securely. But spectrum—the foundation for much of 5G—presents unique security challenges, in addition to the many technical, economic, regulatory, and political challenges. Spectrum security historically focused on preventing jamming, spoofing, and interference. With 5G predicted to revolutionize spectrum use, it seemed time for governments, industry, and academia to examine what spectrum security means from a 5G spectrum perspective.

ISART 2020 aimed to identify challenges for spectrum to be available, reliable, assured, and secure in a no-trust environment; explore potential technical solutions; and identify research areas that facilitate securing spectrum for rapid adoption of assured 5G networks. ISART 2020 maintained the tradition of a "prequel" panel of tutorials to help set a baseline of common terminology and understanding for the discussions that followed. An unstructured conversation between key leaders from the three co-hosts—the National Telecommunications and Information Administration, National Institutes of Standards and Technology, and the University of Colorado was followed by an opening keynote address by Dr. Joseph B. Evans, Technical Director for 5G, Office of the Secretary of Defense.

To accommodate the exigencies of the fully virtual format, ISART 2020 had more, briefer sessions than in past years, spread over four days. The zero trust framing panel featured a panel of experts from government, industry, and academia diving deep into what zero trust means within the spectrum world and the known risks that exist today at the intersection of 5G NR (New Radio) and zero trust networks. Recognizing and naming the risks and vulnerabilities extant in the radio layer is crucial to identifying areas for research and developing solutions to better secure the spectrum relied upon for 5G services.

Four technically substantiative panels were designed to look at the zero trust theme from the design, deployment, monitoring and data collection, and operations perspectives, and the critical importance of feedback among all four components. These were interspersed with deep-dive technical presentations. The design panel focused on resiliency at the radio layer, and looked at design mechanisms and ways (such as RF filtering, new antenna technologies, closed loop systems, and others) that the 5G radio layer might be designed for resilient services. The deployment panel focused on implementing secure and resilient solutions. They explored deployment challenges, including how to implement secure and resilient technical solutions in a rip and replace world within a zero trust network environment.

The monitoring and data collection panel focused on the importance of feedback from monitoring and data to the design, deployment, and operations sides of 5G. They also explored options for effective and efficient spectrum monitoring and obtaining usable data. The operations panel focused on implementing resilient zero trust networks, and examined operations and implementing resiliency within a network's operations. Finally, a wrap-up panel brough together polymaths to help draw new insights and connections, identify potential new research areas, and add to the history of ISART triggering important out-of-the-box thinking, innovative ideas, and novel solutions.

# ISART 2020: PROCEEDINGS OF THE 18TH INTERNATIONAL SYMPOSIUM ON ADVANCED RADIO TECHNOLOGIES — 5G SPECTRUM AND A ZERO TRUST NETWORK

The topic of the 2020 International Symposium on Advanced Radio Technologies™ (ISART 2020), which took place fully virtually August 10-13, 2020, was "5G and a Zero Trust Network." The symposium aimed to identify challenges for spectrum to be available, reliable, assured, and secure in a no-trust environment; explore potential technical solutions; and identify research areas that facilitate securing spectrum for rapid adoption of assured 5G networks. Opening tutorials, a framing conversation, and an opening keynote address were followed by four technically substantiative panels were designed to look at the zero trust theme from the design, deployment, monitoring and data collection, and operations perspectives, and the critical importance of feedback among all four components. A wrap-up panel brough together polymaths to help draw new insights and connections, identify potential new research areas, and add to the history of ISART triggering important out-of-the-box thinking, innovative ideas, and novel solutions. The text of these proceedings is taken from a transcription of the video record. A best effort has been made to correct spellings of names and terms of art, but it is in no way an "edited" transcript.

Keywords: 5G, open radio access networks, radio layer, resiliency, security, spectrum, spectrum monitoring, standardization, supply chain verification, Wi-Fi, zero trust

## 1. DAY 1: AUGUST 10, 2020

### 1.1 Welcome to ISART

#### 1.1.1 Rebecca Dorch: Introductory Remarks

DORCH: Good morning from Colorado, and welcome to ISART 2020. My name is Rebecca Dorch. I serve as the senior spectrum policy analyst at the Institute for Telecommunication Sciences, ITS, the research laboratory for the National Telecommunications and Information Administration, NTIA. I've been involved with this NTIA program, the International Symposium on Advanced Radio Technologies, ISART, since I joined ITS in 2016.

As is a tradition with ISART, we open with a tutorial. The topic ISART is tackling this year, 5G spectrum and a Zero Trust network, involves a tremendous amount of cross-disciplinary understanding. So to help set a baseline of common understanding for those joining us from different disciplines, areas of expertise and levels of knowledge, we asked our tutorial panelists to do the impossible: explain what 5G is from an engineering, architecture, standards, spectrum

and international perspective in under two hours. And then, to record those presentations so that registrants could view them in advance.

On behalf of NTIA and our ISART cohost, the National Institute for Standards and Technology, and the University of Colorado at Boulder, I want to express my sincere appreciation for the outstanding presentations we are about to see. They each did a phenomenal job providing the baseline we sought. I will briefly introduce each of our five distinguished and accomplished speakers prior to showing their presentations, and additional information about all of the speakers is in the ISART program and the ISART app.

At the conclusion of the four presentations, we will all be here live and in-person, virtually of course, and please feel free to ask questions online during the presentations, and to vote for questions that you too would like to have answered during the Q&A portion of the tutorial.

Now remember, of course, that our panelists from government agencies are speaking based upon their knowledge and expertise, and not on behalf of their respective agencies.

So first up, we will learn about engineering and architecture underlying 5G from Professor Jeff Reed and Professor Nishith Tripathi. Professor Reed is a founder of Wireless at Virginia Tech and has a distinguished career teaching, advising, and directing programs and initiatives, and establishing companies related to wireless security and technology. Professor Nishith Tripathi is an adjunct faculty member at Virginia Tech and a research and development strategist at Samsung Research International — excuse me, Samsung Research America. He and Professor Reed co-authored a multimedia book on 5G, which explains the vast potential of 5G and key 5G concepts in about 55 hours. And I've asked them to cover it in about 20 minutes each. So we're grateful to both of them for sharing their knowledge with us. So now, without further ado, we will see the very first video; 5G Fundamentals and Deployment Considerations.

## 1.2 Tutorial Videos: Setting a Baseline

### 1.2.1 Nishith Tripathi and Jeff Reed: 5G Fundamentals and Engineering Considerations

REED: Hello and welcome to our tutorial, 5G Fundamentals and Deployment Considerations. My name is Professor Jeff Reed and my colleague, Professor Nishith Tripathi, will be presenting this tutorial. It's based upon our eBook, "5G Cellular Communications: Journey and Destination." And you can find it at the link below.

First, let me tell you a few things about myself. I'm the Willis G. Worcester Professor of Electrical and Computer Engineering at Virginia Tech. I have founded a number of different organizations, such as Wireless at Virginia Tech, the Ted and Karyn Hume Center for National Security and Technology, several companies, Cognitive Radio Technologies, Federated Wireless and PFP Cybersecurity. I've also co-authored several books, most of those books with Professor Tripathi. I'm also a winner of the International Achievement Award by the Wireless Innovation Forum.

TRIPATHI: Hello, I am Nishith. I work for Samsung and Virginia Tech. With Dr. Reed, I helped co-author a couple of books, including the first multimedia book on 5G and a textbook on cellular communications. I have contributed to organizations such as the FCC, GSMA, Scientific American and CTIA.

REED: Let's talk about the goals of this tutorial. First, we're going to provide examples of services that 5G was targeted to support. Next, we will look at the performance goals for 5G in terms of data rates and latency. And we'll look at the construction of the overall system architecture. There's some very important features of the architecture, including network slicing, a service based architecture and multi-edge computing. We'll summarize the key characteristics of New Radio air interface. This is the air link between the handset and the base station. And we're going to talk about two important features of the architecture, standalone and non-standalone modes for 5G. And this is important, particularly, as we discuss the spectrum aspects of 5G.

So our first topic, let's talk about 5G fundamentals, the services that are targeted by 5G and their respective performance goals. To give some context to 5G, let's take a look at the evolution of 5G. It seems like every 10 years we have a new wireless standard. These standards come from the 3GPP organization. 4G was defined in 2008 and 5G began its definition in 2018 with the Release 15. Phase 2 of 5G is Release 16. And that's expected to occur in July of 2020.

So what can 5G do for us? Oftentimes you'll see 5G represented by this triangle in which we have three pivotal services: enhanced mobile broadband, ultra-reliable and low latency communications and massive machine type communications. These services allow for various applications. For instance, with enhanced mobile broadband we see gigabytes in a second. And with ultra-reliable low latency, we see applications such as self-driving cars and massive machine type communications is there to support smart city. We'll be seeing the combination of these services supporting other applications, such as enhanced 3D videos, or augmented reality, or industrial automation. Combinations of properties of massive machine type communications and ultra-reliable low latency are useful for mission critical applications. And then finally, the combination of enhanced mobile broadband with massive machine type communications. That's very useful for smart home and building applications.

Let's take a look at the performance of 4G versus 5G. IMT-2020 specified the recommendations for 5G while IMT-Advanced specified the recommendations for 4G. And as you can see from this diagram, 5G provides much more performance than 4G systems in many critical areas. Peak data rates of up to 20 gigabits per second, user experience data rates of 10 times the previous ones, spectral efficiencies, three times user mobility, much faster speeds to support things such as high-speed trains, very low latency. And this, I think, is perhaps one of the most important of the properties of 5G, this little latency, because it opens up a variety of new applications. Connection densities, an incredible amount of 100,000 devices in a square kilometer. Energy efficiency of 10 times the previous, and finally the overall capacity 100 times greater with 5G versus 4G.

So how do we build 5G? Well, it's composed of a number of new components, such as New Radio, new network architectures, virtualization technologies, new devices, and new applications that are supported by 5G.

TRIPATHI: Let's start with the system architecture.

We should get ourselves familiar with some definitions. The user equipment, UE, communicates with the access network, which could be 5G access networks, so called next-generation radio access network or a non-3GPP access network. Then we have 5GC or 5G core network, also called next-generation core. NGC interfaces with the outside world, some data networks such as the internet. When we combine the UE, 5G access network, 5G core network, what do we get? A 5G system. A network function, NF, is some 3GPP defined or 3GPP adopted processing function in the network; for example, the base station gNB is a network function.

REED: Let's talk about the major features in the 5G network. First, we have in NG-RAN, the next-generation radio access network that allows LTE and 5G New Radio to work together. Then there's the cloud RAN aspects of 5G. The radio access network can reside in the cloud. 5G has a new core network, 5GC. Sometimes it goes by other names as well. That 5G core is a service-based architecture in which the components of the core network can reside in different locations within the cloud.

There's a number of different radio access network architectures, combination of 5G base stations, 4G base stations, 5G cores, 4G core. The multiple access edge computing network or MEC allows for applications to reside near the edge of the network. This is one of the neat features of 5G that allows for a very low latency.

And finally, perhaps one of the most significant aspects of 5G is that it was developed with network slicing in mind. So you can share a physical network, but the networks can be separated under different slices. Each one of those slices provision for different quality of service experience or different authentication or different security.

TRIPATHI: The next-generation radio access network is N-GRAN. So what do we have in the N-GRAN? So we have 5G base stations, gNBs, next-generation NodeB. So the gNB communicates with the user equipment through the New Radio or NR Air interface. Also, we can have some LTE base stations that have been upgraded to understand the 5G core network. So we call them NG, next-generation, eNB. So these eNBs talk to the UE using the LTE air interface. Now, the standard allows the gNB to be decomposed or desegregated into two components, central unit, CU, distributed unit, DU. So central unit allows the pooling of resources and distributed unit is closer to the cell side. So it has the RF equipment.

Now, what are the key benefits we can get from N-GRAN? Well, we can benefit from high performance 5G NR air interface. We get quite a bit of flexibility in deployment, and we get cost savings when we do such desegregation of the gNB.

5G core. So we have a variety of network functions in the 5GC. Here, we'll take a look at some of those. We have access and mobility management function that exchanges non-access stratum net signaling with user equipment, for example, messages related to authentication. We have session management function that allocates an IP address to the UE. UPF, User Plane Function, is a gateway to the outside world. So the packets from the outside world, a web server, will pass

through the internet routers, will arrive at the UPF, UPF to the gNB and gNB to the UE. The important aspect is that we have modularization. So we have more than a dozen different network functions. This architecture gives us benefits such as scalability, flexibility, OP supporting, networks licensing, a variety of services—some we may not even know today—and it gives us cost savings.

One of the key features of the 5G is SBA, service-based architecture. So each network function provides a set of services. For example, AMF says that, "Okay, I provide certain services." It will let the network repository function know about that. And session management function will also contact NRF. So now, NRF knows that we have this AMF alive, this SMF alive. So if somebody is looking for an AMF, they can talk to the NRF. These kind of network functions can store data in some storage functions, such as UDR and UDSF. So they can store information as well as retrieve information. For example, information about that subscriber.

What are the benefits we get from SBA? Well, it facilities implementation. There is increased resilience because you can tell the data separated from the computing resource. So if we lose the computing resources, we still have the data intact, we can start another processor as the AMF. Another aspect of 5G is MEC, multi-access edge computing or edge computing. So the idea is to bring the processing closer to where the users are. So if we look at traditional processing, then the user traffic will go from application server through the internet routers, coordinate to upgrade your network and to the UE. So this core network highly centralized.

Now, when we go to MEC processing, we bring the application close to the user. So the packet from the application server will arrive at the mobile edge host. And then we place some gateway like UPF we talked about, User Plane Function. And from that gateway to the radio network over the gNB and gNB to the UE. So we are not passing through a big comprehensive core network. So that will give us several benefits. For example, we will be able to reduce the latency because now the server is close to the user. There'll be less traffic in the backhaul and core networks, and we can make use of some things we couldn't do earlier, for example, location of NR services, because this application server is closer to the radio network. And it can talk to the core—the radio network and exchange some information.

Network slicing. Another very important feature in 5G. So the basic idea is to provide custom quality of service for a variety of services as well as customers. So we create different logical networks by using the same physical infrastructure. So for example, in the standard, we have enhanced mobile broadband slice. So that data rates with much more importance, so we provide high data rates to the user. Then we have ultra-reliable low latency communication slice. So here, latency is very, very important. Then we have yet another slice, massive machine type communication. Here, our coverage is very important. Maybe there is a vending machine in the basement of a building. So coverage is important. So basically, we have different slices to take care of different types of services. So we get several benefits, like custom quality of service and cost savings. So we use only those functions that are required. We can rapidly deploy services because we have done the customization.

REED: Now, let's take a look at the fundamentals of the New Radio air interface. Let's take a look at creating the New Radio air interface. First of all, 5G was developed with the ability to support a variety of spectrum, shared, licensed, or unlicensed spectrum. It has the capability of supporting massive Mimo, particularly at higher frequencies, to improve the throughput and range of the system. That's a very flexible framing structure. One thing you have to say about 5G is, it's the ultimate in flexibility. It means that actually a lot of flexibility in the formation of the OFDM signal as well, such as spacing of the subcarriers. There are advanced coding techniques that are incorporated in the air interface and the ability to connect to multiple radio access systems.

Massive MIMO is one of the key features of the 5G physical layer. You can have hundreds of antenna elements at the base station to enhance the overall performance. These antennas when combined properly provide for high gain and narrow beams. They can be used to support multiple users by pointing to different users in space to separate those users and increase the overall capacity of the network. Or you can use spatial multiplexing in order to improve the overall throughput rate by using different propagation paths to convey the information. So you get high throughput and high capacity using MIMO antennas.

TRIPATHI: 5G has quite a flexible frame structure. So we have a self-contained slot where the resource allocation, data transmission, and even positive or negative acknowledgement can all occur in the same slot. Now, the slot itself is of variable length, so we can have longer slot or a shorter one. And that will help us add up to the quality of service requirements. We not only have backward compatibility, but forward compatibility as well. So we have a traditional 1 millisecond sub-frame in LTE. In 5G, that sub-frame has one or more slots. So some slot could be used in future to define a new kind of air interface.

We have quite flexible OFDM numerologists. What is a numerology? It is basically a configuration with a certain subcarrier you're spacing. So for example, if you look at LTE, we have 15 kilohertz spacing for a typical channel. So between two subcarriers, rock solid fixed 15 kilohertz. But now in 5G, it could be 15 times 2, 30, could be 60, 120, and so on. So you have more options in 5G. So that allows us to tell a low complexity processor even though we might have large channel bandwidth. It helps us meet quality of service requirements and it facilitates diverse deployments. So we can have low band, high band and still have reasonable processing complexity.

Channel coding is quite advanced in 5G. So for example, traditionally in LTE when we want to convey resource allocation, for that signaling we use convolutional coding. But in 5G we use polar coding. So that will give us benefits like better error protection, more efficient to decode. When we talk about data transmission in LTE, we use a turbo code. But now, we have low density parity check code. So that has the benefits such as higher throughput, the complexity is relatively lower, and we save some power.

Okay. Time to talk about some 5D deployment considerations. So, Dr. Reed, let's start with network architectures.

REED: 5G has a number of candidate architectures combinations of base stations and core networks. The most popular eventually will be Option 2. We call it the standalone option with New Radio mixed with the next-generation core. Option 3 is what we're seeing deployed today, primarily, the non-standalone option in which we take New Radio and we use the old core network with it. But there are various options. Some of them with different types of base stations mixed with next-generation cores or with the old 4G core. And, of course, there's Option 1 [brief laughter], E-UTRA with an EPC.

The most common option will be the standalone architecture, Option 2, that consists of the New Radio connected with the next-generation core network. That next-generation core network will connect to the 5G base station, the gNodeB both with the user plane and the control plane. And, of course, the information will be relayed for the next generation core through the 5G base station, the gNodeB to the user equipment. It is this architecture that allows us to realize the full potential of 5G. However, it requires a new core network as well as a new radio network. Hence, this is more of the later deployments of 5G.

TRIPATHI: Option 3x, quite popular, also called the non-standalone NR with EPC or eNBC, EU to NR dual connectivity. So basically, our UE can help connectivity with both LTE eNB and 5G gNB. So one of the things that we can do with Option 3x is that data can come from core network to the 5G gNB. From 5G gNB some data can directly go to the UE over NR air interface, and some data can be forwarded to LTE base station and we use LTE air interface. So that is the kind of flexibility we have. So both the base stations LTE and 5G have signaling connection as well as traffic connection between them. LTE is the master node because the net signaling passes through the LTE base station.

So the benefits here include faster time to market, and you can still get pretty good performance from NR Air interface. And we have overall coverage, that is reasonably good due to widely deployed LTE.

Network functions virtualization is important. So we basically go away from physical network functions where we have individual boxes doing the functions. They are purpose-built proprietary hardware, proprietary software, and tightly coupled hardware-software.

But when we virtualize it, then we do the software implementation on generic hardware. So for example, we can put the AMF software on some generic processor. It becomes EMF. So we can use generic hardware, often called COTS, commercial off-the-shelf hardware. This gives us independence of software and hardware. And the software runs on the cloud infrastructure resources and we make use of compute, storage, and networking resources of the cloud infrastructure. We get the benefits like cost savings, scalability and agility.

Software-defined networking is also important for deployment. So the basic idea is that we try to rely more on software to connect different nodes or network functions. So traditionally, what happens is that we have an IP router that has the functions like routing, table creation, packet forwarding. And now, instead of doing all these functions in the same network element, what we do is we divide the control plane and data plane. So it is like divide and conquer. So control

plane would centralize the intelligence to determine optimal paths—effectively routing tables. In the data plane, very simple. It simply forwards the packet. So we separated the signaling from traffic. So now we can use very simple SDN switches or networking devices.

So what are the benefits? Well, since we have centralized intelligence, then we can make better decisions because we know what is happening in different parts of the network. We minimize the manual configurations of routers. And, of course, we reduce the cost because the tabling devices are really simple.

Spectrum, very important for 5G. So in Phase 1, we have Frequency Range 1 that is below 6 or 7 GHz. And we have defined FR2 to cover approximately 24 to 53 GHz. In general, millimeter wave means we should have 30 GHz or more frequency, right? But in practice, even if it's 24 GHz, we say it is a millimeter wave spectrum. So if you look at licensed spectrum, could be below 1 GHz. For example, operators have 600-MHz deployment. Then we have 1 to 6 GHz that is mid-band kind of spectrum. And then we have a millimeter spectrum of above 6 GHz, a variety of frequency bands. So there are several benefits and challenges. If you have lower frequencies, we get better coverage. But channels are narrower, so throughput is low. If you have millimeter spectrum, you have so much spectrum that your throughput is high. But because of larger pathloss, coverage is smaller.

REED: So let's summarize what we've learned. 5G supports enhanced mobile broadband, ultra-reliable low latency communications, and massive machine-to-machine communications. 5G has much better specs than 4G and, note particularly the latency is much lower than 4G. The 5G next-generation RAN includes its base station, gNodeBs, and also the core network is comprised of network functions, such as AMF, SMF and UPF. Network slicing is one of the neat features of 5G, allows custom logical networks to be created to support a variety of quality of service and customer requirements. The New Radio interface includes such features as massive MIMO, different OFDM numerologies, as well as different framing structures for the OFDM and operates over diverse spectrum, and it has advanced channel coding. The standalone New Radio architecture is the ultimate. It works with the 5G core. However, currently we're mostly deploying the non-standalone architecture in which the New Radio needs the old core network, the EPC, and it needs a LTE base station to act as the master node. 5G operates over a very large frequency range. While the lower frequencies are used to provide coverage, the higher frequencies, such [as] in the millimeter wave range provide a higher throughput. Mobile edge computing places the application closer to the users. And that's one of the key reasons why we're able to reduce the delays in 5G. The service-based architecture defines interfaces and facilitates a modularization and virtualization of the core network. SDN is very helpful in improving the routing and reducing cost, and, finally, network function virtualization enables software implementation of a network function using very generic commercial off-the-shelf hardware.

### 1.2.2 Jeffrey Cichonski: 5G Standardization Processes and Status

DORCH: Thank you, again, Professors Reed and Tripathi for that extremely informative presentation. Next up is Jeffrey Cichonski who will provide us with information about 5G standards. Mr. Cichonski is an information technology specialist at the National Institute of Standards and Technology working in the Applied Cybersecurity Division of the Information Technology Laboratory. He's an active member of the 3GPP's SA3 working group, which he'll explain in his presentation. And he has been engaged in the development of 5G security. So now, we will roll the second tutorial video, which is 5G standardization, 5G security enhancements and supporting infrastructure security considerations.

CICHONSKI: Good morning, everyone. My name is Jeff Cichonski. I'm a researcher in the Information Technology Lab at NIST. And this morning, I want to talk a bit about 5G standards, specifically 5G security enhancements that come with the 5G standards and some of the supporting infrastructure security considerations. I want to say thank you to organizers for including me on this morning's tutorial session.

So when we talk about 5G standards and standardization in general, it's important to understand that there's many different standards developing organizations, or SDOs. Many different SDOs are responsible for defining and specifying different pieces of the 5G system. Specific examples are the Internet Engineering Task Force. They define critical internet protocols, like TCP/IP TLS, things like IPsec. A lot of their protocols are used heavily in the 5G system. There's ETSI, the European Telecommunications Standards Institute. They do a lot of work in various different technology standards, but specifically virtualization is very important and different ICT standards as well. And then there's the Institute of Electrical and Electronics Engineers, the IEEE. They're really critical. They've defined the 802.11 specification or otherwise known as Wi-Fi, and they're doing other work related a 5G. But specifically, for 5G, the main group that's defining how the 5G system works is the 3rd Generation Partnership Program. They've defined 3G, they defined LTE or 4G, they defined the voice-over-LTE that LTE brought with it, and now they're working on defining 5G.

So we're going to dive in a bit about 3GPP because that's kind of the relevant standards developing organization for 5G and really the group where the meat of the 5G system is being defined. So 3GPP is really defined as a global initiative and they're responsible for mobile communication specifications. So they call themselves a global initiative because they're made up of partner organizations or regional SDOs. Examples of these SDOs are ETSI in Europe, ARIB in Japan, ATIS in North America, and the makeup of all these developing organizations, these standards bodies contribute to the 3rd Generation Partnership Program. So in order to contribute to 3GPP, you have to be a member of one of these regional SDOs.

So kind of the really short too-long-didn't-read: 3GPP wrote—is writing—the technical specifications for 5G. They're defining the interoperable interfaces, the protocols and the security features, which we're going to get into a bit more today.

And just a little timeline, 3G was defined by 3GPP in Release 3 back in 2000. 4G or LTE, defined by 3GPP in Release 8 back in 2009. The first version of 5G known as 5G non-standalone was released in 3GPP Release 15 in 2017. And a few months ago, we've finally frozen the 5G Phase 2 or Release 16 specification.

So to continue to talk about 3GPP and kind of the organizational structure, it's kind of important to understand they're made up of three overarching groups. Specifically, the radio access network, or otherwise known as RAN, the service and systems aspects, commonly referred to as the SA groups, and the core network and terminals or referred to as the CT groups. So each of these groups kind of has a plenary group that's oversees the sub-working groups, and they're responsible for setting the priorities, the timelines, and the coordination that's happening within each of these technical working groups. So specifically, for the past four years, I've been an active delegate in 3GPP's SA3 working group. This is the groups responsible for defining the security architecture.

When I started attending 3GPP meetings was when 5G security architecture was kind of a blank page and we were just beginning to lay out how the 5G security architecture was going to work and what security features would be included. A little more to continue on about 3GPP and kind of how the group works.

A little bit more specifics about the RAN. They're really responsible for defining all things radio interface. They define the really hard technical aspects of the radio access network. They're responsible for advancing the state of technology and how we're able to send more bits over the limited spectrum we have available. The SA groups are really responsible for the overall architecture and services capabilities of the system from requirements, to general architecture, to kind of specific security architectures. The CT groups are responsible for specifying terminal interfaces, kind of the logical and physical interfaces, the different terminal capabilities and the core network parts of the 3GPP system. If you look at CT, they're the folks that take the high-level specifications and boil them down into the bits and the bytes and actually standardize what each message in each bit needs to look like.

Another important component of 3GPP is they work using a three-stage methodology and that's applied within the working groups as follows. Kind of Stage 1, overall service description from the user standpoint, really high-level coming up with requirements and what are some of the services that the new release of 3GPP system should have included. Stage 2 is the overall description of the organization of the network functions to map service requirements and the network capabilities. So a lot of the architecture stuff is happening in Stage 2. In Stage 3, a lot of times is where a lot of the CT groups comes in and it's the definition of switching and signaling capabilities needed to support the services defined in Stage 1. So really CT is, or Stage 3 is really writing the hard zeros and ones that go into making the system operate.

So some insight into the 3GPP process. As I said, I participate in 3GPP SA3. Each working group is a little bit unique. So my perspective is kind of an SA3 perspective, but the general approach is you study new features, new capabilities, new things you want to include, and then potentially the next release. From a security perspective, this could be studying security issues or security

features that are seen as important. And then kind of the outcome of those studies are made into the technical specifications in the form of normative work, which is actually making it into an actual standard. So the TR really from an SA3 perspective, the technical report or TR presents the different solutions for a specific problem or capability. And a lot of these times we're leveraging protocols, and capabilities, and technologies from other standards organizations.

So as we mentioned ITF and IEEE, 3GPP relies heavily on technologies defined by other standards organizations to make the system work. There is definitely roles and responsibilities for each of these SDOs and they try to utilize each other's technologies as much as possible. It's really—the work really happens in an iterative pipeline, SA3 defines solutions based on SA1's requirements and SA2's architecture and also for mission critical services that are defined by SA6. There's a lot of tight timelines that require the groups to really work in parallel. And sometimes rework is required. If an architecture changes from SA2's perspective, that means the security solution for that architecture might also need to change or evolve. And then SA3's security solutions are really made real by CT1. So they write—they take the high-level security architecture and implement it in the overall system in kind of that really detailed bits and bytes level.

And then a really important notion for 3GPP is it's a consensus-based process. So the idea is all individual contributing companies bring contributions. Those contributions are discussed at a very technical level. They're argued, they're disagreed with, they're agreed with, they're promoted, and sometimes they're kind of not looked on with much seriousness if it's not a real technical solution. So it's really hard to kind of just barge into a 3GPP meeting and try to push your solution to a specific problem because it needs to be really informed at a technical level and it needs to make sense within the system. So these technical discussions—resorting to a vote is really rare. It's kind of seen as a failure of the process. And voting is, from an SA3 perspective really, it's what I've seen has been reserved for electing the leaders of the working group.

Just a quick splash of the current timeline, you can see Release 16 has been frozen in June 2020, Release 17 is underway in many of the groups and Release 18 is beginning or already has begun in some of those Stage 1 groups.

So we're going to shift a little bit and talk a little bit about network security and just the overall security capabilities that 3GPP and 5G bring to bear in this new generation of cellular network. So just the super basics. We have a device that's connected to a network of base stations. That network of base stations or radio access network is then connected to a packet core of some kind, and then that packet core provides connectivity out to different IP networks, whether that's the internet or some specific other IP network that needs to be connected on to. So super high-level.

Diving in to overlay some security around that. An important component of 3GPP and mobile network security is security is provided, but it's provided at a hop by hop level. It's not defined to be end-to-end, there's no security from the 3GPP system perspective from my device all the way to the internet. The security happens at each hop of the network. So from—in the radio

access network, I have access stratum security. There's NDSIP, or network domain security use, which is a 3GPP term for IPsec. And NDSIP is used between kind of the radio access network and the core network. And then there's also non-access stratum security provided from my device into the core network to protect a lot of the signaling traffic that happens. So just the key point is security is provided, it's provided at a hop by hop layer. This is just like a good representation of kind of where security exists. So we have user plane security, we have AS security or access stratum, protecting the control plane from the radio network. And we have non-access stratum security. That's protecting the signaling of the core network traffic. There's NDSIP or IPsec. And then there's TLS provided at multiple layers of the system.

So to overlay, you can see that user plane security and kind of the radio control plane security is terminating through the base station. And then we have security protecting core network signaling going from the UE into the 5G AMF or SEAF. And then we have NDSIP used to protect different portions of the network as well. TLS is becoming widely used within the different functions of the core network. And then over top of all of that from an actual application perspective, a lot of our applications, and our apps, and our organizations, we have user plane application layer security that is providing kind of an overall layer of security from end to end, taking advantage of all of the baked-in mobile network security and layering on top of that. So that was kind of a high-level of where security is in mobile networks. That's relevant for LTE. It's relevant now moving forward for 5G.

So as the standards are defined, there's definitely some known security issues with LTE. The technology has been around for 10 years. It's not perfect. Just some inherent ways in the way the network was designed allowed potential attackers to do some subscriber tracking based on information that was sent over the air in the clear. And LTE based on the key hierarchy, there was no possibility of user plane integrity protection. So no way to protect user plane traffic at that 3GPP system layer. There were definitely some roaming issues. I'm sure folks are familiar with SS7 and diameter threats taking advantage of weaknesses in some of those networks. And then kind of general false base station threats are definitely a real thing with any kind of RF technology.

So moving forward, 5G, the goal really was, from a standards perspective, was to build on the security provided in LTE. LTE had robust security protections. Just because there was some known issues, doesn't mean it wasn't a robust secure system. But the engineers that were defining the 5G security architecture in 3GPP understood some of those security weaknesses and really aimed to improve 5G security. So we'd like to say 5G security is really an evolution of LTE security. It's not a revolution. It's building upon some of the good stuff that was already there. So some of those specific features that we have, are user plane integrity—user plane traffic integrity protection. As I mentioned, that didn't exist in LTE. It's now possible, 5G. There's some subscriber privacy features to prevent some of those subscriber tracking threats. There's this notion of a security edge protection proxy. This network function provides standardized security at the roaming interface. There's a new authentication framework to allow different authentication network methods into the network. And there's this notion of splitting out the

radio unit in this centralized unit and distributed unit, so you can put the—you can do some security enhancements kind of from an architectural perspective.

We're going to dive into a bit of these in more detail, starting with the radio network security piece. So as I mentioned, finally we have integrity protection for the user plane. All the control plane integrity protection was available since the UMTS days. And then as I mentioned, we also have the split out of the gNodeB into a central and distributed unit. The CU or centralized unit performs the security critical functions, terminating, confidentiality, and integrity. And the air interface security terminates at the CU. So that allows you to locate that in a more trusted environment closer to the trusted core network. There's also some language in the specification to provide increased visibility to applications, to have a better understanding of what their security connection looks like.

This could be really promising moving forward as the 5G system evolves. It could allow applications to query the network to understand what their security posture of their current connection is. You can picture a banking app. If you open it, it could hit this—the app could hit this API, understand its security connection. If it didn't meet the requirements for whatever is laid out by that application, that application then could initiate some kind of over-the-top application layer of security to protect against that kind of weak base station connection.

So there's some privacy protections within 5G as well. Kind of the objectives of these were really to protect the permanent identifiers, cycle temporary identifiers in a more regularly scheduled way and more standards-based way, and kind of avoid this re-authentication that posed some threats in previous generations of 3GPP systems.

So the big, big thing that comes up when we talk about 5G and 5G security is the encryption of the subscriber identity. In 5G, that subscriber identity is known as the SUPI. In LTE, that subscriber identity was known as the IMSI, and I'm sure folks are familiar with IMSI catching threats. So now, the 5G system allows you to send this subscriber identity over the air in a concealed manner. So it's no longer sniffable or catchable by a rogue-based station, or just malicious actor.

There's some 5G authentication framework enhancements as well. So the credential storage, we have storage and secure hardware, whether that's a removable UICC SIM card, or if it's an embedded element in the device, like something commonly referred to as an eSIM. You can have the same authentication method to access both 3GPP and non-3GPP access. So picture connection to Wi-Fi using a 3GPP kind of security or credential. There's also native EAP support for 3GPP access. So this could allow in the future, things like IoT devices to take advantage of ETLS to prevent them from having to have that physical SIM card and allow more scalable deployment of authenticating IoT devices on the network.

So one critical thing I'd like to talk about that's really important from a 5G security perspective, is the 5G network is really comprised of many components, utilizing different modern IT technologies. 5G is moving from a legacy kind of network functions as a physical box, to a more softwarized cloud native approach to the system. The packet core network functions are really

being written in a cloud native way, using things like containers and container orchestrations to manage and operate how the system works. So taking advantage of modern technologies. The network functions are really one piece of that 5G system. The network functions are going to operate on top of kind of general-purpose IT components. Things like cloud computing technologies, cloud operating systems. They're going to utilize virtualization and container orchestration. So it's really important that you look kind of below the 3GPP network function perspective, and look at that supporting infrastructure and apply and understand what the cybersecurity best practices that can be used for those various different components of the technology stack. There's a lot of best practices that exist for these technologies. These technologies are widely used in the IT space. So it's really important that you're turning on and enabling the capabilities from a security perspective that exist in that supporting foundational infrastructure layer.

And just to build on that a little bit, there's many different technologies and protocols being used. I mentioned cloud-computing technologies but it's also important to note that internet security protocols are being widely used as well. And these protocols, as I mentioned, are specified by other standards developing organizations. Things like IPsec, TLS, JOSE, many other IT security protocols are being used in these systems. So it's important to understand what the best practices and the best ways to deploy those types of technology are.

So if you have any questions or comments, feel free to reach out to me, my email address here, jeffreycichonski@nist.gov. I really appreciate everyone's time today. And I hope you enjoy the rest of the conference.

### 1.2.3 Monisha Ghosh: 5G Spectrum From an FCC Perspective

DORCH: Thank you, Jeffrey Cichonski, for that very informative overview of the standards process. I'm actually looking forward to asking you some questions during the Q&A period.

We will now learn about spectrum for 5G within the United States, from Dr. Monisha Ghosh, the current chief technology officer of the Federal Communications Commission. Dr. Ghosh is also a research professor at the University of Chicago. And prior to joining the FCC in January of 2020, Dr. Ghosh served as the program director of the National Science Foundation. So our third tutorial video is 'Spectrum for next-generation wireless 5G and Wi-Fi'.

GHOSH: Good morning, everyone. First fall, I'd like to start off by thanking the organizers for providing me the opportunity to spend a few minutes discussing FCC's priorities in allocating spectrum for next-generation wireless, both 5G and Wi-Fi. My name is Monisha Ghosh. I'm in a temporary position at the FCC as the chief technology officer. I'm also a research professor at the University of Chicago, where I conduct experiments and research on 5G and wireless.

So the topics I'd like to cover in the next few minutes start off with the spectrum landscape for both licensed and unlicensed. As we're all aware, both of these parallel technology parts for wireless deployments have been progressing very rapidly over the last few years. Each of them

have designed and specified system designs that are increasingly higher rate, lower latency, providing better quality of service. And in order to do this efficiently, both systems need larger and larger spectrum allocations. So we'll talk a little bit about where we think the spectrum can come from. Then I will talk, move into a discussion of the licensed regime. Talk about spectrum allocations in high, mid, and low bands. All of these three spectral regions are very important in order for us to get a complete user experience. I will also talk about unlicensed. Even though one does not think about unlicensed spectrum as where licensed technologies like the Gs, you know, 1 through 4 and 5G will be deployed. It is increasingly clear, especially as borne out by the deployment of LTE LAA in 5 GHz that cellular technologies will take advantage of the unlicensed spectrum to deploy their systems in a way that they can aggregate channel capacity to give a better end-user experience.

So there are two actions in this area that I would like to talk about. One is a 6 GHz draft Report and Order, and the second is the repurposing of the 5.9-GHz spectrum. No talk on spectrum is complete without this picture, which many of you have probably seen in the past. This basically gives you the, you know, United States frequency allocations. While this is specific to the U.S., similar charts exist for every country in the world. And they're all similarly crowded. The bottom line is that spectrum is scarce. It is a finite resources. And as you can see from all the little colors and the bars on this chart, it is pretty much allocated, especially if you look at the regions of—the regions that have been used the most for consumer communications, which is somewhere up until 30 GHz. You see your familiar services there, your AM radio, FM radio and television, and then the cellular and Wi-Fi services. This is not a complete depiction of everything that has been allocated so far. But it just gives you a general sense of how little of the spectrum that's out there is actually used for the services that all of us have come to depend on. The other thing I should point out, that a large part of these spectrum bands are allocated for federal use. And those have usually been off limits for up until now. But increasingly sharing with federal services or finding ways to co-exist with them is becoming an important part of the spectrum strategy for not only the FCC, but other regulatory bodies around the world.

Now, as you can see from this picture, as you're going from the chart from top to bottom, the scale changes. It's not a linear scale. And so the same area covered by a circle at the bottom of the chart actually encompasses a larger swathe of spectrum. So the 60 GHz Wi-Fi circle is actually 14 GHz of spectrum. And that little cycle there at 60 GHz, which is more than all of the allocated spectrum, saying below 3 GHz, obviously, right? So basically, what this tells you is that if you're looking for more bandwidth, more spectrum availability, you need to go higher in the spectrum band, but at the same time as you go higher, you'll face the problems that physics poses in terms of propagation, the signals don't travel very far. And so you're tasked to come with accompanying change in the way you design your cellular systems or Wi-Fi systems to operate at these higher frequencies.

I'd like to now talk about the FCC 5G FAST plan. So this is FAST stands for Facilitate America's Superiority in 5G Technology. You can either Google their FCC 5G FAST plan, or if you go to the website there. What you will see outlined there is a very comprehensive strategy of how the FCC plans to allocate spectrum in high, mid, and low bands, as well as in the unlicensed band in the

service of future 5G and advanced wireless services. In the high band, which I denote as greater than 24 GHz, this is where one expects the 5G millimeter wave variant to be deployed. Again, because this is much higher in frequency, propagation losses, propagation inherently limits the distance that you can cover with a single base station. This lends itself to small cell deployments. However, the bandwidths are much, much higher. And so you have the potential of actually getting gigabits per second throughput in these frequency ranges.

In fact, as part of the research that I do at the University of Chicago with my students, we've been taking a lot of measurements on the—on Verizon's millimeter wave deployment in Chicago, 5G deployment. And we have measured download speeds of 1 to 1 and 1/2 gigabits per second depending on where we are located.

However, purely focusing on the high band is not an effective way of rolling out 5G for everybody. The mid-band plays a crucial role in getting 5G out to everyone. It is a nice balance between coverage and throughput. The frequencies led themselves to wider deployments and there is enough bandwidth there to get reasonable throughput as well. So this is very, very important for any wide-scale mobile wireless system to have mid-band allocations.

I will not talk or spend a lot of time talking about low band, which is less than 1 GHz. This frequency has been mostly allocated for broadcast television in the past. But over time, more of it has transitioned over to mobile wireless especially with the transition to digital TV. The spectrum was repacked, leading to some auctions of some channels and other channels which are being repurposed for 5G applications. And do keep in mind that the bandwidths that are available at these low bands are pretty narrow. So you're not going to get the high throughput that one expects when one talks about 5G. But on the flipside, you will get very wide area coverage. And this would be great for the next generation of IoT applications, for example, where you need, you know, for example, city scale IoT, where you need large ranges, but your data rates are not that high.

I will also talk about the actions that FCC has taken in unlicensed to enable not only expansion of Wi-Fi, which is the first technology one thinks about when you're thinking about the unlicensed spectrum, but also as we've increasingly seen in 5 GHz, unlicensed spectrum is also a great place for cellular systems to deploy as long as they meet the rules of unlicensed spectrum. We've seen deployments in Chicago, for example, where cellular carriers are aggregating up to three channels in the unlicensed band to enhance the throughput that they deliver to their customers. And we fully expect that the new unlicensed spectrum will be used by 5G and are unlicensed in the same way as well. Oftentimes in industry you see these two technologies set up in a competitive manner. While it is true that they occupy different spaces, we also feel that we need to allocate sufficient spectrum to both, because advances in one enable advances in the other. If you're at your home with a very high-speed Wi-Fi connection, and you're used to that kind of a user experience, you expect the same level of service when you step outside the home, where, of course, Wi-Fi is not going to provide you that experience, but cellular will. And so we view both these systems as, you know, pulling each other up and the consumer benefits. And allocating enough spectrum for both is very, very important part of the FCC strategy.

So let us take a little bit of a deep dive into what FCC has done on the high band. A number of auctions have been completed already. You know, in January, 2019, 800 MHz was allocated in 28 GHz, 750 MHz in May of 2019 in 24 GHz, and just recently earlier this year, 3.4 GHz of spectrum was allocated in the upper 37, 39 and 47 GHz. Now, these, the earliest spectrum allocated was just last year and we're already seeing 5G rollouts happen in the spectrum. So the industry is just waiting for spectrum to get allocated for them to start rolling out systems. So the total of 4.95 almost 5 GHz of spectrum has been allocated for millimeter wave-based 5G.

I believe the U.S. now leads the world in high band licensed allocations. And this has resulted in an extremely aggressive rollout of millimeter wave 5G across the U.S. And as I mentioned before, this is the band where you're going to get the gigabits speeds that we have come to expect of 5G.

On the mid-band, there's a lot actions that have been done and more that have been planned. The 2.5 GHz is actually an interesting band. It's the single largest continuous block of spectrum below 3 GHz. It's going to get allocated to educational broadcast service and the broadband radio service. The FCC has an NPRM out to re-evaluate this spectrum and to say, "What are the current needs of these two services, EBS and BRS?" And then any spectrum that is leftover, there's an anticipated auction that will begin in early next year. Again, this is the mid-band spectrum, which has the nice characteristics of both propagation and sufficient bandwidth.

The C-band Report and Order, which went out earlier this year, will result in a public auction of 280 MHz of spectrum in the 3.7 GHz band. So this is 3.7 to 3.98 GHz. This is slated to start in December, 2020. As—if you remember the chart that I showed earlier on, where you see how crowded the spectrum is, most of the time going forward, if we are trying to free up spectrum in the mid-band in particular for 5G, we have to look at what's already in there. Because there really isn't any spectrum that's sitting there either. So in this band in particular, you have satellite incumbents which have to be moved out of these 280 MHz of spectrum. They will continue to operate in the upper 200 MHz, so 4 to 4.2. There will be a 20 MHz of guard band between the 5G mobile terrestrial and satellite. But that takes time. There is also a process by which the satellite incumbents are paid to move out of the spectrum. And the money for that comes from the proceeds that the auction will raise. So licensing spectrum in the mid-band is usually a longer process than say the high band, where there was a lot more available spectrum. And we're going to see this repeat in other bands that we pick up for 5G as well.

CBRS has been in the works for many years now. This is the 3.55 to 3.65 GHz band where Navy radars operate. The auctions were supposed to have started in June. They slipped by about a month due to COVID, but they have begun. This auction will be for the Priority Access Licenses. So CBRS is a band which is not only being shared by Navy radars through SAS or AFC service, but it's also going to have three different priority classes of service. And so it's the incumbents, then the priority access license, and then the general access category. So the licenses being auctioned today are for the priority access licenses. This will probably be in the U.S. the first mid-band 5G rollout that happens. And the industry is very excited about it. There are a lot of different use cases being planned for this band. For example, private 5G networks is one thing that you can see rolling out here. And also, just early 5G mid-band deployments.

We are also investigating potential sharing in the band right below the 3.55. So this is the 3.45 to 3.55 GHz band, which also has a lot of federal use right now there. NTIA came up with a report on spectrum sharing earlier this year. And we are in the process of refining some of the assumptions and parameters to really understand under what conditions the spectrum can be shared.

So there are a lot of actions in mid-band, and we hope to be able to get a fair amount of spectrum into the hands of 5G providers fairly soon. Low band, as I said, I'm not really going to talk a lot about. There is a 600 MHz band. There's about 70 MHz of licensed spectrum that has been allocated there and a 900 MHz. There is some discussion about repurposing part of the band to enable broadband using LTE for beginning for start and then possibly 5G into the future.

Finally, let me talk about unlicensed. We recently concluded the biggest unlicensed allocation for—that is, I think, this is the biggest that has ever been done, is 1.2 GHz of spectrum has been allocated for unlicensed use in the 6 GHz band, which is basically 5.925 to 7.125. Now unlike the 5 GHz, or at least most of the 5 GHz, this is not a clean band. As, again, I mentioned before, there's very little clean spectrum left. It will be shared with existing incumbents. So there are 6 GHz fixed links and broadcast auxiliary services there, which provide services like wireless news gathering. However, FCC has been very careful in crafting rules that will permit low power indoor Wi-Fi devices or unlicensed devices without any automatic frequency control to coexist with these bands. We have we have created power limits that we feel will not create harmful interference in most cases to these links. There are also going to be higher power outdoor links that will be allowed that will use an automatic frequency control system to coexist with the existing links. We really, even though a lot of the rules were crafted in keeping Wi-Fi usage in mind, we fully expect that 5G NR-U will make full use of this band as well. And given that there's a lot more bandwidth here, we feel that the coexistence problem will not be as severe in this band as it has been in the 5 GHz band. Simply because there will always be more channels that these systems can choose to operate on without interfering with each other.

We expect systems that get deployed in this band to use higher bandwidths. So Wi-Fi, for example, has been moving to higher and higher bandwidth. They are at 160 MHz now and they're moving towards 320. We fully expect that the higher bandwidth systems will find a home here and that the band will not get cluttered by a lot of legacy coexistence issues with low bandwidth devices, which can still continue to operate in the 5 GHz unlicensed. We're also, right now, looking into repurposing the lower 45 MHz of the DSRC band, which had been allocated for Intelligent Transportation Systems. This band has been very underutilized for the last two decades since it was allocated. And given the growing needs of Wi-Fi, the FCC has a plan to repurpose the lower 45 MHz of this band for unlicensed and keep the upper 34 for ITS services. The lower 45, when combined with existing spectrum and the 5 GHz, will create wide band—at least one wide band channel that can be used by both Wi-Fi, as well as for LTE, LAA or 5G NR-U all new kind of services.

At the same time, we've allocated 21.2 GHz and 95 GHz band for unlicensed use. Above 95 GHz is where there's a lot more availability of spectrum. There is a lot of passive uses of spectrum

there which have to be managed and we've made very easy experimental license availability in these bands. And we really hope the academic community, in particular, will utilize these resources to push the boundaries of where we can go for the next generation of wireless systems.

I'll end with some closing thoughts about what a sustainable spectrum strategy is. I don't expect you to read everything that's on this slide, but I just want to point out how often the word sharing comes up in this presidential memorandum on developing a sustainable spectrum strategy that was released in 2018. So as we go forward, we expect to see more and more spectrum being allocated either on an unlicensed or a shared license, or some kind of shared basis, because the bottom line is very little clean spectrum available for all the services we are interested in. Thank you for listening. And I hope to have an engaging conversation after, at the end of this tutorial session. Thank you.

### 1.2.4 Mohamed El-Moghazi: ITU views on 5G

DORCH: Thank you very much, Dr. Ghosh for that excellent presentation. Finally, Dr. Mohamed El-Moghazi will walk us through 5G from the international perspective, including explaining the relationship between 5G and IMT-2020.

Dr. El-Moghazi is the spectrum management research and studies director at the National Telecommunications Regulatory Authority, NTRA, of Egypt. He's currently coordinating several items for the WRC-23 in Egypt. He founded the Global Telecom Policy Research Network, which is an initiative for scholars and telecom policy and authored numerous articles. We are thankful that Dr. El-Moghazi is able to join us virtually. So here we have our fourth and final tutorial video entitled "IMT-2020 Spectrum Identification and Technology Standardization."

El-MOGHAZI: Hi, everyone. This is Mohammed El-Moghazi. I'm working for the Telecom Regulatory Authority of Egypt as executive director of National Spectrum Affairs. I'm also responsible of several related issues to 5G at the ITU on behalf of Egypt and the Arab region. First of all, I'm very glad to have this opportunity to participate in this conference. And I'm very grateful to the conference management, especially my mentors, Professor Dale Hatfield and Dr. Pierre de Vries.

Secondly, you may wonder if this conference is about 5G, why is this specific presentation address what is called IMT-2020? In fact, within the ITU, the International Telecommunication Union, the international community addresses many issues related to 5G and sometimes lead it. But in order not to have a conflict with commercial deployment and the names of the different cellular mobile generations, 3.5G, 4.75G, it was decided, at least within the radio sector of the ITU, not to use the abbreviation of 2G, 3G, 4G and 5G. And instead, we call it all IMT, International Mobile Telecommunications. And the different generation names are not recognized within the ITU.

Also, the ITU is different as an international forum from organizations such as 3GPP, ETSI, and the IEEE, as the process is inclusive for all countries with equal vote. That enables several people from the developing countries, including me, to have a big say when it comes to the technology and frequencies associated with it, which are the topics that we will discuss today.

So IMT. To give you an idea of how IMT was developed, let's read this quote. "The ITU is currently working on one of its most ambitious projects ever, system standards for third generation mobile telecommunications coined the IMT-2020. It will make it possible to communicate anywhere, anytime." That quote was recorded in 1998, and it gives you an idea what the ITU wanted to make at that time. Remember, we're talking about the 3G era. And in fact, the IMT idea was the ITU reaction towards the lack of interoperability between second generation wireless standards. In order also to get more involved with—in the standardization process of mobile system.

I believe many of you remember the rivals between 2G different technologies and the discussion on whether CDMA or GSM is better. The ITU is involved in two main process. One of them is related to the technology standardization and the other one is related to the frequency use associated with these standards or technology. The first process has resulted in different generations of IMT, which are also related to the generations of cellular mobile technology, namely IMT-2000, IMT-Advanced and IMT-2020. All these generations are treated equally in terms of spectrum identification and are called IMT.

The second process is called the IMT spectrum identification. And firstly, we should understand that the ITU mainly allocates the radio spectrum to the different radio communication services broadcasting, mobile. and fixed. But in the case of cellular mobile, the ITUR radio regulations perform what is called the identification, which is a second process to allocating the band for mobile services. Identification indicates some sort of inclination or tendency towards utilizing these identified bands for IMT. Anyway, it's worth mentioning that it's not usually within the ITU to have identifications to specific technology. But certainly, there is a global desire in having more certainty in developing IMT system.

So the first step in the ITU standardization activity of mobile technologies was in the '80s, when the concept of future public land mobile telecommunication system was discussed in the ITU due to the support of European countries that were seeking a successor to GSM. And then the idea of IMT-2000 emerged to reflect that the mobile service would use a 2 GHz spectrum band and be available in the year of 2000. And in the year 2000, five systems were recognized by the ITU after extensive evaluation to be part of the IMT-2000 family. In 2007, a big milestone when the IEEE, WiMAX technology was accepted as the sixth IMT-2000 system. 2008, ITU started the process for what is called the IMT-Advanced, at the time of the 4G era. Four years later, two main technologies were recognized as part of the IMT-Advanced family, namely LTE-Advanced and WirelessMAN-Advanced. Commercially, these systems were called the LTE and WiMAX. 2016, the ITU started the process for what is called the IMT-2020, which is related to the 5G technologies. The process has started in 2016 and has not finalized yet.

In other words, until today, there is no recognized technologies by the ITU as IMT-2020, or what is called commercially as 5G.

So let's start digging to understand where it all starts for IMT-2020. The beginning was to have a vision of what should IMT-2020 system performance looks like? And this famous diagram that you may have seen it in several other presentations, it was originated by the ITU as a vision on how the IMT-2020 should succeed IMT-Advanced, and in which aspects.

Clearly, one main element was big data rate. And the minimum requirements were set to be 20 gigabit per second for download—downlink big data rate. Another important element that was set is download user experience data in practice, in contrast to the theoretical big data rates. And it was agreed that such value should be around 100 megabit per second. The third important elements that reflect how IMT-2020 would be different than IMT-Advanced are the latency, which was agreed to be less than 1 millisecond. And let's not forget about the connection density also. These two elements shows—show the usage scenario 5G that required very low latency and are implemented by massive number of devices.

In this slide, I'm trying to elaborate to you what has been the timeline for IMT-2020 standardization process and how it works. I'm so sorry for the small details, but anyway, the standardization process accommodates some main milestone. Firstly, the ITU issued an invitation for technology developers around the world to propose technology standards that meet the IMT-2020 performance characteristics previously mentioned in the last slide. The ITU issued also an invitation for external independent group to evaluate the applicant's technologies. Again, it's the criteria decided by the ITU members. Following that, these evaluation groups were formed and evaluated the applied technologies. And the deadline for submitting the evaluation was last February of 2020.

Last June, it was a very important meeting of the working party 5G of the ITU, which decided on the main IMT-2020 systems that meet the criteria as decided by the evaluation group. And in next November, the ITU will issue the formal recommendation accommodating the characteristics of these approved systems.

So to this end, what were the proponents to be part of the IMT-2020 system, or as commercially mentioned, 5G? I know there is usually a perception that 5G is the 3GPP New Radio, NR. But this is not quite accurate. In particular, there were seven proponents to the ITU. The first is the 3GPP SRIT or Set of Radio Interface Technologies, which accommodates the New Radio, in addition to the E-UTRA, Evolved Universal Terrestrial Radio Access. The second is the 3GPP Radio Interface Technology or the New Radio. And the third is—or was—a proposal from South Korea, which is identically identical from the technical point of view to the 3GPP RIT. Fourth proposal is from China, which is also technically identical to part of the 3GPP RIT and have another identical part, which is another RIT, to the 3GPP SRIT. The fifth proposal is Telecommunication Standard Development Society of India proposal, which utilize the 3GPP, 5G New Radio, but also adds functional capability to support the low mobility large cell in rural areas. And it's perceived by its proponent as quite appealing to the developing countries. Sixth proposal is by DECT Forum and

ETSI, and it's called DECT-2020 New Radio. And the last proposal is Nufront, which is a proposal from a Chinese company.

So as I mentioned, there was an important milestone in last June of 2020, where only three main technologies, or five main proponents, if you include the proposal from China and South Korea, that proceeded to the final step, or step number 8, which is a development of radio interface recommendation. However, there was a big debate on the way forward for the other two proponent, Nufront, and the DECT Forum and ETSI. And it was decided that these two technologies need additional evaluation.

So as I mentioned before, the IMT standardization process has been associated with identifying the radio spectrum bands to be used by these IMT standards. The first step was in 1992, when the World Administrative Radio Conference of 1992 identified the 2 GHz band despite opposition from countries, such as the U.S. Eight years after that, the World Radio Communication Conference of 2000 agreed to identify the bands 900 meg, 800—1800 and 2.5 GHz for IMT. That decision was a big boost for the harmonization for IMT, considering that the band 900 was used mainly for 2G. That WRC of 2007 was quite important in identifying additional bands needed for the growth of the mobile industry. And then the WRC of 2012 achieved global harmonization between the three ITU-R regions in the UHF bands. And surprisingly, that was in response to request from the developing countries in Africa and the Middle East. WRC 15 identified more frequencies for IMT. And I think one of the most important band is the UHF from 470 to 694 in the United States and a few other countries. And finally, the WRC of 2019 that was held last November in Egypt, identified 17.25 GHz of spectrum, compared to 1.9 GHz before the conference, of which 14.75 GHz are harmonized worldwide. That was a big achievement for the IMT community.

So an important question, do countries usually deploy 4G and 5G systems in bands identified for IMT? The short answer would be, no. As you can see in the displayed table, there are four cases that I can count where there were IMT deployments without IMT identification. So the L band or part of it, for instance, is not identified in CEPT countries for IMT, but still used for IMT. Similarly, a part from the C-band is not identified for IMT and not even—and doesn't have even a primary mobile allocation, but still used for IMT in Europe and CEPT countries, and in some of the Arab countries. The the 26 GHz, although it was identified at WRC-19, several countries decided to utilize it for IMT, without waiting for the conference and before the conference. And finally, the famous 28 GHz is not identified for IMT by the ITU, yet it's still used for IMT in several countries, big countries including the U.S. and Japan.

So a second question, why countries seek IMT identification to deploy 5G? Well, being recognized by the ITU provides greater certainty against interference and is based on international sharing studies. And certainly, it also ensured protection for existing service. But on the other hand, why other countries deploy 5G without IMT, such as the case of 28 GHz? Well, this is related to having less conditions, less deployment conditions, and faster deployment. Of course, this is conditioned by having support from the industry.

So I look forward for the World Radio Communication conference of 2023. And what is at stake for the 5G or IMT community? I think we have four main agenda items that are critical and we need to understand and get a view on them. The first is Agenda Item 1.2, which considers additional identification for IMT including several bands in the C-band in Region 2 where the U.S. lies. And also, some of these bands are in the 6 GHz band, where the FCC has recently opened more spectrum for Wi-Fi. The second agenda item is 1.4, where the concept is of HAPS, High Altitude Platform Stations is used as IMT base station in what is called HIBS. And in such case, the HAPS will act as an extension to the traditional IMT coverage. The third agenda item is 1.5, where the future of terrorists who are broadcasting in the UHF band, mainly 470 to 694, will be discussed. And it will be also discussed whether the band could be utilized for IMT. Fourth agenda item is 9.1.C, which studies the use of IMT systems for fixed wireless broadband and the frequency bands allocated to the fixed service rather than traditionally perceive the IMT as only used form of wired service.

Finally, if you need more details on what's happening with regard to the IMT-2020 standardization, please check the first link. It has a lot of information and it has most of the reference for the content in this presentation. Not all the document on the website are available publicly, but certainly there is much more information that was presented in this presentation. Also, if you are interested in learning more about the coming World Radio Communication Conference of 2023 and the potential frequencies for 5G, please check the second link for the conference preparatory meeting or CPM of 2023. Thanks a lot for your attention and please feel free to email me if you need any further clarification. Thank you all.

### 1.2.5 Tutorial Session: Q&A

DORCH: Thank you, Dr. El-Moghazi, for that insightful presentation. I'd like to now welcome all of our distinguished speakers into the live session now to begin the Q&A portion. And first, let me—we're getting video from everybody? Thank you. First, let me thank you all again for your presentation. I'd like to start with a few questions from me to each of you before we go to the audience questions. And for the audience, please look at the questions that are already in the Q&A section on the right of the screen and vote if you too would like to hear an answer to a particular question. And continue to add questions through the Q&A section if you'd like. I'll endeavor to pull questions based on those with the highest interest.

So let me—I could start with a question here. So Dr. Ghosh provided an excellent overview of spectrum for 5G band in the U.S., and Professor Reed and Professor Tripathi both—let me ask you, did I understand correctly that the basic architecture for the 5G New Radio is flexible enough to work for any spectrum brand where 5G might be deployed whether it's low band, mid-band, high band, including the ultra-high band millimeter wave? And I think Dr. El-Moghazi addressed this in one of his slides about IMT-2020, but just want to make sure that I understood that the same thing applies there for how IMT-2020 is currently conceived.

TRIPATHI: Okay. So you'll—yes. Yeah. So you might have seen acrobats in a circus, they bend their bodies in a way we cannot imagine. That is flexibility of 5G. So yes, we do support low

band, mid-band, high band, even commercial deployments have already begun. So T-Mobile, just recently, couple of days ago, said that now they have a nationwide 600 MHz 5G network. Verizon and AT&T have already deployed in the U.S. at 28 GHz and 39 GHz, which are millimeter wave spectrum. So yes, we already have real world deployments. Thank you.

EL-MOGHAZI: Yes, Rebecca, if you can add, so first of all, thank you so much for those who are attending here. Rebecca has been doing a big, big job during the last week. So thank you so much for this. And thank you so much for the very good question that made me think about what the ITU has been doing. So yes, although the IMT-2020 are just systems of approved systems for 5G including the 3GPP 5G New Radio, but it does provide some sort of flexibility in terms that the spectrum identified for IMT whether it's in low band, mid-band or high band could be used for IMT systems. This include any 5G, 4G, or 3G. So flexibility is provided also by the ITU. Thank you.

DORCH: Great. Thank you. My next question is directed this time to Dr. Ghosh. You mentioned that there's an expectation that wider bandwidths will be used for 5G. And you also talked about how with the higher spectrum bands, there's more capacity and faster throughput. So can you kind of help pull that thread together for us to briefly explain why wider bandwidths are also needed? What is it about 5G that requires so much spectrum?

GHOSH: Thanks, Rebecca. So as Nishith had mentioned, right, so you have 5G in all flavors and depending on the bandwidth that you deploy it in, you will get an attendant data rate. So the wider bandwidths and like 100 MHz, for example, are what you need if you really want to get close to gigabits per second throughput. We have made, the academic community and industry together, have made great strides in increasing spectrum efficiency, which refers to how many bits per second you can push through a fixed amount of bandwidth. And a lot of the advances you've seen in 4G in particular have come from that.

However, having more bandwidth, basically, your throughput scales linearly, whereas everything else, that linear scaling is much more difficult to achieve. So now, if you think that you need the wider bandwidths and you look at where the wider bandwidths are easier to get, we are trying to make at least 100 MHz of contiguous bandwidth available in mid-band as well. But that is difficult. But that is progressing. But meanwhile, those kinds of bandwidths are much more easily available up in the millimeter wave. And so as we go higher up in frequency, you're going to get the wider bandwidths, you're going to get a higher data rates. Lower down in the mid-band, you're going to see systems deployed that do this tradeoff between say massive MIMO kind of architectures that are increasing the spectrum efficiency combined with—I don't think we're going to see too many 5G systems deployed in say 5 MHz bandwidths. But you do have 4G deployed in 5 MHz bandwidths today. So we are definitely looking at 20 MHz and up bands for 5G bandwidths.

DORCH: Thank you. And next question I'll throw one over to Jeff Cichonski. You made for me in your presentation what I thought was an excellent point about security is on a hop-by-hop level. I mean, not across the entire end-to-end system from the device to the internet. This may be a naive question, but does that security apply both ways from both the user equipment to the

internet and then back also from the internet to the UE in that hop-by-hop fashion? Jeff, you have to unmute. Jeff, I can't hear you.

TRIPATHI: Yeah. As he looks—until he gets back.

DORCH: Well. Okay. Well, I was going to say, I could move on to another question while Jeff troubleshoots.

DORCH: You're going to try again, Jeff? I still can't hear you. Oh, no. We thought we troubleshot everything here. All right. Nishith, do you want to give it a quick go and then Jeff.

TRIPATHI: Yeah. Yes. So the short answer is, yes. That hop to hop applies both directions, internet to the UE, and UE to the internet. Absolutely correct. Thank you.

DORCH: All right. And then one more question before I go to the audience questions, because we've got several of those that have popped up with a lot of votes on them, which is excellent. So, Dr. El-Moghazi, does the ITU—well, because we were just going to talk about security there, does the ITU take a view on the security and the reliability issues that this conference is about?

EL-MOGHAZI: Thank you so much, Rebecca. So for the next question, I need a special disclaimer that this is absolutely my personal view on this. It doesn't represent NTRA or ITU, or any of that. So I looked at the conference name spectrum and Zero Trust. And then I looked at the official ITU documents to find what it's all about the security for the IMT-2020. And I found in one of the main reports on IMT-2020, that, I don't know, big, big phrase on security. So it states in the ITU-R recommendation M-2083 on the IMT vision that, "Future IMT systems need to provide robust and secure solutions to counter the threats to security and privacy brought by New Radio technologies." And that's it. Silent. So I guess—and again, this is very personal perspective. We do a lot of things for the future in terms of spectrum, in terms of network architecture, but are we really ready for the future? Unfortunately, at least within the ITU-R it's—I haven't found a formal mentioning of spoofing or jamming or anything like that. They usually talk about interference, but again unfortunately, there is no differentiation between the deliberate and the undeliberate or intentional interference or jamming. We usually, I don't know, suppose the goodwill of the radio receiver. This is not the case. And having said that, this conference is a must attend for me to learn about that and to try to bring some of this information back to the ITU. So long question short, I think there is a long way that we should go at least on the international level. Thank you, Rebecca.

DORCH: Thank you. All right. I'm going to jump over to the highest rated question on the—from the audience right now. So, and this is for Professors Reed and Tripathi. So, you focused on the benefits of 5G. Of course, there's no free lunch. So what are some of the drawbacks and tradeoffs of moving to 5G?

TRIPATHI: Dr. Reed, can you start?

REED: Yeah, I think one of the drawbacks is going to be power consumption. And sometimes, although standards have these lofty goals of achieving certain efficiencies, right now power consumption is the key issue, particularly for the service provider.

TRIPATHI: Yeah, very good. And from the nontechnical side, I would like to add that we have to invest money, right? This is a new hardware, new software. We have changed the New Radio, okay? So this is from old LTE radio to the NR radio. So the radio interface is completely different. Radio network architecture is different. We are breaking the radio into two pieces, central unit, distributed unit. So that is completely new. And the core network, you will not find any LTE network element. Everything is new. And virtualization is the way we implement. So basically, we are changing everything. So that means we have to invest money, right. So that is another challenge. The cost will be also an important factor. But if you look at performance, you cannot compare LTE and 5G. 5G will give you much better performance. So from technology perspective, yeah, 5G is the way to go. But we have to balance as an operator, how fast do we deploy 5G and where to deploy 5G. Thank you.

REED: I'd also say that getting trained personnel who understand 5G, because there are the major significant differences between 5 and 4G. And there's just not that many people who really understand the standard that well at this point.

DORCH: Thank you. Did someone else on the panel want to say something more? Okay. So I'm going to take another—I'm going to combine one of the audience questions with one that I was wanting to ask, and that relates to the security issues that have been fixed in 5G, but then those that remain in—remain as vulnerabilities in the non-standalone deployment. And Jeff, I hope you've got your audio fixed so that you can chime in here. So when you were discussing the security enhancements with a 3GPP standards for 5G, you mentioned separate an SS7 or signaling channel, as an example. And I was wondering is the enhanced security important because in the non-standalone version of 5G, we still have that separate signaling channel? And does the architecture for the non or for the standalone 5G eliminate that separate signaling channel? And then that kind of feeds into what are the vulnerabilities between the non-standalone that we're still dealing with right now? So.

CICHONSKI: Yeah. Can you hear me now?

DORCH: Yes. Thank you.

CICHONSKI: Yeah. So the question from the audience was a very good one. In a 5G non-standalone world security is exactly as it is in LTE. All the new fancy features I talked about are really provided by that 5G core. And we don't have a 5G core until we move into that 5G standalone architecture. So with that 5G standalone architecture, that's when we get some protection from the roaming interface, SS7 attacks with a security edge protection proxy that has been standardized by 3GPP. So it's a really important point that as we kind of—these initial deployments of 5G are rolled out, to understand that all the new security features that get talked to about—in line with in 5G in the same breath that they don't really—they're not

available until we have a 5G standalone implementation where we can enable those features as needed by the different operators.

TRIPATHI: Yes. I would like to add for clarity, because there are different radio and core network combinations as Dr. Reed had mentioned. So we need a 5G core network basically. Until you have a 5G core network or the features that Jeff—not available. Yeah. Thank you.

DORCH: All right. Thank you. I'm going to throw out a request out to the backend folks here. So Matt, when we've got a question that is high, that's listed on the most liked, if it's been answered, would you mind making a note in the chat that it's been answered so that—so it makes it a little bit easier for me to find the right questions. Okay. So the next question that we've got in the audience chat is for Dr. Ghosh and it has to do with the spectrum sharing. And there's a couple—she's got a two-part question here. So I'll just go ahead and ask both of them to you.

Spectrum sharing seems to be a key enabler especially for CBRS—and by the way, congratulations on the status, the bids on the CBRS—so, enabler for CBRS and the 5.95 to 7.125 GHz, should academia revisit the large body of work on cognitive radios that was popular over the last decade? And how do we ensure that the missteps of the TV white spaces related to cognitive radio are avoided? And then the second part is, if indeed cognitive radio technology is seen as one of the enablers to optimize sharing and use of spectrum, does the FCC have a process to certify such devices that can adapt based upon the RF environment?

GHOSH: Thanks, Rebecca and thanks Kaushik for those questions. So I think, as part of the academic community that participated in a large body of work on cognitive radio, I think one of the disconnects has been that a lot of the academic work was done, I would say, in isolation. So today, when we talk about sharing within the FCC, there is still gut level distrust of completely cognitive radios that adapt based on RF spectrum sensing, even though personally, I'm a big fan of sensing. So given the situation we are in most of, if you look at what we did in CBRS, what we did in 6 GHz, we endeavor to make sharing possible by crafting our rules, which were not based on cognitive radio per se, but were based on sharing in such a way that we think interference will not occur. So for CBRS, for example, it was mainly based on exclusion zones based on where these Navy radars were. So there was kind of a combination of sensing and databases, right? So you try to figure out where interference will occur based on sensing, but then you don't leave it to the individual radios to adapt their RF on their own. So I think as we look forward for cognitive radio and how they're most likely to be implemented, the academic community in particular needs to pay, I think, more attention to the realities of how—and that goes into your second part, right? How does FCC certify that? And that in my mind is actually a research question too, which I would encourage the research community to also pay some attention towards that. How would you go about reliably certifying radios that are adjusting their use of the spectrum in an adaptive manner? And definitely, I think, when you say revisit, I hope it's revisiting with a view to looking at what the on-ground reality is and trying to adapt to it. I think the FCC is quite open to new methods. But at the same time, when you're trying to coexist say with a Navy radar, right, you really have to be completely sure that whatever cognitive methods you've developed that rely solely on a device detecting and getting out of the spectrum work in

a foolproof manner. So whenever you're looking at coexistence with some of these critical and life and safety kind of applications, it becomes harder.

But these are important research areas that I think need to continue. And I would encourage the research community to definitely continue working on these. In terms of missteps of TV white spaces, I think, we should learn from them. I think there were a lot of other things going on. This was the first time that the FCC was attempting any kind of sharing. We've learned a lot. And the fact that CBRS today has come to fruition and we're getting licenses auctioned, and there's a lot of excitement, does indicate that we have learned a lot in the process. But there is still a lot of, especially the certification piece does remain a problem that we struggle with.

DORCH: Thank you. Dr. El-Moghazi, I guess the next question is coming in for you. In the U.S. some worry about 5G encroaching on other services. For example, there have been discussions or a lot of arguments about interference to weather satellite observations in 24 GHz and GPS in the L band. Have similar debates occurred in the rest of the world?

EL-MOGHAZI: Thank you, Rebecca. Thank you, Pierre, for such an inspirational question. And, again, I would put my disclaimer that this is very personal view. I think the U.S. and the FCC are on the frontier line for innovation spectrum policy, and that comes at a price. So it was the U.S. that adapted the concept of having Wi-Fi, Bluetooth operating in the 2.4 GHz band, usually called at the '80s, as the junk band—junk bands. It was the U.S. that adapted the 5G and the 28 GHz. It was the U.S. that called for full flexibility in the UHF broadcasting band. And it was the U.S. which allowed CDMA and GSMA at the time 2G and it stimulate competition. So no, I'm not aware of any similar heated debate in other countries, but it doesn't mean that you're doing something wrong. Democracy is not an easy process, and it comes at a price. And yet, I think the U.S. is able to stimulate innovation. Many things will succeed, a few things will not be successful, but at the end of the day, this is the price. If you want to come at the frontier line of 5G or any other spectrum policy. Yeah. Thank you, Rebecca.

DORCH: Yes, Dr. Ghosh.

GHOSH: So thanks for that, Mohamed. And just to add onto this, I think what some of these debates around the 24 GHz and other spectrum bands are throwing up is—and again, I'm speaking—please take what I'm saying as my personal opinion and not as an FCC opinion. But I think what it shows is how important adjacent channel issues are going to be going forward. A lot of these debates are arising because we are trying to find spectrum in an already packed spectrum scenario. We are packing things together, and yes, adjacent channel issues are going to become more important. And that is where I think policy, and technology, and everything needs to come into play as to how we deal with this, because it's not going away, whether it's 5G today or any other system, any spectrum we look at, we're running up against this issue about how do we handle what's in there next to whatever spectrum they're allocating. So again, a meaty research topic for academics in particular to talk about.

DORCH: And I assume also particularly for the not only radio navigation—oh, now I forgot my words. The space observations sorts of frequencies and devices.

GHOSH: Yeah. And I think the faster protecting passive users is really, really hard. And that is something where I think we really need better technical solutions as well as policy angles to address those kinds of interference issues.

EL-MOGHAZI: So Rebecca, you were talking I think about the EESS services in the 24 GHz. And I'm aware that in the U.S. you had a very hot debate on this, but I would encourage, I don't know, participants to look at what's been going on in the ITU. So perhaps the U.S. or FCC view was opposed within the U.S. but it's adopted by other countries outside of the U.S., which means that it's mostly valid. So yeah. Thank you.

DORCH: Thank you. I want to ask, Jeffrey, I think, a question on this one. So in both—excuse me. Jeffrey Cichonski's presentation, you mentioned the various standards development organizations that are working on the 5G related matters. And you also mentioned the IEEE 802.1 Wi-Fi standards. And then Dr. Ghosh in her presentation also mentioned how important Wi-Fi is for 5G for spurring innovations for both licensed and unlicensed. So can you, either one of you, maybe speak to how these different standard bodies ensure that the intersections between their standards actually work?

CICHONSKI: Yeah. I can take a stab at just scope of work from a standards perspective, assuming you can still hear me.

DORCH: Yes. Thank you.

CICHONSKI: Yeah. Great. So all these different standards organizations obviously have different missions and objectives of what their—what they see their scope of work being. As we work through issues, technical issues, in a group like 3GPP SA3, we understand that there'll be an intersection where we want to utilize a protocol that might be defined by a different standards organizations. So there's a process through exchanging liaison, very formal liaison statements and questions that we can send different standards organizations and standards working groups specific questions around kind of, "Hey, this is what we're doing as 3GPP SA3 or as 3GPP. We'd like to utilize this protocol, or we think you need to make a change to this protocol" and make very formal requests from that perspective. But there is a sense of respecting what the different standards organizations are doing and where their expertise is and the understanding that all these groups need to be working together in kind of a collaborative way. I'm not sure if you wanted to add anything else, any of the other members of the panel.

GHOSH: Yeah. So I can say a few words about, you know, coexistence. I think you brought it up Rebecca about coexistence and the unlicensed bands. And so it's mainly 3GPP and IEEE 802.11 who are deploying—who are developing the cellular and the Wi-Fi standards respectively. And I know that they've had joint workshops. They do they do talk about their needs. Personally, I think it could have—it could be a better job, but I think, for example, if you see what ETSI came up with recently in 6 GHz, for example, they've come up with a common sensing threshold, which did not exist in the 5 GHz band. So I think the standards groups are learning and they're understanding that more and more systems have to be—have to co-exist. I definitely think that it could be better, but in the—at the end of the day, industry has partitioned itself into standards

bodies and there are developed standards specific to certain system and they have to talk to each other to better coexist. FCC, at least, unlike some regulatory bodies, takes a hands-off approach. We try to make the rules fairly broad and we leave the details about specifications and standards and how the system should interoperate up to industry. And I personally think that has worked pretty well, and hopefully that will continue.

DORCH: Thank you. Let me follow up with another sort of standards related question. And that is Jeffrey, you had mentioned that it's harder for someone to barge into a 3GPP meeting and push a specific solution to a problem because it needs to be informed at both the technical level and make sense within the system that they're working with. So can academics, small businesses, entrepreneurs, do they have an opportunity or means to be able to participate in those standards organizations?

CICHONSKI: Yeah, that's a good question. Participation is definitely a combination of kind of being in the room, being present, having a voice, having an opinion on multiple different topics as well as providing informed contributions, building kind of that reputation for an organization. So that's kind of what makes it hard for like a newcomer to come in and say, "Here's a solution to this problem." That might be way out from left field. It doesn't quite make sense. It'll be looked upon with more skepticism because that person might not kind of have that presence in the group or have that technical expertise of the system. But it is a good point of, yes, academics, small businesses. Really many organizations can participate in—specifically 3GPP, their working procedures are you have to participate through a membership which you purchase from your regional SDO. So from the U.S. perspective, we are a member of ATIS, and we purchase a 3GPP membership from ATIS and we attend on behalf of ATIS. It is a cost. It's not a small dollar amount. It's definitely an investment to be in the room and making those contributions and having a voice.

DORCH: [Thank you] Jeff. I'd like to go back to an audience question here. And this one is detailed, but we've got four likes on it. So hopefully, it'll—So this one, I guess, is for a Professors Reed and Tripathi. Can you provide a little more detail on the difference between polar coding and convolutional coding?

TRIPATHI: Yeah. Okay. So basically, what we have in LTE for low rate channel, like control channel, physical downlink control channel, we have convolutional coding. But in 5G, we moved away from that and started using polar coding. Now, the way to look at this tool is this, in convolutional coding, we have a formula, a mathematical formula that performs x or functions of the current bit and certain number of previous bits. How can we get the code symbols? Convoluted code symbols. On the other end, this polar coding is kind of a block code. So we have a block of bits that go into the polar coding and we get a block of symbols out. And those symbols that are coming out, they are obtained by doing some kind of transformation, something called channel combining, channel splitting? Okay. But basically, polar coding is a block code. And the reason that we are using this polar coding in 5G is that compared to the convolutional code, this kind of polar code is more efficient. So it can be obtained reliably, plus it consumes less power. So you get better performance at a lower power consumption. So that is why we moved from convolutional to polar in 5G. Thank you.

DORCH: That one. Thank you. Next question is, I think this may be about, well, close to the last of the audience questions, and then I'm going to ask some closing questions for the panelists. But there's a question for, I believe, Dr. El-Moghazi because it says there's been some concerns about the security, especially of the cybersecurity and threats. Is there a plan for the ITU to incorporate the Zero Trust Architecture?

EL-MOGHAZI: Thank you, Rebecca. Again, I was motivated by the title of the conference to dig more into what the ITU is doing with security and the standardization sector, the ITU-T, is doing a lot of things when it comes to security. In fact, it has a dedicated study group for security issues. However, I haven't found the Zero Trust architecture adopted in there. And, again, nothing related to the security on the spectrum level. So maybe in the ITU, we are talking about different language. Remember it's 193 countries. So perhaps it's still too early for a concept like Zero Trust to be adopted at the international level. Thank you, Rebecca.

DORCH: I think we've got about 10 minutes left and I'd like to kind of open it up to the panel and ask each one of you if you can talk a little bit about what you see, I guess, or perceive or envision for 6G.

REED: I can go first. My view of 6G, I think there's two key things. One is that'll fix problems with 5G [brief laughter] as both standards try to do, fix the problem, the issues with previous standards. I think that they'll probably try to improve the latency and some of the power issues associated with 5G. And number two is the inclusion of AI everywhere throughout the network. And although this is being done today to some extent, and there's a lot of research going on within academic circles, it's going to take a standardization process to get the full benefit of AI. It's going to be tough, but I think it's going to be an important contribution of 6G.

TRIPATHI: Yeah, I would like to add. So as Dr. Reed mentioned, latency would be probably around 100 microseconds. Today in 5G, it is below 1 millisecond. The peak data rate would also be very high, right. So from 20 gigabits per second. So we plan to go to 1 terabits per second. Let's say it's like 1,000 gigabits per second. So it will be very high. What technologies do we use? So as Dr. Ghosh mentioned, if you need high data rate, you need to go to higher band. So the FCC has done something called some Spectrum Horizons Order, but they have released some spectrum or experimental licensing at this moment. It's more than 100 GHz, kind of a spectrum we're looking at. So maybe we'll see some terahertz communications and we will need new kinds of antenna technologies and power amplifier technologies that because Dr. Reed mentioned the power efficiency is a big problem. You can lose 50% of the power just within 1 inch. Okay. Within 1 inch, you will lose 50% of the power in the power amplifier. So you have certain power amplifier rating. By the time it goes out of the antenna, you lost 50%. So efficiency will be a problem. So we need to do something to make it work. Yeah. Thank you.

GHOSH: So if I may add to those thoughts from Jeff and Nishith, I think, well, there is this feeling in the industry that the even Gs are more successful than the odd Gs. 4G was more successful than 3G so as Jeff Reed mentioned that maybe 6G will fix all the problems of 5G. But just seriously, 5G is attempting to sort of do many things in one standard. And the expectation is that not all of it will be completely come to fruition in the 5G roll out. So if you look at spectrum,

6G definitely there is a very strong, active research community and effort in the, I wouldn't necessarily call it terahertz, but in the high hundreds of GHz range. But when you go up there, your architectures change completely. And it'll be interesting to see what, you know, how you make a mobile cellular network work when your propagation limits you to maybe a few meters. And another thing I want to mention, which we didn't talk about much in this panel is about both the core networks as well as the virtualization, the open RAN movement where now you're talking about really having remote radio front-ends, and then everything is done, you're basically disaggregating the entire radio access network. Yes, that will happen in 5G and we'll get started in 5G, but I think making it standardized, right now you have a lot of bodies working on this, but there isn't—it's not a standard in the sense of how 3GPP has standardized the radio interface. Doing that will really open up what you can do with things like AI, for example, because now you have a lot more control points into the network. You have a lot more ability to get data from different parts of the RAN. Today, the RAN is a very closed system where unless even the operators sometimes have a hard time getting into the internals of the strand. Again, a lot of these ideas will be fleshed out in 5G, but maybe they get actually standardized and deployed in larger scale in 6G.

TRIPATHI: Okay. But I will like to add—one point that we are looking at the tip of the iceberg right now. 5G has a lot of potential. Okay. So by the time we go to 6G, we will see many more things in 5G.

EL-MOGHAZI: Rebecca, if I may add, I'm taking advantage of the hat of the developing countries given that perhaps I'm the only one in the African continent right now that will talk about the 6G. So my question is that, do will really need 6G things? Are we already utilizing the 5G? Not talking about some countries that have not yet deployed 4G. And a second question inspired by Professor William Webb he's one of the participants, why are we still playing the generation game? Why is 5G or 6G? At least in the 5G, this is a unilateral word. Everybody is talking about the 3GPP. For me, and this is my personal view, it's not a good thing. We need some sort of competition. We need countries like the U.S. investing in having new technologies for the radio access. Otherwise, I don't expect 6G to be much different from 5G as currently designed to be. And if you look at the draft white papers of 6G, it's enhanced its vision of 5G. So perhaps it's time just to relax and think about what we really need for the future. And thank you, all.

CICHONSKI: Yeah. And I'm happy to go last. I'm hoping you can still hear me. I think from a security perspective as it was with 5G, the security architecture, we're going to continue to evolve. And first of all, fix things we didn't quite get to with 5G. And secondly, we're going to have to address all the security issues that researchers find as the 5G implementations become more and more mature. But just like what happened with LTE, it was a technology that was around for 10 years. Researchers continually find issues with the standard, with the implementation, with the deployments. So from a security perspective, I think the security posture will continue to evolve and become better and better over time, and that is very relevant for 6G. And I think from a kind of functionality and feature perspective, I think with 6G, there's the opportunity to actually realize like the cloud-native design principles that went into 5G that we might see realized, but we might not as was mentioned. I think there'll be the

opportunity to actually deliver on some of the promises 5G brought, but we didn't quite get to. And I see some of those cloud native principles making their way to the RAN. So that antenna really just becoming a physical piece of hardware where everything behind it is virtualized kind of like an internet application.

DORCH: Thank you for bringing us back to the radio access network also [brief laughter]. So we've reached the end of our allotted time for the tutorial panel, and I would like to sincerely thank all of you on the panel for your generosity in sharing your knowledge and your time with all of us. So virtual applause for all of you.

We will now go into a break, but before we go, let me just say that the agenda for the day will be visible on the BlueJeans Events platform during the break. ISART 2020 will resume at 1 o'clock with opening remarks from Dr. Sheryl Genco, the director of ITS, and that will be followed by our key leader round table discussion, joining NTIA's Doug Kinkoph. From our ISART co-hosts, we will have Walt Copan from NIST and Terry Fiez from the University of Colorado Boulder, who will then set the stage for the remainder of ISART. And then we will follow this afternoon with Dr. Joe Evans, we'll close out the formal presentations for today with a keynote address. The afternoon panelists will all be available to chat with you in breakout rooms after the conclusion of the Q&A following Dr. Evans' keynote. Information on accessing those breakout rooms is in the confirmation email that you all received and in the ISART app for those that are able to download and access it. And technical support will be standing by as this is our very first, fully virtual ISART. So thank you all for joining us this morning from the tutorial. We'll see you this afternoon, and good day for now.

## 1.3 Opening Discussion: Setting the Stage

### 1.3.1 Sheryl Genco: Introduction of Panel and Opening Remarks

GENCO: Hello, everyone, welcome to ISART. My name is Dr. Sheryl Genco. And I'm the Director of the Institute for Telecommunication Sciences, the Nation's spectrum and communications lab. On behalf of NTIA, I welcome all of you to ISART 2020: the returning ISART veterans and those who are new to ISART, those joining from different time zones around the world, especially students who will become the next generation workforce leaders for 5G and beyond. Welcome, and thank you for joining us.

Along with our 2020 co-sponsors, University of Colorado Boulder and the National Institute of Standards and Technology, NIST, we have put together an agenda and a roster of exceptional speakers, panelists, presenters to tackle the challenging technical and policy issues around securing spectrum for 5G in zero trust environments. Our collective goal is to leave ISART 2020 with new insight, hopefully, some eureka moments and ideas to propel us forward to solve some challenges and for securing 5G and a zero trust network. Maybe even some ways we can all work together. I'd like to quickly introduce myself. And then I'll provide some insight into our theme this year, run through the overview of the layout, the flow of this first ever fully virtual

ISART and explain some logistics. Then, I'll introduce our distinguished leaders who will set the stage for the remainder of this symposium.

So I came to ITS, the Institute for Telecommunication Sciences in May, and prior to that I was with Honeywell Quantum Solutions. My PhD is in electrical engineering and I specialize in microwave optics. I've been around for a while and I am very excited to be part of NTIA and working outward with all these excellent people throughout the government and the country. ITS realizes, its goal is to realize the full potential telecom into new eras of innovation. And these eras are just what I wanted to do when I applied for this job. So if any of you would like to contact me or talk more about and I'd be happy to do that.

Focus of ISART 2020 is on 5G spectrum and zero trust network. This was settled before I even joined ITS. It was sparked by the closing keynote address by Dr. Lisa Porter, whom we are honored to have on our morning panel tomorrow, at the University of Colorado Silicon Flatirons "Saving Our Spectrum" conference last fall. At that conference, Dr. Porter said: "There's no such thing as a secure system. We can work to make things more secure, be mindful of vulnerabilities. But ultimately, we must effectively use networks in which we have zero trust." This prompted ITS, whose researchers are all too familiar with spectrum interference issues, to look into what the new significant research and writings were around zero trust concepts and what they were saying about spectrum. Finding none at that time, the theme for ISART 2020 was born. The future wireless systems, 5G and beyond are expected to offer major economic benefits to countries and companies that could deploy those networks and services reliably, quickly, and securely.

Yet spectrum, the foundation for much of 5G presents unique security challenges in addition to a multitude of technical, economic, regulatory political challenges. While spectrum security historically focused on jamming, spoofing, interference, a consensus developed that ISART was an appropriate vehicle to bring together those experts from government, industry, and academia to reexamine what spectrum security means in the context of zero trust environments, architectures, and networks. As ISART veterans will be shaking their heads, "yup," while I bring up a little historical aside to explain why I think this symposium is so important. For others, I share this story to emphasize why your participation in ISART is so incredibly valuable and potentially transformative—transformational.

About 10 years ago, nearly simultaneously with the 2010 presidential memorandum that directed NTIA to identify 500 MHz of federal commercial spectrum that could be repurposed for wireless broadband, ISART facilitated open and well-engineered dialogue between government, industry, academia about the broad topic of spectrum sharing. An IRAC panel for example, illuminated existing interagency spectrum sharing processes and set a basis for overall discussion. In 2011, ISART focused on the unique challenges and opportunities related to spectrum sharing with radar service.

A consensus was reached that spectrum sharing in the 3.5 gig band was a good potential for economic success. ITS followed up with ISART 2012 ,with occupancy measurements in 3.5 GHz near San Diego, which fueled emergency policy discussion around Citizens Broadband Radio

Service. Ten years may seem like a long time, but to go from theoretical analysis of potential feasibility of using the same spectrum band for high powered DOD radars and a low powered commercial wireless terrestrial service to initial commercial deployment of actual proven operational spectrum sharing is remarkable. I hope that ISART 2020 proves equally, foundationally important for 5G and beyond wireless services.

Our virtual ISART 2020 is structured into two, two-hour blocks each day. The organized—organizing committee has worked very hard to find ways to incorporate tools real time interaction among our panelists and in depth, plenary talks, highly interactive Q&A and opportunities for networking and conversation breakout rooms. Right now, I'd like to thank our co-chairs Andy Thiessen from ITS, Melissa Midzor from NIST, our Vice Chair, Rebecca Dorch from ITS and a special thanks to an ITSer, Lilli Segre. In addition, our Technical Advisory Committee members from CU, Dale Hatfield, Pierre de Vries and Keith Gremban, all of whom you'll see in various capacities and settings throughout the next three and a half days. Thank you all.

I'd like to encourage all of you to use the interactive tools, ask questions, converse with our panelists and presenters in the breakout rooms. We hope this will be very fun for all of us.

This morning, many of you tuned into an excellent tutorial session that provided a baseline understanding for current engineering, technical, security, spectrum, and international aspects of 5G. The tutorial presentations were graciously recorded by the presenters allowing any of you to return and check them into the baseline understanding later on.

This afternoon, we officially kick off the formal ISART program and with a roundtable discussion between leaders of NTIA, NIST, and CU to help us set the stage. Then, our keynote will be given by Dr. Joe Evans, who is spearheading DoD's efforts to operate in zero trust environments. Tuesday morning will feature our framing panel of experts with experience in government, industry and academia diving deep into what zero trust means with spectrum and then the world, and the known risks that exist today at the intersection of 5G, new radio, NR, and zero trust networks.

Recognizing and naming the risks and vulnerabilities is crucial to identifying areas for research and developing solutions to better secure the spectrum that 5G serves. The technical core of this program is contained the next four panels which will examine 5G networks from the perspective of first, ways to design 5G radio layer for resilient services. Second, how to implement secure and resilient technical solutions during deployment of new networks, including new network parts and features. Third, ensuring resiliency within a network set of operations including handling spectrum interference. And fourth, how monitoring and data collection can and should provide valuable input feedback into design deployment operations to improve resiliency of the network. The final closing and wrap up panel on Thursday afternoon features polymaths to help draw new insights and connections, identify potential new research areas, and hopefully add to the history of ISART triggering important out of the box thinking innovative ideas I'm particularly looking forward to this week.

The last half hour of each of the two-hour blocks of ISART content is actually reserved for our breakout rooms. We hope the breakout rooms can begin to replicate to the extent possible, a virtual environment where we can have critical personal interactions with speakers and other participants that has always been a hallmark of ISART. After each panel concludes, the panelists and speakers from the sessions will exit the BlueJeans Events platform and head over to the BlueJeans meetings platform for their breakout room. For those of you able to download and access a brand new ISART app, all the information and links needed to find in the breakout rooms are the app. In addition, in the ISART confirmation email, everyone should have received last Friday, there was a Quick Links that contains a nine digit room number for the date and time each speaker and panelists will be in the breakout room. They'll be ready and available to chat with you at that time. Room hosts from ITS, NIST, and CU who are our co-host organizations will be there to help if needed. If you run into technical difficulties reach out to the conference services staff listed in your confirmation email. Yes, our app will allow you to reach out and connect with each other. By default, the only information anyone will see on the app is your name and affiliation. So if you're open and interested in chatting with others, networking, exchanging virtual business cards, please remember to go in the app and add whatever information you're comfortable in sharing. We're also able to get a few 5G equipment suppliers and vendors to join us today this week. So please virtually wander over to their rooms on the app tomorrow and check out the demo videos and ask questions.

I'd like to just take one brief second to thank conference services as well. They've done a great job of preparing us for ISART. So thanks everyone out there.

Now, without further ado, I'd like to briefly introduce our distinguished guests for the opening of setting the stage roundtable discussion. Full bios of speakers are in the program and in the app. I encourage you to check them out and read more about their wonderful accomplishments.

Doug Kinkoph, my current manager and boss has a very long official legal title. But for brevity, he is the Acting Assistant Secretary and the head of NTIA, a position he has held since January of this year. He has been with NTIA for more than 10 years, and when not serving as the acting head of NTIA. Heads up the NTIA's Office of Telecommunications and Information Applications that administers the Administration's broadband programs.

So you all know Walt, right, you're probably better. So Walt Copan is our NIST, the leader of NIST. He is director of NIST, since I believe it was 2015, 2016. He served as the DOE's National Renewable Energies Lab Principal Licensing Executive, and joins us today as our leader from NIST.

Terri Fiez is the Vice Chancellor for Research for the University of Colorado Boulder, a position she's held since joining CU in 2015. After 15 years at Oregon State University and including as a head of their Department of Electrical and Computer Engineering, and a Vice Chancellor position at CU, Dr. Fiez leaves the campus research enterprise and this summer has been working diligently on securing the campus for students to return. But with that, I want to thank everyone again. And I'll introduce Doug. And with that, Doug, you can take it away. And we'll talk to you later.

### 1.3.2 Doug Kinkoph

KINKOPH: OK. Thank you, Sheryl. Thank you. It's a pleasure to be with you today. And I welcome everyone who's tuning in. Sheryl, thank you for that great introduction on the role ISART has had in advancing thinking on spectrum solutions. This year, even in our virtual environment, ISART continues to provide a unique opportunity for people with diverse interests to share their perspectives in collaboration and collegial environment. I want to thank our ITS staff and our co-hosts in Boulder for their dedication to the success of this year's conference. I do want to take a moment to recognize Dr. Genco, Sheryl, who joined us this summer as ITS director. It's really hit the ground running. And I'm not surprised, and anybody that knows her is not surprised with such an impressive background from her work on quantum computing breakthroughs to her support on STEM education. So it was really become a fierce advocate for ITS and its staff. And we're lucky to have early this extraordinary team. So thank you, Sheryl.

We've been asked today to help set the stage for this year's theme on 5G spectrum and zero trust network. The conversations we'll be having today and throughout the week on 5G and security are really essential. From day one, the administration has recognized the importance of 5G wireless technologies to our economic and national security. They've also been clear-eyed about the risk and vulnerabilities posed to those who seek to exploit these technologies. NTIA has played a key role in a collective effort to ensure that the U.S. leads the world in secure 5G and beyond that includes our work on botnets that began early on in the administration, our work to implement the National Strategy to Secure 5G and our ongoing collaboration with federal agencies, and the FCC to free up spectrum for commercial use.

Over the years, our expertise with experience and expertise with spectrum clearing and sharing has taught us that a mix of techniques can free up spectrum while still protecting federal capabilities. While we will always look at clearing, a combination of some relocations and innovation, sharing methodologies can often be the fastest most efficient way to accommodate federal and nonfederal uses.

Last month, we delivered a report to Congress summarizing our assessment of a key swath of mid band spectrum the 3100 to 3550 MHz range. Our report concluded that the 3450 and 3550 sub-band is a good candidate for potential spectrum sharing, including at the commercial power level sought by the wireless industry. We are moving forward aggressively on the work needed to make the spectrum available as soon as feasible.

150 MHz spectrum just above that is the CBRS band which represents a watershed moment in the development of dynamic spectrum sharing mechanisms. This year, we've seen licensed by rule commercial services launched throughout this band. The FCC is currently offering licenses for the CBRS service, and bids are now approaching $3 billion. It appears that the demand that we had thought was there from mid band is active. CBRS is a culmination of nearly a decade of hard collaborative work with our partners at the FCC, Department of Defense and the private sector. And NTIA is proud of our contributions to the success of CBRS, including the work of its ITS Boulder shop, which conducted prototype testing of the key components of the innovative spectrum sharing technology. We are eager to see this technology achieve its full potential.

Collectively across government, we're taking action so that we can meet the demand of spectrum to enable the promise of 5G and other technologies of the future to come to fruition. Achieving that promise is about more than just building out networks. It's equally important to ensure that 5G services can be safely and securely accessed by Americans to consumers and industry. In March, the president signed the Secure 5G and Beyond Act into law. And the administration published national strategy to secure 5G. The strategy is focused on four lines of effort: facilitating the domestic rollout of 5G, assessing the cybersecurity risks of 5G capabilities and infrastructure, addressing risk to U.S. economic and national security, and, fourth, promoting responsible global development and deployment of secure and reliable 5G infrastructure.

This summer, NTIA sought public input to inform an implementation plan to secure 5G. We would like to thank everyone who took time to provide their views, the National Security Council and close coordination with NTIA and a range of other departments and agencies leading the development of a plan which will lay out specific activities to achieve the strategy's goals.

In a separate track last month NTIA announces establishment of a communications supply chain risk information partnership. This is a program required by law that is targeted towards small and rural equipment suppliers and providers of communication services. Our goal of the program is to improve their access to information about risk, the key elements in their supply chain. We plan to build it out in phases, and we'll be incorporating feedback from recent public comment to ensure that this important risk information is relevant and accessible.

On behalf of our co-hosts, I once again want to welcome everyone to ISART. I'm excited about our program this year. On Wednesday, you'll hear from Jaisha Wray, who recently joined NTIA to head up our international office. We're excited to have Jaisha join us. Even as we're limited in our ability to travel right now, our work continues with our international partners to achieve the U.S. interest in the future of a secure 5G and beyond environment. That's what we're all here to work towards. I'm so glad we're able to offer this forum to talk about how we can get it done. And thank you again to everyone for joining us today. And with that, Walt, I'll turn it over to you.

### 1.3.3 Walt Copan

COPAN: Excellent, Doug. Thank you so much, and I'm delighted to be part of this fireside chat session to kick off ISART 2020. The National Institute of Standards and Technology, NIST has been a leader in developing innovative, groundbreaking research and development solutions, measurements, and standards for communication technologies for nearly a 100 years and we continue to do so today. The mode of NIST operation is as a partner, a partner to industry and across government and the public sectors.

The history of NIST goes back to 1901. NIST created the first radio that could run on AC current and pioneered a number of military applications including the radio triangulation that was successfully used to locate ships and coordinate battery fire during World War I. NIST is known as America's innovation agency with wide ranging collaborations around the globe, including

with national metrology institutes and across the science, technology, and industrial communities.

I'm just delighted to be part of ISART this year. NIST has a lead role in standards development on behalf of the US government and coordinating with other agency experts, as well as, with the private sector. In advanced communications for 5G and beyond, we're a leader in wireless R&D and in standards development with over 30 NIST experts engaging in international standards development activities for communications. Just within our communications technology laboratory held in Boulder, Colorado, we've published over 320 research papers just in the past five years. Our experts lead in the all-of-government efforts to secure the future of 5G and beyond wireless communications infrastructure for the United States. And we truly are partners across governments and with the telecommunications sector in our standards development and the sector looks to NIST for strategic guidance, such as the publication of the Future Generation, Wireless Research and Development Gaps Report, which identifies several of the most significant needs facing the wireless industry today.

NIST also lead the IEEE 5G and beyond roadmap working group to identify hardware technology gaps for deploying millimeter wave fixed and mobile wireless resulting in the IEEE 5G and Beyond Roadmap white paper. Just last week, NIST announced that our Communication Technology Lab engineers have developed a flexible, portable measurement system to support the design and repeatable testing of fifth generation wireless communications devices with unprecedented accuracy across a wide range of signal frequencies and scenarios. The system is called SAMUAI which is short for Synthetic Aperture Measurements of Uncertainty and Angle of Incidence, which is the first to offer 5G wireless measurements with accuracy that can be traced to fundamental physical standards. The traceability is a key feature to assure accuracy of results. And it's small enough to be transported to field tests. So we're looking forward to this system being even more broadly deployed in active arrays in millimeter wave frequencies above 24 GHz with highly directional actively changing antenna patterns. And of course, we know many of these are now utilizing artificial intelligence and machine learning protocols as the guide.

NIST also relies on public-private partnerships in carrying out our programs. For example, the National Advanced Spectrum and Communications Test Network, NASCTN, which is a multi-agency chartered partnership that includes DOD, NASA, NOAA, NSF and, of course, NTIA, as well as academic partners and commercial carriers through the coordinated carrier test program and CTIA, the Wireless Association. It's great to have a facility like NASCTN, which leverages leading experts in radio frequency spectrum analysis across its partnership to understand the impacts of potential interference, and also to evaluate spectrum sharing strategies for both federal and private sector users. And these analyses are neutral and informed by expert science to allow industry to build value using spectrum while maintaining important national missions. NASCTN has issued a series of important reports in both 4G LTE, CBRS, and now beyond in the build out of the 5G testbed. And NIST and NTIA are working hand in hand to implement the government's strategy to secure 5G most notably in developing R&D priorities for 5G and beyond and in developing strategy for international engagement in communication standards as Doug has mentioned. Also, the 5G Millimeter Wave Channel Model Alliance is a NIST-sponsored

International Research Consortium to advance breakthrough measurement, calibration and channel modeling approaches that are used for 5G and beyond.

And of course, cybersecurity is its top priority for the United States. And NIST has a unique leadership series of roles in cybersecurity for the government and industry. Our Cybersecurity Framework has been adopted by many nations and organizations. And at the [National] Cybersecurity Center of Excellence, the NCCoE, which is a federally funded research and development center, we partner with industry to provide practical example solutions to help address pressing cybersecurity challenges, in particular with 5G deployments.

And we've been pleased to provide foundational guidelines, including our Special Publication 800-207 on Zero Trust Architecture, which I know this conference will be discussing in detail. The zero trust architecture guideline is a series of model architectures and best practice guides. And it's intended to be a living document to continue to evolve as we look at deployment of security in zero trust applications for 5G and beyond.

Another important area we're leaning forward on is strengthening supply chain security. Clearly working with our government partners and also, within industry and academia, to develop guidance to ensure that supply chain for communications infrastructures will be secure from cyber or counterfeit threats, and that we can provide measurable guidance on how to maintain that security through manufacturing and distribution processes. And so, there's a NIST program that is a planned approach for supply chain security that's intended to be less expensive to implement than provenance base security strategies that can be implemented and independently verified at multiple levels across the supply chain through a rigorous testing protocol.

Public Safety Communications Research is another elements of driving innovation using price challenges and strong partnerships, including FirstNet and NTIA, advanced cryptography is another key element of NIST work, supporting secure communications and data protection, including post-quantum cryptographic algorithm and key distribution systems for the future.

So in wrap up, NIST is committed to developing leading edge solutions from our unique vantage point grounded in rigorous measurement science and standards, and engaging broadly in stakeholder partnerships. Thanks for being part of our conversation today. Let me turn it over to Terri Fiez from the University of Colorado Boulder.

### 1.3.4 Terri Fiez

FIEZ: And I'd like to cover three things. The first I'd like to talk about is the research landscape, not only nationally, what you've already heard a part of that, but also looking at what is—what we're doing at University of Colorado, followed by workforce development. I don't think we can have a conversation about what universities are doing without talking about workforce development and how we're helping to provide the workforce of the future. And finally, I'd like

to talk about the whole continuum in the development of, you know, of these technologies from the basic sciences to engineering to commercialization.

So let me start with the research landscape. In the United States, there were priorities established that really the focus is leadership and industries of the future. And those industries are, as you might expect, artificial intelligence, quantum information science and computing, advanced manufacturing, and, of course, advanced communications networks and autonomy. And this is where the 5G strategy and the national spectrum R&D strategy falls into play. And in from this, they're prioritized to develop R&D funding sources that will lower the barriers for spectrum 5G and also autonomous vehicles fitting all into that.

The U.S. government then, with a priority of 5G and spectrum, has put into place a number of different efforts already. The Department of Defense has a 5G program installing 5G testbeds on military bases to hasten DoD adoption of 5G technology, enhance 5G, and invest in next G.

NSF, another funding agency, the National Science Foundation in 2020 initiated two new spectrum programs, the first, Spectrum and Wireless Innovation enabled by Future Technologies or SWIFT. A key aspect of this program solicitation is its focus on effective spectrum utilization and/or coexistence techniques, especially with passive uses, which have received less attention from researchers.

The second program is the Spectrum Innovation Initiative, the National Center for Wireless Spectrum Research. The focus of a Spectrum Research SII Center, which is what these are called, may go beyond 5G IoT and other existing or forthcoming systems and technologies and chart out a trajectory to ensure United States leadership and future wireless technologies, systems and applications in science and engineering through the efficient use and sharing of radio spectrum.

So now looking at, with those programs and framing that, and looking at what we're doing at University of Colorado, and our efforts spanned a broad set of research that I'd like to just briefly highlight today given our time constraints.

So let me start with antenna technology. The CU Antenna Research Group led by Dejan Filipovic is making significant contributions towards frequency-independent ultra wideband antennas, antenna arrays, and simultaneous transmit and receive antennas. The antenna research group works across the 5G electromagnetic spectrum from standard cellular frequencies up into millimeter wave.

The RF engineering group, the microwave and RF research group, which is led by Zoya Popovic, the Lockheed Martin Endowed Chair of RF engineering. Her team focuses on microwave and millimeter wave circuits and antennae but even reaches into terahertz frequency; her area search is ongoing work in high efficiency power amplifiers for communications, among other applications.

As we talk about the basics of the building blocks to create these kinds of 5G systems, we couldn't—the University of Colorado has a really strong strength in position, navigation and timing or PNT. This connects to our aerospace department in the strengths that we have in aerospace is very—our aerospace department is very renowned for the PNT work that's been done. For example, the Satellite Navigation and Sensing Laboratory, led by Jade Morton, deploys and maintains a global network of Global Navigation Satellite Systems, receivers, and RF sensors. The network provides continuous real time monitoring and space weather and environmental propagation effects.

So with our strengths in aerospace, I would be remiss to not also talk about part of the generation of this particular theme for ISART, and that's policy. The Silicon Flatirons Center at CU has a spectrum policy initiative led by Dale Hatfield and Pierre de Vries that seeks to inform and influence the national debate about events on spectrum security. This fall's spectrum conference will be on evidence-based spectrum policy.

And finally, the last example I'd like to give from CU is wireless security. This year's ISART is about zero trust. I should mention the recent work by a team led by Dirk Grunwald, which demonstrated a practical spoofing attack on the Presidential Alert system. Using commercially available hardware and open source software. Needless to say, after demonstrating the practicality of the attack, the team has been funded to develop defenses. So that gives an overview of what it is we're doing on the research side, just touching a few key things.

Now I'd like to talk briefly about workforce development. That's a really important part of what we do as an educational institution. Any of the research that we're doing or the courses that we teach engage students in really preparing them for the workforce, whether it's at a national lab, NTIA, or in industry, or starting something on their own. And so, we have a significant amount of effort going on through, tied to the research that we're doing.

There are several approaches that we're taking. We have outreach to local and national industry partners to determine the kind of training needed so that we really align it with what the needs are in the workforce. Second, we were developing more interdisciplinary programs to adjust system level challenges. It's easy to be in the component levels, siloed areas that we work in, but it's really systems that are going to solve the problems of the future. And third, we're committed to inclusiveness and diversity, as demonstrated by our BOLD center, which Is Broadening Opportunities through Leadership and Diversity, which focuses on bringing underrepresented populations into industry.

Finally, I'd like to talk a little bit about support for fundamental sciences to engineering to commercialization. It isn't enough just to study technologies. We need to also engineer them and pursue pathways to commercialization, and then accelerate the incubation of these technologies. We need to partner nationally, internationally, and regionally and think about how we do raise all of the boats up. As a major research university, we can help facilitate bringing together all of the parties to create a playground that is neutral.

And that's the role that, at University of Colorado Boulder, we really work to partner with our industry partners, with our national lab partners and really helped to accelerate these new technologies as they're developed. Our goal is to foster economic development through our role as an enabler. So with that, I want to thank all of you for being here. And I'll turn it back over to Sheryl.

### 1.3.5 Opening Discussion: Q&A

GENCO: Thank you, Terri. You make me feel like I almost want to go back to school. So, very exciting stuff over there at CU. We only have about five minutes. We had some questions for our roundtable participants. Maybe what we could do is try to shorten it up for your responses and let's try the first question. Why is your organization important to 5G? Doug, why don't you take that first and we'll go in the same order as …

KINKOPH: Sure. That's fine. Thanks, Sheryl. You know, as the principal advisor to the president and the administration on telecom and technology issues, NTIA plays a number of key roles. We work often in collaboration with our partners across federal government, and with other stakeholders, including state and local governments. And of course, as a bureau in the Department of Commerce, NTIA is keenly focused on advancing U.S. economic activity, globally competitiveness, you know, and 5G will drive growth across many sectors, create jobs, and improve lives for the Americas. But NTIA spectrum management responsibilities are critical to 5G and beyond. And obviously, our spectrum powers 5G communications, the air waves are heavily congested, and we need to find a way to use spectrum efficiently and effectively as possible so that we have it available for 5G and other critical uses. And, you know, our ITS research mission is, you know, to advance telcom, inform our stakeholders, and investigate challenges. When our unique experience that they have an RF and radar is combined with 5G and beyond technologies, ITS has a unique capability for our country. So I think NTIA, just from a spectrum and ITS Boulder labs standpoint, and then you throw that on to our expertise in like broadband USA where we actually work directly with communities on advancing networks, which will help with the 5G networks throughout rural America, and our work on—in the federal government side on to helping lead the American broadband initiative with the White House. I think we're well-positioned to play an important role in advancing 5G for the American public. Back to you, Sheryl.

GENCO: Thank you. Walt, why don't you take the same question?

COPAN: Sure. Similarly, the role of the NIST director is to serve as a principal adviser to the president on standards and technology matters. And so on issues related to 5G and spectrum utilization, we are a partner to NTIA, and to the other elements of the federal government, pushing the boundaries of measurement science to make new spectrum accessible and ensuring a science-based approach in 5G standards. NIST also has leadership in the development of trustworthy AI machine learning, which has led to breakthroughs and spectrum sharing strategies for 5G and that links to the standardization efforts that NIST leads for the nation in trustworthy artificial intelligence. Lastly, I would say that the collaboration on large scale

research programs, such as the role of NASCTN that I mentioned previously allows collaboration to go forward on an accelerated timetable and whose research outputs informs policy decisions. And so it's an important part of the national infrastructure with regard to effective standards for the future.

GENCO: Thank you, Walt. Terri, would you like to add anything? We have a few more minutes.

FIEZ: Yeah. I'll just make a quick, a couple quick comments. You know, when I think of the university, I think of it as been—being the ultimate playground. We can try out ideas and we can actually fail. And the best way to be innovative is have an opportunity to be able to try things that aren't going to work. And that's where you get solutions for the future. So I see the university doing that on the technical side, as well as on the policy side, and really helping to inform our partners, NTIA, NIST, industry, and other national labs. And then, of course, I already mentioned the workforce. You know, we've got to continue to think about the workforce of the future. They've got a different skill set than many of our more senior workforce. They can work on the AI machine learning. They have computing skills that are advanced. They have a different way of working. They're used to working in a different kind of environment, like all of us have moved to now being online. So, you know, it's an exciting time. And I think all of us being able to partner to address this is really how we're going to move forward.

GENCO: Thank you, Terri. I agree. Collaborations and technical achievements have to go hand in hand. We have exactly three minutes. So why don't you each take one minute and try to help us understand what you feel your most impactful objective or the role of your organization, the most impactful role of your organization le? Doug?

KINKOPH: OK. So that's like asking me which of my children is my favorite. Oh, let me l—but—boiling it down, it's hard not to stop at the critical role of NTIA spectrum management responsibilities and the team there. And that, of course, it's supported by research at ITS and the advance communication, electromagnetics propagation modeling, and RF, etcetera, and it goes on and on. But, you know, we're entrusted to and do manage the federal government's use of the spectrum, and it's the one thing we do that's closest, probably, to being a regulator, during managing the radio spectrum with the FCC, which manages the non-federal use. I think it's difficult for people to really appreciate how diverse federal government uses of spectrum are, and ensuring that we have the most capable military in the world, to space exploration, weather forecasting, controlling the nation's airspace, while also leading the world in 5G and the industry side. So I think that is a huge load that NTIA carries, and one that we take great pride in taking on. So, that keep this short, I'll just turn it back over to you, but I would say spectrum management role.

GENCO: Thank you, Doug.

KINKOPH: Thank you.

GENCO: Thank you. Walt, how about you?

COPAN: Yeah, very briefly. People know NIST for its wide portfolio of science and technology development, that touches upon all market sectors, all industries and ranges from foundational research in our labs to manufacturing deployment. And is known as industry's national lab as a trusted partner globally, together with a strong focus in cybersecurity. So it's that broad interdisciplinary focus from the laboratory to the marketplace that characterizes NIST and our role for the future.

GENCO: Thank you. Terri?

FIEZ: Yeah. Really quickly, I think one of the things in terms of the impactful objective is identifying and filling the gaps of shortages. So as we talk about RF engineering, for example, there are major shortages in the workforce. And through the research, we really can partner with the, again, the industry and our federal labs to fill the gaps to basically make sure that we have the workforce that we need in these areas that are very difficult to hire in. And then finally, a major part of what we do is become a convener, and also an entity that can look far out into the future to help create the vision of what the future could look like.

GENCO: Thank you, Terri. And I agree RF engineering is very difficult to find folks who are in that field, and I'm very proud of what you're doing over at CU. Thank you.

Well, with that, I think this session has come to a close and I'd like to introduce Dr. Joe Evans. We enjoy working closely with Dr. Evans and his team on DoD's 5G deployments, that are captivating the attention of industry as DoD embarks on a number of important 5G projects throughout the United States. So with that, I'm going to ask Akeem if Dr. Evans is ready.

## 1.4 Keynote: Joe Evans

EVANS: Can you hear me?

GENCO: Now I can. Nice to see again, Joe. Take it away.

EVANS: Thanks. And I can see the slides. That's great, I hope everyone can see those. And so I'm Joe Evans. I'm the Principal Director for 5G with the Department of Defense. We are, you know, currently engaging in a number of activities across the Department of Defense and working with our government partners, as Sheryl said, and so I hope through this presentation to convey, you know, what we're doing, and specifically a few things on the topics of the ISART 2020 Program, 5G Spectrum and Zero Trust. So let's go to slide two. And that will provide a little bit of context.

So why do we care? Well, we care about 5G because it's transformational and not just new radios and faster cell phones and kind of a slightly better 4G. It's really designed to be ubiquitous connectivity, the fabric to, you know, connect not just to human to human, but machine to machine and human to machine. And so it's this connectivity fabric that really makes 5G exciting in terms of what it's going to offer in terms of services, but also in terms of how it changes the network architecture and how you have to think about the network. And so, one of the—that's some of the good things about 5G.

On the other hand, we also have to acknowledge that there's no such thing as a secure system. So we have to operate on networks in which we have zero or little trust, and be able to operate through adversary impairments and impediments to our ability to use those networks. And because 5G is such a re-architecting of the network, it presents a lot of attack surface that just didn't exist on previous—in previous instantiations of cellular technology. So we have to focus on those types of things going to the zero trust philosophy, as well as all the good things that we can get for DoD by using that technology.

One of the key things that we're doing is partnering with industry to understand and influence 5G. That has to be the fundamental aspect of our approach, because industry is driving 5G. The DoD is relatively minor player in an industry that's going to be, you know, spending $355 billion on capital expenditures alone to deploy 5G in the United States. So that's a massive investment. And, you know, the DoD, you know, just doesn't do things at that scale in networking communications.

One of the numbers, other numbers I like to cite is Samsung, one company, in 2018, one year, their R&D budget alone as $16.7 billion. There's never been a DoD networking and communications program of that scale. You know, we are, you know, a minor player in this industry. And we are getting dragged along in terms of networking and communications capabilities by the commercial world. Our users, the, you know, soldiers, airmen, marines, sailors are all expecting to be able to use capabilities like you get with 5G. And so DoD needs to enable those capabilities, but they need to enable it by building upon the massive investments that the commercial world is making. And this is critically important for the military.

So if we go to slide three, this gives us little bit of an overview of the overall DoD 5G strategy. And I'll focus in on a couple of these items in the remainder of the talk, really, mostly the top two here, but I wanted to give a sense of all of the things that are going on throughout DoD on—in terms of technology development, security and operating through vulnerabilities, standards and policies, as well as partner engagements. And it's—yeah, I'd say a pretty broad-based strategy with many participants throughout the department.

So, in terms of technology developments, probably the thing that's been most obvious to the outside world has been hosting 5G demonstrations, prototyping experimentation on networks and applications enhancements. But we've also been looking at RF technology, spectrum sharing, open architectures. All of those are wrapped together into some of our prototyping and experimentation as activities. And in the future, we plan to work on workforce development as well because we need to make sure that DoD has the right folks to be able to utilize this technology and the right type of folks that can also, you know, work on U.S. military bases and so forth.

The—in terms of assessing, mitigating, and operating through vulnerabilities, we're certainly working with our partners throughout the U.S. government throughout the both DoD and the intelligence community on looking at threats and how to minimize those threats, and then also how to use 5G globally despite adversary capabilities. So we believe this cybersecurity zero trust piece of the program is very, very important.

We've also been working across the interagency and throughout DoD on standards. We have partnered certainly with our colleagues at NTIA on this and DoD CIO within the Office of Secretary of Defense. DoD CIO is really our lead organization on standards working, closely with them to work across interagency.

DoD CIO is also very involved in advanced spectrum management. We believe that we need to modernize policies to be more dynamic as we develop those—further develop those technologies as part of this program. In terms of engaging with partners, obviously, national engagement, that sort of thing, but we think it's also important to engage with our international allies and partners on everything from supply chain and assessments, as well as we're starting to look at how we work with allies and partners on particular experiments.

And just to wrap this up, industry engagement, as I mentioned before, is kind of a fundamental aspect of this program. And we're working with industry through several mechanisms, both—well, a couple of consortia in particular, both the national spectrum consortium, the NSC, as well as, IWRP, the Information Warfare Research for Program, we think that they can provide kind of complimentary consortia capabilities and also, you know, wider variety of contracting options to work with our industry partners.

The next slide, slide four, starts to ... Next slide, slide four talks about the—a little bit about the 5G prototyping and experimentation aspect of the program. So this is kind of taking the first couple of areas on that previous slide and drilling down a little further into those. And I'm, gonna, you know, wrap even further down into those as we go forward here. So in terms of—sorry, can we go back on slide four, we have three thrust areas as part of the overall program.

The first is, is what we call Accelerate, which is hastening DoDs use of 5G technologies. And that's what you see throughout the, you know, initial like, throughout the initial release of solicitations. The second area called Operate Through is focusing on ensuring that we can operate wherever and whenever we deploy because DoD does go quite a few places around the world. And this is a mix of dynamic spectrum utilization, dynamic spectrum sharing as well as this idea zero trust to be able to operate over, you know, networks in which we don't necessarily have a tremendous amount of trust. And then this also includes perhaps DoDs specific enhancements to commercial technology to fill gaps where we need to.

The last area is Innovate and that is enhancing 5G technology and investing in future 6G, 7G and so forth technologies because this will be a continual race. There's no finish line. In terms of the, you know, scale of these programs and current activities on the first two areas there, Accelerate and Operate Through are, you know, 6.4 research in DoD parlance, so pretty high TRL, advanced development and prototyping, and those are meant to be—those areas are, you know, meant to be providing prototypes that can be then be used in actual DoD systems at the end. That, the scale of that effort is, you know, on the order of about in the President's FY21 budget that's on the order of about $449 million for FY21.

The last area, Innovate, is essentially 6.2 research so that we can reach out to a wider range of those that have more basic research level, universities, for example, that is about $35 million in the FY21 budget request. So that gives you a sense of scale of those activities.

In terms of—can we go back one slide, to slide four again, the first area accelerates, that is being executed through the Tranche 1, 1.5, and Tranche 2 experiments. And those solicitations are on the street. Operate Through, we are anticipating solicitations in that area. Some of those will be unclassified, some, perhaps. classified, those will be in early FY21. And the Innovate area will also be solicitations in early FY21.

So, the next slide now, slide five, talks specifically about some of the ongoing solicitations and where they are and the experiments that were just standing up. So Tranche 1 consists of four sites with essentially three to four types of experiments. Hill Air Force Base is focusing on dynamic spectrum sharing, Joint Base Lewis-McChord, that's focusing on augmented reality, virtual reality for distributed ground combat training, scaling up to larger unit sizes up to brigade level and then Naval Base San Diego and Marine Corps Logistics Base Albany are focusing on smart warehousing. At Naval Base San Diego, it's really transshipment: putting things in pallets to ship to ships at sea. And then at Albany, really focusing on vehicular maintenance and warehousing, things like MRAPs and trucks, you know, being warehouses. So, those are a couple of the—a few of the initial Tranche 1 experiments. Those experiments are in the middle of source selection, and we're hoping for announcements of the awards on that within, you know, kind of the next few weeks, we hope.

In Tranche 1.5, kind of an intermediate step of working with the folks at Nellis Air Force Base on a distributed combined air operations center concept, basically distributing command and control functions that normally would sit in a, you know, big single big building, distributing those in multiple locations to make them more survivable. We're also hoping to be able to announce the awardees there, probably next month to six weeks.

Next slide, slide six, talks about some of the specific, one of the specific—oop, slides six. Next slide. Yup. There we go. OK. The slide six talks about one of the specific experiments and this is the AR VR work at Joint Base Lewis-McChord in Washington. And this is using virtual reality type or augmented reality types of headsets in order to perform, you know, distributed combat training and actually in the end actually support operations in the field as well using that AR capability or AR overlays in those goggles. The experiment is being performed at both JBLM, as well as, the Yakima Training Center, which is out in more central Washington across the mountains, where you can do larger scale maneuvers, again, because we want to reach this goal of brigade-size deployments.

So the next slide dives into the warehouse activities at Naval Base San Diego, so slide seven and that said – and Naval Base San Diego really focusing on that kind of, I think they call it, retail warehousing, you know, small pallets being collected for transshipment to other locations and so we're focusing on that at Naval Base San Diego, setting up a warehouse in order to start looking at integration with maybe logistics systems and automation of those types of warehouse functions.

The next slide, slide eight, talks a little bit about the Marine Corps Logistics Base Albany smart warehouse, which again, is focused more on vehicular warehousing, large vehicles and large warehouses where there's also a maintenance aspect associated with the warehouse because you have to pass, you know, keep track of the health of those vehicles, the oil leaks, and all those sorts of things that come with maintenance of the large combat and logistics types of vehicles.

The next slide, slide nine talks about the work at Hill Air Force Base and we consider that one of our, you know, most interesting experiments because it is really focused on understanding how radar systems and 5G can work together, particularly in the mid band spectrum that is of incredible interest right now throughout the nation in order to make 5G deployments more widespread and more economical. And so, we are focusing on basically testing, evaluating the impact of 5G on the airborne radar, as well as, the impact of the radar on the 5G system. And so, we're building and deploying mobile infrastructure at Hill Air Force Base, as well as, the Utah Test and Training Range. So using cells on wheels, or as they're called now, cells on light trucks (COLTS) to implement the 5G, to deploy the 5G network so that we can then instrument it and understand what is happening in the interaction between these different waveforms in that those particular bands.

So you can see just to briefly recap Tranche 1, you can see that, obviously, the dynamic spectrum access has, you know, direct commercial interest in being able to use that spectrum. But the other thing we'd like to emphasize is that the other experiments have a dual use aspect. And so we're also providing, you know, an opportunity for industry to come and use these bases as a place to experiment, at a relatively low risk—the DoD in this case is a friendly customer, and will help with permitting and access to the bases—so offer an opportunity to do some dual use experimentation. In other words, in the smart warehouse case, there are direct analogs in the commercial world for smart warehouses, and there's a direct analog for AR/VR, obviously, gaming and things like that, as well as support of maintenance and so forth. There are direct analogs between the DoD use cases, those applications at the high end of the value chain, and what is, you know, being explored in industry. This is an opportunity for industry to experiment in a friendly environment and hopefully move this technology forward for both the benefit of DoD and our U.S. industries.

The next slide, slide 10, talks a little bit about the Nellis Air Force Base experiment, and really focuses in on, you know, a very war fighter-oriented project. And in this case, its distributing command and control functions throughout an operating area in order to reduce, you know susceptibility to targeting and attack, and so disaggregating those command and control functions to multiple locations. So, you know, as with many of our different testbeds and experiments, really has three parts. One is build a localized 5G network that can be distributed, develop the command and control capabilities, and then do network enhancements to kind of fill the gaps to support the military operations and as needed.

Slide 11 dives a little bit deeper into the Nellis Air Force Base activity. And talks a little bit about the phases and gives you a sense of where we're going with this. And so, in phase one, it's really, you know, pull the primary operation center pieces apart and be able to put them in multiple

locations interconnected with the 5G network. The second part is, well, can you then speed up the cycle so that you can make these functions nomadic and move those functions around in trucks or whatever? And then in phase three, can you make it actually, you know, truly mobile so you can perform these functions on the move, make it very difficult to target the command and control capability. So that's where we're going with the Nellis experiment, like I say, a very war fighter focused activity in that particular case.

Slide 12, then talks a bit more about what we're doing in terms of the next Tranche of bases that we've announced, Tranche 2. So that's slide 12, I believe. And at—in this particular case, we've named seven different locations for this experiment—moderator, slide 12—and the Tranche 2 is really a pretty broad-based set of experiments and locations. And so, at one of these locations, we're doing essentially ship-wide and pier-side connectivity, that's with the Navy and at Naval Station, Norfolk.

The idea there is you know, communications within a vessel using 5G technologies. Can you reduce poles and bulkheads and provide better conductivity for sensors moving around the ship and personnel moving around the ship, and also can you provide connectivity from the ship to the pier-side as you're arrive? You can think of dual uses here as well in the logistics industry where you may be monitoring containers on a cargo ship or at pier-side, a cruise ship arrives, and you want to be able to quickly download information from all those passengers to the pier-side. So you can think of dual uses for many, many of these applications.

Enhancing mission aircraft readiness, that's a Joint Base Pearl Harbor-Hickam with all the services most likely, including Marine Corps Base Hawaii across the mountains with that. And that's really looking at how you download data from the aircraft when they land, upload information for missions, and do maintenance. One of the things that we discovered with commercial partners, Boeing, Airbus and so forth is that they have set similar types of problems. They want to do predictive maintenance, collect data when an aircraft lands, pull the data off and understand, you know, if there are any issues before that aircraft turns around and 30 minutes at the gate and leaves. And so, we need that, you know, high bandwidth capability in order to quickly get that data on and off the aircraft as well as support, you know, high levels of maintenance where you might want to have some sort of augmented reality display showing schematics or so forth or the ability to reach back.

Which is also, the topic of the next experiment, which is AR support for medical training and telemedicine. And this is at Joint Base San Diego with the Army and the Air Force. And this is looking at both medical training, you know, sort of the see one, do one, teach one type of thing, but with augmented reality support so that multiple individuals can get a, you know, kind of surgeon's eye view of what's happening, as well as the ability to reach back with telemedicine, so that say, a medic in the field can reach back to a doctor or specialist in order to provide better care at the kind of tactical edge.

The next experiment is wireless connectivity for tactical operation centers and combat operations centers, using the different terms for the Army and Marine Corps. And the Army will be doing this at the National Training Center at Fort Irwin in California, as well as, the unit being

trained will come from Fort Hood, Texas. The Marine Corps will do this at Camp Pendleton. And really what this is, is we're replacing all the wires that run around a tactical operation center, seeing how much of that you can make wireless, but add multiple security levels.

The next experiment is a pretty exciting one that really spans the nation. This involves Joint Base San Antonio as kind of the hub or center of gravity of the experiment, but also multiple remote locations, basically all of the sites that we're looking at, and this is kind of under the auspices of the Air Force, but really will involve all the services in the end. And it's really looking at 5G core, how—yeah—how secure can we make it? So doing security evaluations, but just as importantly, understanding interoperability between 5G core instantiations, different implementations from different vendors. We are working with partners at DARPA, as well as NIWC-PAC on this particular experiment.

The last Tranche 2 experiment I'll mention is bidirectional spectrum sharing. And that's basically the ability to share spectrum between DoD applications, either DoD 5G or DoD some other wave form and commercial 5G. And really more of an emphasis here on communications, maybe than at Hill Air Force Base, where we're doing, you know, the high power radars. But a variety of waveforms at Tinker, as well as, this will be Air Force and focusing really on emergency national security types of instances, trying to do bidirectional spectrum sharing where both entities are co-primary in a band and how you might share that spectrum, you know, rather than kind of the model that we've used for CBRS and some of these other bands where there's, you know, a clear primary and a clear secondary, and we get through kind of a co-primary type of relationship, and really primarily be exercised and—of national security.

So, I'm going to change topics a little bit. Why don't we go to slide 13, which talks a little bit about our Operate Through activities. And so what this is doing is trying to lay out a way to think about DoDs security needs as we move forward. And so many, you know—DoD use cases have security requirements similar to commercial use cases. And so if you look at this graph, you know, that lower left-hand corner, kind of is where commercial systems live on. And, you know, they obviously have quite stringent security needs, but maybe they don't have, you know, nation state adversaries to deal with all the time, as kind of the bread and butter. And so, you know, DoD needs to be protected against more sophisticated national security threats, and also needs to assure resilient operations in multiple threat environments. So that's what this graph is trying to capture is that we believe that DoD can used commercial systems throughout a range of situations, you know, different threat environments, and also different threats sophistication. It won't answer all of our questions in terms of, or all of our needs in terms of what DoD must have in order to operate, you know, everywhere every time, but we believe that we can cover down a significant part of the space through our investigations as part of the Operate Through activities.

And so our kind of direction forward on that, and as highlighted by the topic of this event, is that, you know, we really think zero trust is very important and not just kind of zero trust research is what we're looking for, what we're really looking for how we create the zero trust applications, frameworks, systems in order to start deploying those, and use those for secure operations in many of these different environments with different levels of threat sophistication.

We, you know, believe that we can—we need to get away from perimeter defenses and, you know, really move towards the zero trust aspects where we have layered security with different types—with, you know, authentication and authorization down to the finest grain, you know, encryption so forth, really embedded throughout the protocol stack from, you know, the ground off and, you know, again, not believe that we can build a perimeter and everything will be OK within. So that is, you know, one of the key messages we'd like to get across is that, we want to not just research that, do that in a little way, we want to move towards how we create the DoD applicable infrastructure, as well as applications that use the zero trust philosophy.

We don't think that that's just the cyber side, by the way. We also believe that that we need to, you know, carefully understand what, you know, our spectrum needs will be and how we will work in spectrum in unfriendly environments, as well as in a friendly environment.

So the next slide, talks a little bit about some of the expected outcomes from the program. And I won't go through all of these, but I just want to give you a sense of where we think we're going and where we, you know—the results we hope to get. So we hope to be able to, you know, certainly hasten DoD's use of 5G by, you know, coming up with expedited authorizations to operate, bills of materials, basically make it easier to deploy more quickly and at lower cost, on U.S. military sites. Make DoD operations more efficient by network autonomy, things like that. And then finally, improved DoD operations, rapid deployment, use of 5G systems both, use—use of the systems, as well as, use of the piece parts, we believe, well, the antenna systems, things like that may be deployable as well. So we need to explore the range of possibilities there. In terms of Operate Through, well, you know, counter adversary attempts to deny access to the spectrum, as well as network, so that we can do this, have this ability to go anywhere, anytime and use 5G. And then finally Innovate, you know, start to produce those or help produce those next G technologies that will make us competitive as a nation in our 6G, 7G and beyond.

So the last slide, just, you know it's kind of a summary slide that, you know—this is very important for DoD. It's a major initiative within DoD that spans the entire department. We are working, you know, with our partners within DoD as well as throughout the interagency to both, you know, use 5G, as well as, to help secure the 5G ecosystem. We also acknowledge that we need to be doing this for 5G but we also need to make sure that 6G and 7G and beyond are on our roadmap as well. And, you know, it is a fundamental technology that DoD needs to leverage and work with 5G—the U.S. 5G industry to make sure that the U.S. is competitive and able to use these technologies in the future. And with that, I will turn it over for questions. Thanks.

### 1.4.1 Keynote Q&A

GENCO: Thanks, Joe. We have a couple questions here. So the first one is, Dr. Evans, how scalable do you think the sharing solution between 5G and radar will be? For example, will it scale to include DoD comm systems? Or, do you envision different sharing techniques between 5G and other systems, depending on the coexistence scenario?

EVANS: On that, that's a really interesting question. And in the part, it's answered by our additional work that we're going to be doing at Tinker Air Force Base, because that's really more focused on communication spectrum sharing. I view the radar spectrum sharing problem to be, you know, one of the hardest for spectrum sharing because of the vast power differences, first of all, between the systems. Most of the—many of the systems DoD uses in terms of radars in these bands are pretty darn high powered, but also, in terms of the sensitivity of the radars to interference, essentially. And so, we, you know, certainly, we need to work on that problem in general for radars, but we're hoping that, you know, that the communications problem might be—I won't say a little simpler, but at least it's a—you know, the physics of it won't be quite so daunting.

GENCO: Very good. I have another question. Does it cause you any concern that the DoD and the commercial sector are putting so many of their communication eggs in one 5G basket? What are the drawbacks of depending in so much on a single standard or technology?

EVANS: That's a very fair question. And the, you know—I think the, you know, DoD approaches most comm systems, we have an acronym by the name PACE, the Primary, Alternate, Contingency, and Emergency. And so, rarely is there one single solution that is viewed as the be all end all for DoD. One of the things I'm trying to convey with that graph of, you know, threat sophistication and threat environment is that we really think that there's a range there and we need to architect the network solutions, 5G or otherwise, to fit the cases in which we operate. And so, if we're talking about, you know, 5G operations in—or operations in the U.S., 5G may be completely applicable to a smart warehouse, something like that. It may also be, you know, applicable to a smart warehouse in a deployed location depending on what's the adversary. And so if you, you know, went back to like, our deployments in Iraq or Afghanistan, there's a pretty wide use of, essentially commercial technologies at various levels within that environment and not necessarily for cellular, but for other types of communications and so forth. And so, you know, not everything has to be, you know, the best tactical radio that you can ever build because DoD doesn't operate in, you know, a high threat tactical environment all the time everywhere. A lot of our operations are fairly boring. And, you know, in a, you know, base in the U.S. or in, you know, an allied country, and we don't need and it's not cost effective for the U.S. taxpayer to pay for, you know, the most extreme systems that are needed in emergency situations for every single communications. We need to architect appropriately to the threat environment.

GENCO: Very good. Let's see here, are there any roadmaps or specific requirements for the zero trust for 5G and beyond for DoD, government agencies, or for the industry to adopt?

EVANS: We have not developed what I would call a roadmap for zero trust yet. We are in the process of working with our partners within, you know, DoD CIO in particular, but also as part of the 5G initiative in, you know, putting together some plans for that. We, as I mentioned earlier, will be standing up the Operate Through area in early 2021, bringing on a leader in that area to start putting together solicitations for release focusing on Operate Through and that will include zero trust architectural work. What we hope to do is to prototype systems based on that type of architecture that we can then move towards, you know, wider deployment within DoD. I would

expect to see a roadmap for that as we move forward in the next year or so. But, you know, that's still a work in progress to be fair.

GENCO: That's—that is very fair. In leveraging RF technology, where is the United States millimeter wave expertise and technology best applied to meet the goals at the DoD 5G office? Thank you.

EVANS: Thanks. That's really good question. And so we're very excited about the use of millimeter wave. The U.S. has some pretty significant advantages in that area. We've worked millimeter wave systems for many, many, many years both at kind of the lower end, low power, but also, you know, the high power, you know, mobile airborne systems, I mean, we really have quite a bit of expertise in that area. We think that that—some of it may be for kind of traditionally uses like backhaul and that type of capability. But we're also excited about the idea of using it in places where we don't want such an obvious RF signature. And so, we think that the lack of good propagation of millimeter wave that at lower powers is actually an advantage in many DoD scenarios. So we would like to be able to use it in order to provide high bandwidth services, but not be radiating, quite so obviously, and thereby become a target. So, we are definitely interested in that kind of different view of the use of millimeter wave in 5G. We do think that there are some early examples that we've seen from industry, U.S. industry of, you know, exciting millimeter wave beamforming capabilities, things like that that fit wonderfully with our needs. And so, we hope to see that as part of several of our early tranches of projects.

GENCO: Excellent. At this time, does the DOD envisage working with the allies on 5G? That's Pierre de Vries, everyone.

EVANS: Yes, you're right. Yeah. We certainly do. And, you know, I think both the DoD, 5G strategy as well as the National Strategy to Secure 5G, both call out a, you know, an interest in working closely with our allies and partner nations. And yes, we certainly anticipate doing that. We are, again, just in the process of putting some of that together. But I think probably over the next, you know, half year, we'll be kicking off some opportunities there. We certainly had early conversations, and we see tremendous value from that sort of interaction.

GENCO: The DoD announced the 3450-3550 spectrum would be redeployed to commercial use. What use conditions do you see for this transition? And do you know the timeframes?

EVANS: I've—Off the top of my head, I don't actually know the timeframes. I haven't kept up with the latest auction announcements and so forth. But we see a trend where, you know, we have to do increased spectrum sharing in general, not just in that band, but in other bands. And what we're trying to do with our 5G initiatives is—in spectrum sharing is, you know, exercise some of those use cases so that we can offer technology solutions to the policymakers so that there are, you know, different ways we can move forward to start sharing more of that spectrum. And we think that benefits not just U.S. industry, just flat out in use of the spectrum, but we think that it benefits, you know, DoD and in terms of being more agile in general, but also maybe even offers an opportunity for U.S. allies and partners and U.S. domestic industries to develop and deploy technologies that are, you know, leading edge and useful around the world.

So, that's really part of the reason for our emphasis on this dynamic spectrum sharing and several of the aspects.

GENCO: Very good. Can you talk a bit about spectrum deconflicting, such as on ships and aircraft and other anti-self jamming needs within the DoD and where this is happening?

EVANS: Yes, we need that. The—so certainly, those are hard problems. And I'm not sure I have a general solution or a general comment on that other than as part of some of our individual projects we'll be looking at those problems. So certainly, you know, some of the things like at Hill Air Force Base looking at airborne platforms and so forth but, you know, obviously with the ship-wide and pier-side connectivity projects with the Navy very, very tough electromagnetic environment in those cases. One of the things that we're hoping is that with the use of some of these other bands, millimeter wave bands and so forth, we might be able to make—so make some progress by essentially going where there aren't a lot of systems already. That's a hypothesis. We'll see what we can do in the awful environment of a metallic ship but, you know, that—that's what we're looking forward to.

GENCO: Very good. I don't seem to have another question for you, Joe. So I want to thank you from NTIA and the ITS and look forward to meeting you someday in person. And I think now, if any—everyone wanted to go to their breakout rooms, some of the speakers will be available. I believe that Doug Kinkoph got called away. He may be in his breakout room a little bit later on. So again, Joe, thank you for your time in support of ISART and with our co-hosts, we will extend you invitation to speak to us again sometime.

EVANS: That'd be great. Thank you very much really appreciate it. Thank you.

GENCO: All right, so long.

EVANS: Bye-bye.

# 2. DAY 2: AUGUST 11, 2020

## 2.1 Melissa Midzor: Introduction of Opening Panel

MIDZOR: Welcome everyone to day two of ISART. Yesterday we set the baseline with a series of tutorials on the current state of 5G, a fireside chat giving the unique perspectives and efforts being undertaken by NIST, NTIA, and CU Boulder. Our keynote speaker, Dr. Joe Evans, shared the latest efforts spearheading this push to operate in a zero trust network environment. And although we were virtual, there were numerous opportunities for you, the attendees, to interact one-on-one with our speakers during live Q&A and in the breakout rooms.

This morning we'll feature our framing panel of experts with experience in government, industry and academia diving deep into what zero trust means with the spectrum world and the known risks that exist today at that intersection between 5G new radio and zero trust networks.

The technical core of the program is contained in the next four panels over the next two days, which will examine 5G networks from the perspective of ways to design the 5G radio layer for resilient services. That will be this afternoon. Then on Wednesday, we will cover our second technical panel on how to implement secure and resilient technical solutions during deployment. And third, the how to ensure resiliency with a network operations within handling the spectrum. Then on Thursday, we will cover the fourth topic on monitoring and data collection and how that can and should provide valuable input and feedback into the design, deployment and operations, which we discussed the priorities to improve the resiliency of the network. And then finally, we will have a wrap-up panel on Thursday afternoon, which features polymaths, who will help us draw new insights and connections across all those different panels and our technical speakers and identify potential new research areas and hopefully add to the history of ISART triggering important out-of-the-box thinking innovative ideas and novel solutions. Also with several of the panels, we'll be privy to some deep dives into some technical talks, so we can get a better hands on feel for the boots on the ground type effort each of those areas.

But before we start the day, just a few logistics to remember for not just today but the rest of the week. Our virtual ISART 2020 is structured in two, two-hour blocks each day. The organizing committee has worked hard to find ways to incorporate tools for real time interaction amongst the panelists with in-depth planetary talks, highly interactive Q&A sessions, and opportunities for networking conversations in our breakout room. Please feel free to ask questions during online, during the presentations with panels. And remember to spell out in your acronyms. If you look over on the right, there's a Q&A button. Please look at the questions already listed and vote if you would like to hear more about that particular question. The panel moderators will endeavor to pull questions based on those of highest interest. We will also take some of those unanswered questions into the breakout room.

The breakout rooms are the last half hour of each of those two hour blocks, those are reserved for breakout. We hope that these rooms replicate to the extent possible in a virtual environment.

That kind of a personal interaction with the speakers and other participants that had always been a hallmark of ISART. After each panel concludes, the panelists and speakers of each session will exit from this BlueJeans events, and then head over to the BlueJeans meeting platform for those breakout rooms. For those of you who are able to and using our brand new ISART app, all the information and links are needed to find the breakout rooms are in that app. Just go to that session and click on the link. For non-app users, ISART confirmation email sent out Friday has quick links that contains both the link and the phone number for both breakout rooms. For each breakout room, there will be a host from the conference to help you there, if needed. If you run into technical difficulties, please reach out to our conferences service staff listed in the conference email.

Just a quick technical note, the code to access the main sessions, these mean sessions for each BlueJeans events, is the same each day. So if you have a problem with one link, just go to the next comparable link and click on that. We did have that issue yesterday. We do apologize for that glitch and the link to Dr. Evans' keynote, which prevented or delayed some people from accessing the afternoon session. To address that, we will be posting in that one video from yesterday's session as soon as possible, so that those who are affected will be able to view it.

Just remembering that the ISART app will allow you to reach out and connect with each other. By default, the only information people will see on the app is your name and affiliation. So if you're open and interested in chatting with others, networking, exchanging virtual business cards, please remember to go to the app in the app and then add whatever information you're comfortable sharing. I'd like to encourage all of you to use these interactive tools to ask questions, converse with our panelists and presenters in the breakout rooms and connect with other attendees.

Just one quick other regret, we did run into technical difficulties getting the 5G equipment vendors and suppliers involved with ISART this year. We're truly sorry. And we will be sure to have them all in the next year's ISART. So please take advantage of the app and all the opportunities our virtual conference offers.

And with that, we will get underway with our first panel, our framing panel to discuss what zero trust means within the spectrum world today and the known risks that exist. It's my pleasure to introduce the moderator of this panel, Bryan Tramont. He is widely recognized as one of the nation's top Media and Communication lawyers. He served as chief of staff at the FCC under Chairman Michael Powell. And he is now a managing partner at Wilkinson Barker Knauer LLP. There, he leads the strategy and implementation of WBK's communications, media and technology team. I encourage you all to use the app and the program to peruse the complete bio information to learn more about him and all our amazing panelists. And now, I will turn this over to our esteemed moderator, Mr. Tramont.

## 2.2 Opening Panel: Framing Zero Trust Today

### 2.2.1 Bryan Tramont: Panel Introduction

TRAMONT: Thank you, Melissa. It's a pleasure to be with everybody this morning. I'm very excited about the group we have together on this panel. As Melissa alluded to, they bring vast experience in the regulatory government and business sides of spectrum management, both at NTIA, the FCC, among international regulators, DOD. And so, I'm very excited to get their perspective on what framing the zero trust relationship means today vis-à-vis the spectrum in the radio layer in particular. And one of the most important things is recognizing and naming the risk and vulnerabilities in each layer of the network so that we can better do a job of comparative risk assessment both for purposes of making public policy, but also in terms of making investments in our networks and assessing where we go from here from a policy perspective.

So it's my pleasure to introduce our panelists. First up will be Lisa Porter, who's the President of Logic and the former Deputy Undersecretary of Defense for Research and Engineering. Next we'll go to Anna Gomez from Wiley Rein. Then William Webb from the University of Cambridge, and Henning at Columbia, and Charla, formerly of Verizon, and now CSMAC co-chair.

I want to encourage all of you, all 79 attendees out there, to do send in your questions. Otherwise, you'll be subjected to the questions that I have prepared in advance. We'd love to hear what you all were thinking around the country and around the world as you listen in this morning. But the run of show will be each of the panelists will speak for a few minutes about framing this question. And then we will turn it over to questions from you or from me, depending on where we are. So welcome, everyone. We're thrilled to have you here. And I want to turn it over to Lisa first.

### 2.2.2 Lisa Porter

PORTER: Good morning, everyone. So thank you, Bryan, for the intro, and hello to everyone out there in virtual space. I'm going to confess that I'm not really good at this. So you all have to just put up with me and my weird awkward 50 looks at the camera. But anyway, it's really pleasure to be here.

I thought I would start off by framing zero trust a little bit, as Bryan alluded to, and making sure we're all on the same page regarding what does it really mean fundamentally. And I like to point out to folks, that zero trust isn't just about networking, or cyber security or 5G. It's really a fundamental philosophy. It can be applied to any complex system, including things like supply chain management. And there have been a lot of erroneous commentaries I've noticed in the press recently, some of the press, about what zero trust is. As it sort of gained some buzz and people started talking about it, the inevitable occurs and people start kind of going off and talking about stuff they don't know what they're saying. So some of you may have seen zero trust commentary where people say, "Oh, it's really a misnomer. And you know, it really isn't

about zero trust. We have to trust people to get stuff done, and blah, blah, blah." No, it really is what it means. Zero trust is all about recognizing that trust is a vulnerability that can be exploited. So you have to eliminate trust as your goal when you're designing complex systems. That's really what people have to embrace when they embrace the zero trust philosophy.

So when you think about it, if you decide you trust something, then you're basically assigning zero risk to that thing. And once you do that, you've introduced a vulnerability. So pursuing trust is not what you should be doing. And you cannot both ask for a trusted system and say claim that you're pursuing a zero trust approach. Those things are, you know, oil and vinegar or oil and water. So, you got to let that that whole paradigm of pursuing trust go. And the reason I make a really big deal about this is because people are trying to hold on to both. And it's really problematic to do so.

Now, I do want to point out that zero trust is actually not a new concept. People talk about it, and they talk about it as though it was invented in 2010. Or maybe 2004, depending on different literature you read. That's not really true. I mean, zero Trust has been something that is really ingrained, if you will, in the culture of the intelligence community. So anybody who's ever watched a good spy flick kind of knows that. But ironically, back in the mid 2000s, when the intelligence community, the national security community as a whole was really grappling with cybersecurity, they kind of forgot about the fundamental principle that they apply to a lot of other things. And so, at that time, and I was at the director of DARPA at the time, so I kind of can speak to this with some authority.

At that time, a lot of the senior leaders were asking how do we build secure cyber systems? And some of us were speaking up and saying, "No, that's the wrong question, right? The right question you should be asking is, how do we operate in systems that are inherently not secure?" But unfortunately, you know, this desire to build secure trusted systems was so appealing, and it drove a lot of the decision making to the point where there was a real problem and a real devastating result. And that devastating results was someone that you probably have all heard of, a gentleman named Edward Snowden. He actually did unbelievable damage to our national security, because people had not embraced the zero trust, but rather had tried to develop perimeter-based, purely trusted systems. That was really the consequence. And so, when people ask why zero trust, I say, a really good answer is Edward Snowden.

So I'm emphasizing this because today, where we are today, we're at a pivotal point in next generation communications. We're all here talking about 5G, we're all very excited about what 5G has to offer, and we should be. We recognize it's a transition from discrete to continuous compute and comms, and it's all wonderful, but it's all very complex. And we have to be very thoughtful. And there is a strong push by some people, particularly in policy domains, and particularly in senior positions in government in some places that we should be going after trusted networks. You'll hear that over and over again, trusted 5G networks, trusted supply chains, trusted suppliers. And I'm trying to raise people's awareness that that is actually a very dangerous approach to thinking about how we're going to execute in our complex real world systems.

So if we actually are foolish enough to think that we can build truly trusted 5G environments, then what we're basically going to be doing is building our own Maginot Line. And for those of you guys who are history buffs, you know what the Maginot Line refers to. You know that France learned the hard way, the lesson of putting a lot of effort into building a false sense of security. So we don't want to fall into that trap.

And I think it's really important for people to stop talking about desiring to build trusted systems, but rather fully embrace what is actually very powerful and empowering, the concept of, "Okay, I am not going to assume I can trust things in my system. That's not even my goal. My goal is to develop architectures that enable me to move in an environment in which I cannot trust anything." And of course, that then leads us to a risk-based approach, which Bryan actually referenced in his opening comments. It's all about applying data-driven quantitative risk assessment and risk management techniques. That's what zero trust is really about. It is not a promise to make things perfectly secure, right? That is not what zero trust is saying. It's saying, "Look, this is the better way to operate in a system in which things are very complicated and therefore cannot be trusted."

The one final point I want to make before I turn it over to Anna, I think is next in the list, is to say, you know, when you hear people like myself and others talking about zero trust, we come from the intelligence community, we come from the department of defense, we often think about trust in the context—sorry, I'm sorry, security in the context of adversarial attacks, right, malicious attempts to take down networks and to do great things.

But zero trust isn't just about preventing malicious attack. It's also about preventing stupid, or not so stupid, human errors, right? We know that, in fact, human error is often much greater problem for us to deal with and to think about. Poorly designed or poorly operated systems are just as problematic as systems that are under malicious attack. So we have to keep that in mind.

Zero trust is a way of thinking that applies broadly. It basically says, "Hey, things are going to go wrong. There is no part of my system I can ever count on with 100 percent certainty. I cannot assign zero risk anywhere. I've got to think about constantly understanding through measurements and transparency and awareness, what is my risk? Let me assess it. Let me mitigate it, let me understand the best ways to apply that, understanding, of course, that nothing's ever going to be perfect." So I think zero trust is a really nice way of reframing how we approach complex networks. We've got to all make sure we understand that means we're abandoning this frankly naive and dangerous goal of trying to build trusted perfectly secure systems. So with that, I'll turn it over. Thanks for letting me give some opening comments.

TRAMONT: Thank you, Lisa. I'm going to jump back in, Anna, and I want to ask a quick follow up with Lisa, before we get to you Anna, if that's okay? I know you're chomping at the bit down there to talk, Anna, but okay. So Lisa, thank you. That was terrific. One of the things, though, you referred to it a couple of times is how naive and dangerous the approaches that we're trying to build trust in supply chains or trusted networks. Do you believe, as a policy matter, we shouldn't pursue components of that? Or do they not contribute to overall risk-based approach or do

you—so, are you saying, zero trust is to the exclusion of these other things, or these other things are not a solution, I guess?

PORTER: Right right. So, it's more of the latter. And of course, so people who have not taken a logic class and don't understand that A implies B doesn't mean B implies A, that people sometimes take these comments to mean that we're saying, "Oh, you can go ahead and use anybody because it's equally the same." No, no. Obviously, you eliminate the obvious sources of threat. You don't purposely go out to engage with untrusted, clearly untrusted suppliers, right? And we know who those are. And we know that there are bad actors out there or we know there are suppliers that are incompetent. You don't go after incompetent suppliers either who don't know what they're doing. That's just as bad. But you can't, by contrast, say, "Okay, now that I've gotten rid of them, I now have a trusted system." That's my concern. And that's the Maginot Line, that example that I like to give, okay, as sort of that keep that in mind. Just because you eliminate the obvious stuff, doesn't mean you got a secure system.

TRAMONT: Pretty good. Thank you. I just wanted to tease that out a little bit less. We have some questions on that front later. All right. With that, thank you, Lisa. That was terrific. And I will now turn it around, turn it over, rather, to Miss Anna Gomez.

### 2.2.3 Anna Gomez

GOMEZ: Thanks, Bryan. Hi, everybody. I have to say it's hard to follow Lisa, that was really an amazing way to frame our conversation. As Bryan said, I am Anna Gomez. I am a partner in the telecom media and technology practice group at Wiley Rein. I also co-chair our unmanned aircraft systems practice, although I guess that is tangential to our conversation today. Before I came to Wiley, I was the deputy administrator at NTIA for a little over four years. So I am delighted and humbled to have been invited to join this wonderful conference. I'm delighted because I feel like I'm that's a part of my heart at NTIA when I left. It's such a wonderful organization full of talented, hardworking and can-do people. And I should also mention that I am sure I am not the only one chagrined not to be able to be there in person, as visiting Boulder is always such a treat. And I'm humbled because of the non-engineer and a non-technologist, I never expected to be addressing the ISART, which I see is an elite engineering and technical conference and I am neither an engineer nor a technologist.

When Pierre and Rebecca reached out to me to talk about zero trust in the next generation radio layer, I thought they might have been dipping into some of the edibles that are now legal in Boulder. After all, what can I add to this conversation? Fine as I thought about it, I hope that I can contribute from a policy experience based on my 25-ish years in telecom, 12 years at the FCC, four plus years at NTIA.

So Lisa already laid out the concept of zero trust, so I'm not even going to try to do that. But one of the things that I would underscore is that eliminating trust in the radio layer means doing more than just being concerned about traditional cyber hygiene. It is about figuring out where the vulnerabilities lie hopefully, as you're designing the architecture, and how zero trust applies

to those vulnerabilities. We have experience from our prior networks and from prior studies, we have standards organizations, we have research institutions like ITS and NIST and, you know, private R&D that are all looking at these issues. And that's something that we should continue to incentivize.

Just coming up, I'm going to actually paraphrase what Lisa said in her remarks at Silicon Flatirons last year, when she said, and if Lisa disaagrees with me, you can say it later, I guess, that zero trust architecture is about resilience, which is something we often talk about when we talk about our telecom network. And her message was, you need to wrap zero trust into your network architecture ahead of time, especially the more complex and interconnected the system is, which is what we are looking at as we look at next generation networks. So thank you, again, for inviting me. And I hope next time you invite me, we can do this in person, and I look forward to our discussion.

TRAMONT: Okay, Anna, let me ask you a quick follow up question. You referred to your distinguished career, both at the FCC and at NTIA, where you did remarkably good work, we miss your contributions to government, I will say. You know, you saw two models, but more than that, probably in all the roles you've had, of institutional effectiveness in government. Lisa had a different component of that. Do you see the tools there to make the kind of comparative risk assessment across layers? And where do you think that sits? And is the FCC going to do that for commercial and NTIA is going to help do that for government or is it going to be like—how do you feel about institutional capabilities and competence across these types of issues that we've been discussing this morning?

GOMEZ: You know, this is a really good question. And part of the answer to this question, part of what makes it so difficult, is the massive scale of what we're talking about, and how it touches on so many different regulatory institutions. So right now, I can name an alphabet soup of agencies that are looking at security in one way or another in the multiple layers of our networks. And that's great, because it's good to have eyes. It's dangerous, because what you don't want to have is some type of framework in which you have different regulatory agencies, either freezing technology and time through regulation, or imposing differing requirements that make it impossible to really innovate, and coordinate. So is there a perfect place? I don't think there is. I think what you need to have is a coordinated and collaborative effort, which is a lot of how things have been done, right? A lot of what NIST has been doing in this area, and NTIA have been doing in this area, and DHS have been doing in this area has involved coordination, collaboration, multi stakeholderism, relying on standards, relying on research in order to get to propose solutions, rather than individual regulatory activities.

TRAMONT: I want to come back to this theme, I think, to the larger group, because I want to bring in the other panelists on this as well. But I think that the issue of comparative risk assessment across the network and where the risk occurs, and then looking at it from a government network versus a commercial network versus public safety network, and where that all sits, I think is a really important thing that I'd like to talk about as we move on. So thank you, Anna, for that. William, you're up next. Take it from here.

### 2.2.4 William Webb

WEBB: Thank you very much, Bryan. So I wanted to try and frame this now a bit more in the context of a radio system and ask, where are the key issues in terms of trust? And so, we made sure that we tackle the most important items, and not spend too much time on items that are very little significance.

So, I thought I'd illustrate it with looking at one of the services that's sometimes talked about with 5G. And that's remote surgery, the idea that you could be somewhere, the surgeon is somewhere else, and they could be operating on you. So let's imagine you've had some kind of heart attack, you're in the ambulance, and you need some urgent surgery before you get to the hospital to keep your life. The surgeon's in the hospital. And there's a radio link between the hospital and the ambulance and that's being used to conduct the surgery. What should you worry about most at that point in time in terms of the radio link? And I suggest that you're not simply worried about the Chinese eavesdropping, or the Russians hacking into the system and trying to insert a chip into your brain rather than fixing your heart. What would I be worried about? I would be worried about coverage. This ambulance is rushing through an open area into some forest and radio link cuts out and there I am with my heart wide open, critical insertion about to be made and the coverage drops out.

And if you think about it in our normal life, with cellular systems, when it's not working for most people, most of the time, perhaps my two cents of the time, practically 90 percent of the time cellular is not working, it's a coverage issue of some sort or the other. And actually, it was 5G that could be worse than 4G, particularly for these kind of very high bandwidth services that need to be delivered in the higher frequency bands, where the propagation is poor, and so, the coverage is naturally less. So actually, we may be in a situation where 95 or more percent of the time where the radio link is not working well, is actually down to coverage.

The next category of problem, which I suspect is about one 10th as big as the coverage problem, is the congestion issue. So there is coverage, but all the radio channels being used by other people, and I don't get a channel or I get much reduced bandwidth and it's insufficient. That is an issue, of course. Hopefully less of an issue of 5G, actually, because some of the concepts like network slicing and others ought to be able to keep high priority channels with high bandwidth. And I hope that I have one of the highest priority channels there. So hopefully, 5G will solve that particular problem.

What else? Well, about another order of magnitude below that is just network failure. The network just falls over. Perhaps it's because there's been a software update that didn't quite go right, perhaps there's been some kind of central switch meltdown, perhaps there's been a local base station shutdown, because it's run out of power or some other kind of issue. And that can happen. But it's pretty rare, actually. Certainly, the network's achieve 99.99 percent reliability, typically, perhaps sometimes even better than that. So, you know, it's a slight worry, but that wouldn't be one of my biggest concerns.

And then the very bottom of the stack, as I sort of hinted at at the start, I think security would be the least of my concerns in that particular issue. Now, of course, I could have picked a different example, which was much more related, perhaps to national defense or something where security would be a much higher concern. But I think for the vast majority of people, that's going to be roughly the order that the biggest problem is coverage, an order of magnitude less congestion, an order of magnitude below that is reliability, an order of magnitude below that is security for most applications.

So what can we do about it? Well, we can't just say we can't trust cellular, and therefore we're not going to have remote surgery, because then potentially, a service that could save lives might not happen. But the most obvious thing you can do in a situation like this is rely on multiple networks. And so, the simplest solution of all in a way to these trust issues that I've highlighted, is just to have the ability to roam across different cellular networks or wander to different Wi-Fi networks. And indeed, if you look at, for example, the performance of Google Fi in the US, which does roam across two, cellular networks and Wi-Fi, it is materially better than other networks, both in terms of its coverage, its capacity, and its reliability. So these kind of things, perhaps are some of the easiest solutions we might want to look at, as we try to understand the issues of trust. So I'll stop there. I'm sure we'll pick up some of these things later on.

TRAMONT: William, can I ask you a quick follow up question? So, you did a hierarchy of risk coverage, congestion, network failure security. From your perspective, are the commercial providers' incentives to solve those problems aligned with what government would want to have happen? Or is it someplace where there's a market failure where you think there's a role for government in ensuring those four primary threats? And you said it's a certain use case versus commercial use case? But so, it's limited to that. But do you think that the government, the commercial entities 'incentives align with government? Or do you think government needs to do more to facilitate solving for those four risks?

WEBB: Yeah, good question. So I think the short answer is no, the commercial centers are not well aligned. For most of the cellular operators, by and large, they know that actually, price is the key driver. So when we go to make a choice as to which cellular operator we're going to choose for our next contract, we look at who's the cheapest that provides whatever it is, 12 gigabytes a month and an iPhone, I'll choose them. So actually, the incentive on the operator has to spend as little as possible on coverage and so on, as long as it delivers that okay service. Clearly, if they spend so little that actually, word gets around that their service is absolutely awful, then nobody's going to choose them. But there's not that much incentive to expand coverage. And that's why we see all these government initiatives for rural broadband and so on, because the incentives are just not there. So, if we want really highly reliable networks able to deliver remote surgery, for example, then we may well need to have some kind of governmental intervention of some sort to incentivize the right drivers to achieve that.

TRAMONT: Excellent. So I know we have two commercial mobile carrier veterans executives here on the panel. So I'll be curious if we hear anything more from Henning and Charla as we go to the next round. And so, no, it's terrific. All right. I think Henning, you're up next. Are you ready for us?

### 2.2.5 Henning Schulzrinne

SCHULZRINNE: Certainly I am. Thank you for kind of setting the stage in general terms. So let me, as kind of one of the more engineering-oriented participants, dive a little bit deeper into some of the issues that were raised earlier today. So I find it useful to look at two separate issues in this discussion. Namely, one is what has really changed compared to previous generations of technology? And I'm not talking specifically about 5G that is really broader than that. It's 4G largely and whatever comes after 5G. And secondly, what exactly are we looking at when we—what system parameters are we looking at?

Let me start in the first one. So, interference at radio layer is clearly not a new thing. We've had jamming in radio probably as early as we had radio. The difference, I think, was two facets, namely, one, and this works in both directions. Namely, as we know, I mean, even in the Cold War, it was routine to jam shortwave radio stations that you didn't like, whether it was, you know, Moscow doing it or the US jamming Cuban stations, whatever it happens to be. This was even outside of a kind of a hot conflict, it was quite common. And the advantage was that you could do that pretty much globally. I mean, you could have a few HF transmitters, and you could make it very difficult to receive Voice of America, for example, in large parts of the country.

One of the primary differences, and this was alluded to earlier in kind of a remote surgery example, in one way is that it is now much harder to do that at scale. So, in order for the Russians mentioned to do that, they have to be quite close in physical proximity. Having a transmitter in Moscow, working at any cellular frequency isn't going to reach, I mean, some streets in London. So that's, I mean, in some sense, that inherently makes the job for an attacker much more difficult because physical presence before taking over an existing radio system is required to do these kind of large scale disruptions, right?

What is easier to do is to do very localized disruptions, or other attacks in that, which are then also much harder to detect. It's very easy to see if somebody has an HF transmitter and locate it. It's very hard to find out if somebody just plopped down a almost-invisible radio transmitter. Because that's really the second difference is the technology that you can use to deploy interference-causing devices is just so much more readily available, and not just for nation state actors. It's just almost impossible to detect physically, it's not like you have to have a radio tower and so on.

The second one, which I think it is useful and previous speakers of the panel have kind of alluded to that, that we really should separately look at kind of usual triad, the CIA triad, and not really in the agency; confidentiality, integrity and availability one. And I think like the radio layer, it is really primarily the availability case that we worry about, because I think we have learned that protecting confidentiality and integrity of information at the radio layer is just not appropriate. We tried that by prohibiting people from having radio scanners for confidentiality. That clearly was not terribly helpful. And integrity, generally speaking, injecting radio signals that emulate other radio signals, it's just too easy to prevent in that. So I think at radio layer in the CIA triad, availability, really, a difference.

And finally, I will say one difference that was alluded goes beyond just the notion of carrier diversity is the notion of frequency diversity. It used to be that communication devices had one radio transmitter operating at one frequency or frequency band at a time. Now, all of our devices, even the cheapest kind of cell phone operate on multiple radio transmitters on a frequency agile, meaning that it's quite possible to rapidly switch to a different frequency, different transmitter, different tower, possibly to reduce capacity and reduce performance. So having devices that are frequency agile and can circumvent radio disturbances both intentional and otherwise. It is one of the key design characteristics where the lower radio layer interacts with the higher layers. And it's often the higher layers that are not terribly good at doing that. We've all experienced, we have our Wi-Fi connection connects to a supposedly functioning access point, which provides RF energy, but no internet access, and we can't get our laptop or whatever to connect to a weaker but functioning radio access point on the Wi-Fi products. And similar issues exist at the cellular layer as well. So we should see that as a combined issue that we have a radio layer that needs to talk with the upper layers.

TRAMONT: And to build a little bit off the question I asked William, do you think on the frequency diversity dynamic, is the commercial sector adequately incentivized to create frequency diversity for its network today or is there a role for government in that? And it's obviously maybe a different question for government users, but do you think that the commercial user, the commercial entities, incentives align with government on frequency diversity? You had a lot of things in here, but I'm going to kind of tease that one out since we can tie it back to William.

SCHULZRINNE: Yeah. So I think as I mentioned before, frequency diversity, often these days because of a historical notion of the idea of evolution, that different carriers have historically acquired different frequency bands, even 4G. I mean just [inaudible] when the old [inaudible] when obviously lots of 2 GHz spectrum and AT&T and some of the client AT&T Verizon have much more low band spectrum and so on. So they've each had niches of spectrum. And so, I think there are two notions that I think are important. One is, I don't think there's the incentive we've seen now that only after natural disasters do carriers typically allow unauthenticated roaming, or I do roaming, allow even authenticated roaming. And that, I think needs to be just much more part of routine operations just because frequency diversity also implies carrier diversity, largely. But it also means for devices, I think this is getting better. But with 5G, I suspect will be better stacked to an environment where devices are not necessarily optimized to operate across frequency bands because of a difference, particularly cheaper devices. They often have a limited number of bands that they support, so they're optimized for a particular carrier, even if they provide basic functionality across carriers. So they're normally, not carrier type, but practically there. And it's often difficult to tell from a user perspective. I mean, how many people know how many bands their have current cell phone supports? It's not advertised, typically, both for government users and for more critical infrastructure type users. I mean, you would have to dig deep into the specs to find out which bands are supported on that, which gives you back at least theoretical hardware diversity.

TRAMONT: It's a great party trick, though, do you go up to people and ask what how many bands their phones operate on? They love that question. It just really gets … how that works in the breakout rooms. At any rate, I'm going to turn it over to Charla as our last panelist, but I want to also encourage our panelists to have comments ready to what other folks have said. I've asked a few additional questions, but if you all want to comment on what others have said, I don't want to diminish any organic conversation. And we have started to populate some questions from the attendees as well. So we'll turn to those but before we get there bed and clean up, Ms. Charla Rath. Madam CSMAC guru . You're still muted, Charla. There you go. Okay. There you go.

### 2.2.6 Charla Rath

RATH: There we go. Good. Thanks. Thanks. Appreciate it. And I was debating whether I should just go ahead and answer all the questions that I think have arisen from various comments made here, but I am going to stick just a little bit to some of my prepared comments.

First, thank you to the organizers. This has been great. Like Anna, I have a very fond place in my heart for NTIA. It's actually where I started my telecom career on spectrum working on UHF taboos. Though for those of you old enough to know what those are, you can ask questions about it in the Q&A later. I have been—I am not an engineer, I'm not even a lawyer. And you know, I'm one of those nameless sort of people here. I've been primarily focused on the policy issues. So starting my career really in the radio later layer and looking mostly at the efficient use, from an economic perspective, which, you know, those of us who have studied economics view the technological efficiency as being a component of economic efficiency. And later then, when working for Verizon, I actually was very focused on the acquisition of spectrum.

So the early part, what we were doing in the 90s, was really looking at a way to get around and get through the block allocation system, which essentially was set up, managed one of the risks in the radio layer, which is interference. You know, if you could set up, you know, know what was going to be in each block and know what the technical criteria were, you could actually presumably manage your interference in a highly regulated approach.

So what happened is people started thinking, should there be greater flexibility? There's this increased demand for spectrum, we need to get beyond this. So the engineers in the room and these conversations would always be like, but you're going to create problems with interference. And those of us on the other side will say, "Well, we'll just fix that with technology." So, you know, again, I'm simplifying the discussion. It was much more robust and, you know, and well done than that.

But it essentially, really, a lot of our changes, particularly in the mobile industry, were based on this idea that we needed to figure out ways that to provide economic incentives to use spectrum more efficiently. So, as I said, I mean, interference has been seen as a key vulnerability of the radio layer made worse, not just by these more modern approaches, but by the increasing

number of radio systems and devices, which really gets to one of the fundamentals of 5G, when people used to ask me, "Well, what do you think 5G is?"

You know, to me, it was a combination of things, one of which included an incredible increase in the number of devices that you might be seeing. And everybody on the, you know, the panels and everywhere has been talking about that that is really key for what 5G is going to look like. It's also going to be an incredible increase in the number of people, organizations, you name it, that are going to be operating at very high bandwidth simultaneously.

So those two things together, are, I think, what is, you know, going back to what William was saying, and what Henning was saying both is going to create, you know, a fair amount of the risk in the radio layer, is actually how do you manage that piece, how do you manage that growth?

Later in my career, where I spent the time expanding Verizon's footprint, and by the way, just to address one of William's points, we went from covering 90, when I started, we covered around 88, 90 percent of the population of the United States. And anybody who knows how the population is distributed in the United States would know that we actually are a fairly rural country, in the sense that I think it's something like 50 people per square mile is what the average with incredible pockets in cities. So it's really easy to cover the cities, not so easy to cover rural, by the time I left, we covered 98 percent of the population in the United States, every percentage.

You know, some of those percentages, were actually through a program that Verizon had. And, you know, you get very few people and a lot of land for the coverage that we got. So I agree coverage is an issue. I also think, you know, I'm not quite sure they're the same thing, but I think capacity is also an issue. And, you know, William was talking about congestion. I am concerned that, you know, the trade off in spectrum from a physics point of view is very clear. You know, the higher bandwidths actually give you more capacity, but they also create problems with coverage.

So, in a sense, you know, what, again, we've seen some of these issues resolved through technology through antenna technology, through processing. But that really, to me, is the dichotomy here as we go into the 5G era, how do you actually get the kind of coverage you need at the same time you get the kind of capacity you need? There are going to be a lot of things that can operate at lower frequencies with great coverage. But I would argue that that surgery example that's given, you know, depending on the kind of surgery it is and the kind of MRIs you might be needing to pull up and all of the different things you might have, that that's a pretty high capacity type of example, the where are you going to be able to do that, that you get the kind of, you know, get the kind of coverage? And how are you going to solve for that problem?

So, in any event, I'm going to skip through some of my comments, because I've already spent a little too much time here answering some of the other questions. But just the final point I wanted to mention is, as Bryan mentioned, now, my latest gig is as co-chair of the Commerce

Spectrum Management Advisory Committee, which has one of the worst acronyms you can imagine CSMAC or CSMAC. And one of the things that we just adopted in our recent July meeting was on unique identifiers. And what was interesting about that is I think there was a lot of sense, "Well, this will solve all the problems."

But in fact, what the CSMAC found and what the committee that Bryan was actually co-chair of found is that it makes sense to do it in some instances, in some instances, it doesn't make sense. And there are all sorts of issues involving security-privacy cost, that actually surround every single one of these solutions that you're going to try and do to have a zero trust at the RF layer. So with that, I will stop and we can move on. And Bryan, I'm sure you're going to ask me a follow up question.

TRAMONT: I just got so excited when you talk smack to the group like that. CSMAC! Okay, anyway. So, my follow up question is, you know, William talked about the four vulnerabilities and ranked them and you responded a little bit about where their commercial sense lie. Do you believe there is a role for government to enhance any of those four vectors or do you think those are things that are better left to the commercial sector therefore being, you know, coverage, congestion, network failure and security?

RATH: Well, you know, it's funny. I think there's probably a role in every one of them, depending on, you know, where you're talking about. I mean, coverage in rural areas continues to be an issue. And by that, I mean, the truly rural areas. The interesting thing is, I think one of the roles and that both Henning and William alluded to it is making more spectrum available. I mean, what happened, for example, when I was at Verizon, we actually did create a fairly robust spectrum portfolio. But the first part of that was not on purpose, in a way. I think if had we had our choice back in the early days, we would have loved to have gotten more cellular spectrum, but instead, we got PCS, and then we got AWS. And then, you know, we went back down to 700. The decision at the time for Verizon to go into millimeter wave, though, was a very definite decision to diversify portfolio. And I think many of the decisions after that have to do, in answer to a lot of the questions that William put forward. So fundamentally, what can the government do? They can make more spectrum available in a variety of bands?

TRAMONT: All right, thank you for that.

RATH: And that's the answer.

### 2.2.7 Panel 1: Q&A

TRAMONT: All right. Well, I was going to—well, I mean, Verizon built their network without universal service support, as I recall, and arguably has the best coverage. So I guess one question too, you know, I mean, William pointed out, I think that, you know, government subsidizes the building of networks for coverage purposes, and they do, for billions of dollars right now. But it's interesting that Verizon is not one of the companies that's taken that over the years, so it's interesting on that point?

RATH: Yeah. No, and that's true. I don't know whether, you know, honestly, I'm not sure what's happened in the last, you know, couple of years on that, but absolutely true, when we were building, you know, the coverage, the footprint in the 2000s.

TRAMONT: In different build-out rules, and all that sort of thing back in the day, but understood. Understood. I'm going to try and bring back in Lisa, if you don't mind. You want to react to anything, let's see, on this front?

PORTER: Oh, I thought everybody had really great points to make. And I would actually say William's absolutely right when he emphasizes, you know, there's a difference between use case, right, that the DOD and the National Security want to think about problems differently. So, you know, and I've made this point many times, the commercial sector is going to drive the technological advances that occur here, and the DOD and the National Security are going to need to line themselves up to take advantage of that, and those advances and all the things that everyone was just talking about, and then try to tweak and tailor them to our specific use cases, which may be a little bit more weighted toward risks associated with malicious actors. But if we're thoughtful as a community and technologists in particular, we try to design resilience such that we can accommodate as those dials turn, as William gave that one example that I thought was a really, really great example. So I just wanted to emphasize that I totally agree with that point that, you know, the average person on a given day may be much more worried, and rightly so, about a coverage risk versus a security risk. On the other hand, you don't want to only have the ability to deal with one of those risks. Even very low risk, but high consequence events, as we all know, are particularly important. And that's part of how good system engineers apply risk assessment techniques, right? It's all about managing risk and understanding the consequence, if a risk materializes, and how you minimize and mitigate that impact.

TRAMONT: I want to follow up on that, because, for me, at least, it's one of the most interesting questions is that, and maybe I am too institutionally focused, but whether or not there's somebody with vision sitting in, and I guess it's the government, that is looking at comparative risk assessment, and in an institutionally effective role to help the government or to help the country solve for those risks. And whether, you know, you just mentioned some cross pollination between the commercial sector and the DOD, and I suspect some will go the other direction. Do you think those lines of communication are there, are the institutions effective, or, you know, God forbid, should there be a different institution, or are the current tools the right way? I'd just like to explore that a little bit for the audience.

PORTER: So I don't want to hog the hog the mic here. I will say, God forbid, and other institution is the answer, just as we have enough of those in the government already. I do think it's a really hard question. I think Anna touched on it, Charla touched on it, we all touched on it. And you know, part of the challenge as well, as you guys were alluding to, is the incentives even on the commercial side, to enable the full ability, right, to build out what we need. And all of this becomes very complicated. So the short answer is right now, there certainly is not one government agency that's doing that cross cutting, holistic look. I think the government as a whole is still trying to just get its head around what does 5G look like and how do we take advantage of what's coming in a way that's beneficial to us, and the benefits outweigh the risks?

So I'm not giving a good answer other than to say, I think it's what Anna alluded to earlier, a lot of coordination and collaboration has to happen at the working level. And I'll just share with you and the audience, that when I came into the job that I was just, you know, that I just left recently in the department, I didn't know anything about spectrum and 5G. In fact, I thought it was a really boring topic. And I apologize to everybody on the line. I was like, "A spectrum? What is that?" You know, I'm a classically trained physicist, I'm like, you know, give me quantum physics any day. But then as I delve into it, I said, "Man, this is so fascinating." And I got to know the folks at NTIA out in Colorado, and I got to know a lot of the folks at FCC and I said, "My goodness, our country has so many really smart people. This is real hardcore engineering. This is awesome." So I think we have the sort of raw ingredients as a country to pull together that expertise, the hard part is just allowing and enabling it to happen. And that may sound a little pollyannish, but I really do believe, from my exposure, that we do have a lot of really talented people. I think if we can incentivize them to get together and think holistically about how we process, I mean, to Anna's point, and she said it a lot more eloquently. So I'll shut up now, turn my mute on here.

TRAMONT: All right. So I don't know if Anna rather would have jumped in. Anna, do you prefer quantum physics or 5G, and tell us why?

[ Laughter ]

Come back and from the institutional point and I want to bring William and Henning in too, but Charla or Anna, whoever wants to jump on?

RATH: Yeah. Actually, the only thing I would say back to Lisa is I feel the same way about cybersecurity. And I think that there's the same sort of learning process that can take place, for those of us who come more from the spectrum side, that, you know, every time I talk to people about the security issues, I have the same sort of reaction. There are a lot of things. Even just preparing for this conference, it started making me think a lot about, you know, various ways that I just think about spectrum and that maybe, you know, I need to rethink and have a new way of thinking about some things based on, frankly, not just cybersecurity, but this concept of zero trust. So I think it works both ways. But I do think there's a fundamental issue and is I went back and reviewed materials and looked at the Silicon Flatirons, it seems that everybody keeps coming to the same thing that there is this issue of, you know, maybe it can be solved through a multi stakeholder approach that Anna talked about earlier. But I do think that is a fundamental issue in the government is who's in charge in a way?

GOMEZ: Yeah. So here's the issue with any one institution having control or for some type of regulatory authority over the entire framework. And that is that each institution has a different mission. And that mission doesn't necessarily align with the holistic mission that our country should have of, you know, having a strong economy, having innovation, research and development, more than just a mission of security. And we see this every now and then when we see things come out, like we should have a private 5G network, because that is the only way that we can have a truly secure network. That, it doesn't work, although it may enhance a single agency's mission. So, I find it very difficult to say, we're going to have a single entity that is

going to basically work to eliminate every vulnerability in, say, a 5G network. So, I do think that the answer is some type of collaboration. To Bryan's point is, but who's that person at a very top that is pulling together all of these folks? You have DHS that has the coordinating center, you have NTIA that has its various activities, you have NIST. My view, based on my past experience, is you should have somebody at the White House that has a portfolio that involves both your economic side and your security side, that is the one that ensures that all of the right parties in government, and in the private sector and academia are talking to each other and working collaboratively towards this exact mission.

And in the end, zero trust isn't going to be the silver bullet that says, "Boom, everything's secure, we're never going to have a problem." So that's, I don't think that's not the mission that we should all be working towards. We should be working toward identifying vulnerabilities, trying the best that we can to anticipate them, and where we do find them, as well as also learn from our past mistakes. Where we do find vulnerabilities, how quickly can we resolve those issues? How do we ensure resiliency through lots of spectrum allocations, through diversity of suppliers, et cetera, et cetera? All of these things that all the stakeholders should be working toward, but that you can have a government person sort of at the top, making sure that all of these different missions, and all of these different goals are being addressed by all of the different agencies that are involved in all of this. And then, you know, let's not even talk about sector-specific agencies that are involved today in thinking through these types of vulnerabilities.

TRAMONT: Great, thank you. And I think, William, you want to jump in?

WEBB: Yeah. Thanks. So, I mean, I think it's right that in an ideal world, you can imagine a situation where you would have somebody who having a perfect knowledge of everything, could sort of sit at the top and say, "Actually, we need to do this, invest in this, this, and this, but these are the key issues. Let's get it done. And let's make that happen." But as we've all kind of said, that's just not going to happen.

If we look at what's happened in the last year or two, the government has got very concerned about things like Huawei, which, as we sort of talked about, is probably an issue, but it's probably one of the smallest issues of all in terms of the bigger holistic picture. So I think it's very easy for the government to go down the wrong direction.

So what are the solutions? Well, there's no easy solution, of course. Otherwise, we would have found a long time ago. But one thing I think we are missing is some really good consumer information. So what I'd love to know, for example, is what's the best mobile operator for me, given that I live in one place, I work in a different place, I commute there by the train, I then go out on my bike, and I like to have coverage on my bike when I cycle in the countryside, I use certain applications, and they have a certain degree of reliability, which is the perfect operator for me? And of course, that's really hard for me to know without trying all four of them, one after another.

But equally, it's pretty straightforward for some kind of an app to measure where I go, to have knowledge of what the coverage and performance of the operators is and to deliver that as a

personalized recommendation to an individual. And I think that's why government could help is by actually making sure that as the information is out there for people to make very well informed decisions that fit their needs in terms of the trust they can put into the network or the degree of reliability and so on that they need. And that can then send better signals to both the commercial entities, the operators, and so on, but also principal to government just to understand why there are areas that perhaps people's needs aren't being met, and have a more of a sensible structure for intervention.

TRAMONT Great, thank you. Henning, you want to jump in as well?

SCHULZRINNE: Yeah. So I wanted to make it slightly more concrete because I think some people might have been a little bit polite, too polite to mention this. Namely, that we have also intentionally, I mean we or some parts of government have intentionally, disabled and defanged mechanisms that we actually had. You know, talk specifically about the FCC, Federal Communications Commission, in two dimensions. And namely, one, and this goes directly from what William just said, is one of the classical roles of a regulator, and I think this is different from some of, I mean, Deputy Assistant Secretary in the White House type thing and somebody's way deep staff and long term operational interaction wavy networks as opposed to in a more a policy sense. I used to have two role, or had, so namely, one is I'm tracking network reliability. And that's been one of the earliest responsibilities for a regulator. And it's true for Ofcomm it's true for FCC, it's true for others in that because in my mind, it's just like for air travel reliability, many of big problems have indicators in small problems.

If you have continuous reliability issues at a small scale, that's probably an indicator that maintenance and operations are not what they should be. So if there's a larger outage, either induced by nature or induced by an adversary, you're more likely to also fail that test. And this is the usual problem when you look at airlines, it's the ones that have active big accidents are usually ones that have lots of maintenance problems, that didn't cause an accident before. And we have essentially disabled that capability by choice.

I have reliability data, it's not just coverage. Reliability data is not disclosed to consumers. And this is particularly important, I would say, because many of our networks, we are particularly, and for first responders that used to be operated by first responders kind of your land mobile radio, and FirstNet were operated by commercial carrier. I mean, as best as I know, no public disclosure, if you've a local fire department as to what reliability has been, both locally and global. And it's true that many of the kind of—the other thing that was done in the past was that there were reliability requirements. For example, for kind of what used to be called N-rake and NCIS rake and so on, but also by the state law typically on service quality requirements, time to repair reliability requirements for networks. We have abandoned that. As some of you know, I was under the previous administration attempt to for example, force backup power. We bended that effort intentionally. This was not some—I mean, this was an intentional political decision not to require backup power on cell sites, you know. So there are numerous example where the tools that we had available were chosen not to be deployed.

TRAMONT: All right. I think we can talk about that for a while, I suspect. But let's throw it open. We've got some questions that are from our audience. And I'm going to take this first, most liked question from Mark Norton. To all the panels, which specific elements of a trusted architecture, if any, you envisioned to be replaced by a zero trust architecture, device certifications, trusted certificates, encryption algorithms, something else? So who'd like to jump in on that one first? Lisa is going to go. All right, thanks, Lisa.

PORTER: Sure. So Hi, Mark. It's good to know you're out there. Mark Norton is one of the great government folks so many of you guys know who he is. He did great work for us the DOD for a long time. So, I do think it's not. We have to be careful when we pose a question. And first of all, there are no trusted networks, but I think what you're asking is what are we doing talking about in terms of migrating the existing paradigm to a paradigm that incorporates zero trust? And it is kind of the types of things that you mentioned.

I think most people are aware, or if you're not aware, you should know that NIST just put out a special publication, I think in February, basically going through zero trust in quite some detail in terms of what is currently understood, the types of approaches that can be used specific to networks. And those are the kinds of things we're talking about incorporating. You know, micro segmentation, in general, I think is a good approach. Understanding the user, the device, the application, all of those in context, dynamically allocating access, not one time means all time, all the things you can read about in the various literature that's out there. That's what we're talking about. And it is a shift.

And of course, I think everyone here knows that Google has already at least demonstrated proof of concept in their BeyondCorp back in, I think it was 2014, when they started putting that in place. So the concept of how you implement zero trust architecture in a network sense is not an unknown. That said, as we migrate to 5G, and we have more and more, you know, devices and more and more use cases, and we introduce more virtualization and all the other stuff we've been talking about, it does become more complicated. And there's an issue of overhead, which I think was one of the other questions I saw in the Q&A. And that is certainly the trade, right? So that's why zero trust isn't saying we're going to make perfectly secure systems in a new way, right? It is abandoning the notion that you can have perfect security. And it is instead bringing in the classic system engineering approach of risk management, and recognizing there's always risk. And then understanding where those risks are, trying always to improve your knowledge, developing mitigation strategies so you can limit the, you know, the impact if a risk materializes. All of that kind of thing is what you're bringing to bear in a zero trust framework. I know that-

TRAMONT: Yeah, this is very helpful, I think. Can I do two quick follow ups, though? So just for the group's benefit, can you briefly define or discuss what micro segmentation is just so they have that as a benchmark?

PORTER: Sure. And then- I'm sorry, go ahead.

TRAMONT: I want to talk a little bit about the risk management and the cost benefits question, both as to commercial networks and government networks.

PORTER: Okay. So micro segmentation basically means you're basically bringing your perimeter, if you will, down to a very tight circle. And you're only allowing access to a very specific, what, you know, let's say somebody wants to access your printer, they're only getting access to that printer for a particular period of time. They can't touch anything else, even though you have decided because you've looked at who they are, you've looked at their device, you've looked the application that they're interested in running, you've decided that the risk is manageable, you're still only allowing them access to a very small element of your network. And that's one natural way, of course, to mitigate risk. So it's a term you'll hear a lot. And again, it's, you know, there are more formal definitions, which I don't have one written in front of me. But that's the essence of it. And you'll hear that word a lot. And in fact, the DOD is, in our 5G strategy that we put out, I think we actually referenced this concept of part of what the DOD is looking at when we talked about to zero trust. And you had a second question?

TRAMONT: The role of cost benefit analysis in some of these conversations about relative risk and managing risk.

PORTER: Yes, and that of course, gets back to our other huge challenging question of that. The equation is going to vary depending on who's deploying the network, right? However, if you have in place, the right data driven tools, and again, these are going to be constantly updated. It's not that you solve it once and you're done. This is the whole point of zero trust is you assume you're never done, right? There's no finish line here. But whatever tools and algorithms you have, whatever measurements you're putting in place, and I think it was one of the panelists was talking about the need for much more dynamic radios present. There's a lot of technology that goes with this, right, because the more you can respond, the more you can measure, the more you can sense, the more information you have, the better decisions about risk you can make. If I'm using a network from a DOD perspective, I may dial my cost benefit trade analysis very differently than William does when he's driving, again, you know, he's got the heart attack situation, you know, God forbid, in his ambulance. So you want to have an architecture that allows you to make those trades depending on what you're doing and what matters to you.

TRAMONT: Great, thank you for that. It's interesting too, the way that that conversation just draws back in Anna's point about emerging the economic and the security interests of the country, in one entity or looking at it being able to look system-wide either DOD or commercial. Public safety networks are a whole different animal because of the local control, with the exception of FirstNet that Henning referred to before. Do others want to comment on cost benefit Henning?

SCHULZRINNE: Having done my fair share of it, I'm more tempted to do a networking space, cost benefit is like one of these things that truly is a good idea in theory, or and I mean by any economic rationale. In practice, certainly in the cases that I found, it is extremely difficult to do with high uncertainty situations, because—and this is what we're dealing with really, namely, we're dealing with probability estimates, for example, what is the probability that an adversary who followed on that is able to disrupt a particular network? Or what is the- or converge some other part of the infrastructure into jammers, or whatever the case may be?

Now and since picking that number is essentially guesswork by necessity in that sense, it's a way- most of these estimates are really difficult. Secondly, estimating the cost is difficult simply because many of the defenses that you institute, and this is very similar to the issue for environmental regulations, they have other benefits. So for example, I mentioned backup power, that has an advantage so that if an adversary is able to disrupt your electric supply, that provides protection against adversarial interference. But it obviously also provides protection against more mundane events, like a local power outage or storm, whatever, in that, and how do you attribute the benefits to that. And then thirdly, even measuring the benefit is hard because I mean, you mentioned that there is a kind of government networks versus private network. But if we read your layout, I suspect within a number of years, that distinction will be fought all by me tactical networks are built into chains and things will basically disappear. They'll all be operating on commercial networks. It's true for utilities today, that you still have our own LMR systems. It's going to be true for public safety. It's going to be true for local government. It has always been true for local government, they don't run their own network, wireless networks, certainly not cellular network, and that's certainly not internet-based networks largely, and so on. And so, that distinction, how do you attribute value to disruption-free operation for about I don't know how to do that. So cost benefit analysis sounds good. In practice, it is essentially usually used to confirm your hires.

TRAMONT: Okay, thank you for that. Charla, you want to jump in on this before I have to feel the need to discuss the perils of a mandated backup power plan at the federal level?

RATH: Yeah, yeah. No, I'm hoping you will address that. But I just quickly wanted to go back to one of the things in Mark's original question about device certification. Anybody who's dealt with that process at the FCC knows that one of the issues with device certification is also the enforcement because you can get a device certified, but then it doesn't necessarily, when it's sold, doesn't actually operate the way it's supposed to, according to the way the device that was at the commission was certified. So, you know, so I look at that, and I go, "Well, so how do you deal with that, particularly in an IoT world where you'll have all of these devices?" And again, I'm talking about the interference piece of the risk and vulnerability that we've been talking about, not necessarily, you know, something related to cybersecurity.

So how do you actually go about ensuring that the devices that then are sold in the marketplace actually operate according to the way that they're supposed to? And maybe there is some sort of identifier, maybe there is a way in the network, but then that means the network becomes more costly. So there are a lot of issues there.

And then on top of that, this gets back a little bit to Henning's point about things that the Commission doesn't do anymore. You know, one of the things that it did do a couple years ago, was get rid of a lot of the field operations, which, you know, as an ex-Horizon person, you know, a lot of the engineers that worked in those groups were very helpful in tracking down interference. You know, we had an incident many years ago, but it was huge incident in Manhattan, where, you know, somebody put, you know, put a device on, I forget, like the 30th floor of a Manhattan tower and it knocked out 200 base stations in lower Manhattan and New Jersey. And with the help of the FCC, we were able to track down, you know, where, you know,

where that was. But, you know, that may not happen now, there are certain other things that have taken place. But I just wanted to throw that in that a lot of this, you know, from the commission point of view, we still have to think about how do we make sure that whatever it says should be done actually happens?

TRAMONT: And does anyone else want to jump in on that? If not, we have a question from Pierre that I feel like, you know, I want to get invited back next year. So I need to ask the Pierre question. And this is for Henning. So you mentioned that for the radio layer confidentiality, integrity and availability is CIA, the main risk is availability. How do you think about spoofing on the integrity front and rogue base stations like Stingray, which remain a vulnerability even in 5G, the radio access network.

SCHULZRINNE: And thank you for following up because I think that probably when I said it first came across, not quite late. And it's why I mentioned that we should really think of a radio layer as integrated, even if we think this is truly just kind of physics to pick up kind of the earlier comment from one of our panelists, here namely like kind of electromagnetic radiation type thing and so on. In fact, the spectrum is useless unless you can access it. And that plays out in two ways.

I want to emphasize this, namely, one is truly, we need to base station authentication. And my understanding, and others who are closer to that can correct that, that 5G itself is pretty good on that. But because of fallback characteristics, because we're not just operating a 5G network, in fact, we're operating a 2G through 5G network. If your adversary can force you to go to 2G, you're right back in vulnerability land because of all that, Pierre was mentioning kind of the ability to switch to 2G towers, which actually made that trust assumption in a wave, which turned out to be short sighted-wise.

I do want to point out one additional kind of interlayer issue that we haven't talked about, namely, almost all new bands are going to be database driven, as in availability of spectrum is driven by querying a database of a spectrum database. This is true for CBRS, this is true for many of the millimeter wave bands, because of incumbents are enough. And so, when we think about spectrum availability, we need to think about what kind of a basic availability, can I switch spectrum and so on? But the inter-carrier availability, which I mentioned, which I think deserves more attention as well.

But thirdly, if I wanted to disable a network, the best way to do that is to disable access to a spectrum database. Because as a single point of failure, no device is allowed to just connect without getting an okay from the spectrum database. And now, all the spectrum in the electromagnetic spectrum may be available in theory, but no device can access those, at least most of us that use that, in that it was not a radio issue is a fundamental vulnerability even at the spectrum level.

TRAMONT: So, and Henning when you refer to that, are you thinking is 3.5 a model that you would point to, is that going forward?

SCHULZRINNE: Yeah, my CBRS is 3.5 GHz. Yeah.

TRAMONT: Yeah. And in that case, there are multiple spectrum databases available. So you refer to a single point of failure, is your premise that it would get behind the individual database or the coordinators and attack it at some central level? Is that the thesis?

SCHULZRINNE: Yeah, so because we have two vulnerabilities. Namely, one is and one thing that I don't know in terms of how this has been handled operationally, whether a device actually is able to query multiple operators or database or whether it is essentially tied to one and how would I know ahead of time? Though I may not be able to knock out everybody but I am and if I know that my local, whatever, my local National Guard unit is using one of the spectrum databases, if I knocked that one out, then obviously I've disabled frequency access for that important user in that.

And secondly, there's a backend database which feeds based on, for example, the military useful radars and 3.5 GHz band. So if I can disable the feed into most multiple databases, then I have achieved kind of universal blockage, if you like, in that sense. And I think this has not been received the kind of attention that it deserves, because we have to, even though it's a zero trust network, we all essentially have to trust, and we're force by regulation, I have to trust the database. If the database tells me no, and particularly because no answer means no, it is not a failsafe. I'm not allowed to use it unless I receive a positive go-ahead answer. I have created a system where I essentially need to trust the availability of a database, and for good reasons. I mean, good reasons not to allow transmitters to just blindly go ahead if I can get a reliable answer.

TRAMONT: I do want to bring other people in, and this is a model that has been increasingly turned to by policymakers has not yet been as proven in the marketplace on a commercial basis. And I'm sure that I would be remiss if I didn't point out to our DMRS friends would say that this is the why it's so important to clear spectrum completely, so you don't have to rely on a database like that. But does anyone else want to come in on this? Because it is an emerging field, obviously, of study here. Anybody want to bring? Come on in William? Yeah. Come on, William.

WEBB: Yeah. So, Henning's exactly right, that if you have a single point of failure, and you have a risk in the system, building away, those are the easiest ones to defend, because it's very clear, they are high risk. And you can add in any level of redundancy that you want. You can duplicate them, you can geographic-distribute them, you can come up with all sorts of mechanisms that effectively ensure that they remain extremely reliable. So, you know, I think it's important to identify them when we take the appropriate measures. But I think actually those are fairly tractable.

The one that actually worries me the most is GPS. If you turn off GPS or take it out, then you'll take out all communication systems pretty quickly, because they rely on GPS at some point for timing or something else, or for backhaul synchronization somewhere in that whole process,

they will rely on GPS. And that's the thing that really is the weak link across the whole of our communication network systems.

TRAMONT: Now, we're talking about some GPS vulnerability in here. Lisa, you want to jump in on this? Anybody else? Can we say the L-word, Ligado stuff in our group here now? I'm sorry. If anybody else had to come in on the database or Henning, come on back, yeah.

SCHULZRINNE: Yeah. So I'll just say quickly under GPS, because actually illustrates a note, I know. I won't touch the Ligado issue, but I will touch the other one because, and I think this is favored of some participants possibly. And particularly Pierre, just a minute ago, we talked about the FCC certification process does not really cover operational devices. They cover what's submitted to the FCC approved lab. And we found the problem, as a normal consumer, I have no way to verify or even as an institutional consumer, like when a Public Safety Agency, how robust is a particular GPS device in this particular case against external interference?

I will just say if it is so easy for Ligado to interfere by setting up a transmitter, building a transmitter that emanates in that spectrum is not exactly hard for anybody does not require even advanced knowledge or advanced technology. So if you want to disable GPS, if all it takes is a single transmitter in downtown D.C. to disable GPS data, we have a bigger problem than Ligado. So I would argue that the lack of robustness tracking by either the FCC or other agency is a big informational deficit. You mentioned market forces earlier, that doesn't allow agencies in particular, also private users like utilities that are critical to make reasonable choices to pay more money for more spectrum robust, I mean, interference robust devices enough.

TRAMONT: William, you want to come back in on that? I think there's a lot of market forces stuff to be-

WEBB: Yeah, so just a very quick response. So, actually, I'm not worried about interference really, on that. I think taking out a small error with some interference is fine. Like, it's not a particularly big issue. I'm more worried about the whole system going down. So, you know, something catastrophic, like a software upload to the GPS satellites that turned out to have a built-in vulnerability that meant they all suddenly turned off at certain points in time, that that is my key concern. I don't think we would have particular interference problems to worry about anytime soon, for cellular networks here.

TRAMONT: Great, thank you. That was really important distinction. So we have about five minutes left. I want to have a closing question for all of our panelists. And I'll give you a multiple choice. So what is the one policy issue that most troubles you in 5G security? And what should policymakers be doing about it? Or if there's some area for additional research in the zero trust area that some of our audience might go off and write a paper about that you think would really benefit from some additional intellectual work, what would that area be? So I'll give that choice and let's go in reverse order of the opening. And we'll have Charla start. Is that okay? Oh, surprise. You're on candid camera. Come on back on the screen here, Charla.

RATH: Actually, I don't know what happened to me. Can you hear me? Hello?

GOMEZ We can hear you, Charla.

TRAMONT: You're back now.

GOMEZ: You're back.

RATH: Oh, good. Okay, great. I wasn't sure. Well, you know, I realized that this is what the conference is about. But I think there is an interesting place for just further discussion of zero trust and RF, and really looking at, you know, really going in and maybe even looking at some of the things that we were talking about. Like what kind of model is the best sort of model? You didn't really get into the question, you started to allude to it a little bit before about, you know, is everything going to be database or, you know, is exclusive use gone forever, despite the fact that there might be some benefits?

As, you know, in a zero trust world, you know, it's, I think there's a lot of work to be done, and then maybe can be generated out of this conference on just looking at, and maybe taking a good, you know, the idea that database is going to be the future, also, I find that somewhat difficult, because then what it does is it locks in place, what could be very inefficient uses of spectrum. So, in any event, I think, you know, looking at that in the context of, you know, zero trust networks, just strikes me as being, I realized, it's a little bit of a cop out, because it's saying, "Just do what we're doing here." But I think we're only going to touch the surface here. And I think there could be some really interesting economic papers that come out that talk about the economics of spectrum that are tied into this issue.

TRAMONT: Great, Charla. Thank you. Henning, you're up?

SCHULZRINNE: Yep. I would emphasize that we need a much better understanding of a little bit interlocking both on abilities, and what kind of hidden dependencies that we may not realize kind of outside the spectrum databases as a topic, we talked about. And so, we tend to organize engineering and research by layout, but many of the vulnerabilities are really costly vulnerabilities that we need a much better handle on. And finally, I'd say, when we talk about vulnerabilities, we should really be clear of what we are worrying about. I think the panel has teased that out, but often in the public discussion is just one big kind of security, a thing that is mentioned without really saying, "Are you worried about a nation scale disruption? Are you worried about localized attacks? What is the effect model?" Because without effect model, there is no engineering and there is no even rudimentary cost benefit analysis.

TRAMONT: That's terrific. And of course, it plays to essential one of my hobbyhorses, which is the importance of cross layer and interdisciplinary approach to a lot of these issues in University of Colorado, and I sort of been very dedicated to those ideas. So thanks for that Henning. That's great. William, you're up?

WEBB: Thank you. Yeah. So I think I've actually pretty much aligned with Henning. You know, I think we need research in many areas. And of course, there's lots of great research going on. And it's very much needed in interference management's with other kinds of things. But actually,

it strikes me that the key question really is, what sort of levels of reliability do we actually need and are prepared to pay for either as a nation or as a commercial entity? And therefore what kind of levels of intervention are going to be needed in order to make these kinds of things happen? And I take all the points that Henning made before that it's really difficult to do these analyses, and it can only be pretty much a guesstimate. But even so, I think it would be important to start to understand whether, as a country, we should be focused on ensuring we have one super high reliability network that the government is going to put a lot of money into, or can we just leave it to the commercial world and we'll take whatever we can and get away with it and where do we sit between those two? So that's where I would focus the research, I think.

TRAMONT: Great, thank you, William. Anna, and then we'll wrap up with Lisa.

GOMEZ: Okay. So, policy that would trouble me is sector-specific agencies going beyond their traditional remit to try to regulate the networks. And I'm going to give an example that's not a perfect example. But I don't know if you remember, Vice President Cheney had a pacemaker-defibrillator, that was wirelessly connected somehow. And because of concerns about a possible assassination plot, they had to turn off the wireless connectivity. And so, that is a worst case scenario risk that really applies to one person, a handful of people around the world. And what you don't want to have is that it's very unlikely risk driving regulations that then affect the entire system. And that is my worst case scenario way of explaining that my concern is to make sure that we are balancing incentives, balancing economic and security, ensuring that we continue to drive the innovation that has gotten us to where we are today in a way that is good for consumers, but also good for the deployment of the technologies.

TRAMONT: Great, thank you, Anna, and then Lisa, and then we'll break out into our rooms with Melissa.

GOMEZ: Great. Well, fortunately, you guys all said awesome stuff that I really can't add to very much. I just I guess I would close with reminding folks that what we're trying to say with zero trust is not that we have a solution, right? We're not saying we have a new silver bullet, here it is, it's zero trust. We're actually trying to invite people to think deeply about the fact that these are going to be complex systems that there are going to be vulnerabilities we don't anticipate some of that was alluded to, that we do the best that we can to continually learn and improve.

But always keep your guard up. Because frankly, you've got to be prepared for stuff to go wrong. And so, resiliency is really the goal, as opposed to perfect security, or perfect trust, or all these other terms that can lead you to design things in a way that historically have been proven out to be very, very dangerous, frankly, and to have bad outcomes. So we're really trying to get people to rethink how you approach the design of complex systems recognizing all the complexities that everybody has highlighted. And there's a lot of work to be done. I could probably spend an hour talking about all research areas that I think are going to have to be needed to really bring to bear the full- full fruits of the vision, I think, that people are excited about with 5G. But we'll leave it at that. And I personally want to thank everybody so far. It's

been a really great panel. And I've enjoyed it. Thank you for everybody who's online and listening.

TRAMONT: Absolutely. I also want to join in thanking the entire panel. You guys were terrific. I'm sure there'd be a loud round of applause if we were in an auditorium. With that, I'm going to turn over to Melissa is coming back on, I believe, and then we're going to adjourn into our breakout rooms.

RATH: Thank you.

TRAMONT: I think that's happening? Yes, there it is.

MIDZOR: Well, thank you very much. That was an exciting panel and so many different aspects to consider and think about. You know, I learned quite a new avenues I need to go research now. So now we will go into our breakout rooms for one-on-one interaction with the panelists and moderator. Information on accessing the breakout rooms in the ISART app. Or you can just use the links that was sent to the confirmation email they received. And a reminder that after the breakouts, ISART 2020 will resume at 1pm Mountain Standard Time. Do send in the breakouts.

## 2.3 Brian Daly: Current State of Open Radio Access Networks

MIDZOR: Welcome back everyone to the afternoon session of day two of ISART. This afternoon, we will be focusing on ways that to design the 5G radio layer for resilience services. We will start with a technical talk on O-RAN and then move to our panel of experts from government industry and academia. A reminder, at the end of the panel, we will then move to breakout rooms where you will have that opportunity to interact one-on-one with not only the panelists, but also our team.

Our technical presentation today will offer a deep dive into the current state of open radio access network, known as O-RAN. Please remember that you can submit questions during this presentation in the Q&A button on the right. This technical presentation will offer a deep dive into the current state. And it is my pleasure to introduce Mr. Brian Daly, the Assistant Vice President for Standards and Industry Alliances for AT&T, where he oversees AT&T's strategy in leadership and global industry standard. His focus includes, among other things, emerging technologies for 5G and beyond, public safety initiatives, including FirstNet and wireless emergency alerts, and IoT, including smart cities annuities. And of course, cybersecurity. Mr. Daly is extremely active in guiding wireless development around the world, whose many roles include Board of Directors on the IEEE, ISTL. He's co-chair on the FCC's technological Advisory Council 5G IoT working group, and also the co-chair of the O-RAN Alliance Standards Development Focus Group, and several other key industry organizations. There is much more I could say about him. But I will encourage you to use the app and our program to peruse his complete bio information where you can learn much more about him. And now I will turn this over to our speaker, Mr. Brian Daly.

DALY: Thank you, Melissa. I appreciate the introduction. And we'll start with the slides. So if we move to slide 2, we'll jump right into the open radio access networks.

So first off, why Open-RAN? As most of you are probably aware, the goal of having open interfaces is to avoid a lock-in effect, where we have proprietary or semi-proprietary implementations, especially in the radio access network, which tends to inhibit competition among suppliers. When we look to the future, we want to see RAN, the radio access network, built on a foundation of virtualized network elements, white box hardware and standardized interfaces that really embrace what we're trying to do with intelligence and openness at the radio access network. This will allow operators to have a mix of equipment from different suppliers in the same RAN, something that's challenged today. And also allows us to bring other layers of the network into the RAR, for example, the operations and maintenance layer and provide a common OEM platform for both the core and the RAN network elements. Next slide, please.

So, one of the things I would like to make sure we're clear on is some of the terminology. When we hear Open-RAN, O-RAN and so forth, they mean slightly different things. So Open-RAN itself is the general idea of disaggregating the RAN functionality using open interface specifications between the elements. This is what we think of when we talk about Open-RAN. When we use the term O-RAN, typically, that means the O-RAN Alliance, or the specifications that are being developed by the O-RAN Alliance. This is a group that's defining the next generation RAN infrastructures and really is looking at those intelligence and openness principles that I mentioned earlier.

But they're not the only group looking at opening up the RAN. There is also the telecom infrastructure project or telecom infra project, which is another community that has more than 500 network operators and telecom companies, et cetera, that are also developing open and interoperable interfaces and technologies. And then finally, there's V-RAN, or virtualized RAN, which is implementing the RAN in a more open and flexible architecture that allows the virtualization of the network functions into software platforms. So that really tries to summarize the different terminologies that we use when we talk about openness in the RAN, as well as highlighting some of the groups that are involved within the Open-RAN development. If we move to slide 4, please.

So when we look at Open-RAN standards, 3GPP, I'm sure everybody's familiar with, is the third generation partnership project which are really developing the global 5G specifications. However, the openness of the interfaces between elements within the RAN or core network, that's really the key to disaggregating the RAN, and allowing additional suppliers to enter the market. So, the O-RAN Alliance and TIP are developing specifications that go beyond what 3GPP is developing within the RAN itself to allow this disaggregation of those elements. And these are complimentary to standards promoted by 3GPP. It's not, you know, a competition between standards, it's really taking 3GPP standards, taking the RAN that's being defined by 3GPP and advancing it such that you can disaggregate it into further functions that allow this virtualization and softwarization. The O-RAN Alliance, as I mentioned, has developed specifications for this. And the TIP project also are looking at that. If we move to slide 5, please.

There is also the O-RAN software community, which is a collaboration between the O-RAN Alliance and the Linux Foundation. And this has the mission of actually creating the software for the radio access network in the open source community. It's leveraging other Linux Foundation projects, and addressing challenges and performance scale in 3GPP alignment. There was an initial set of projects being discussed, including the intelligent controller, and we'll talk a little bit more about the architecture on the next slide, cloudification and virtualization platforms with an open central unit, an open distributed unit, as well as testing integration efforts, so that we can provide a reference implementation. Next slide, please.

This is the O-RAN Alliance architecture. We're not going to be able to get into too many details on today's session, because it does require, you know, quite a bit of effort to go through and define each one of these. But it's sufficient for this effort just to say that this architecture is based on well-defined standardized interfaces. And what we want to do is have an open interoperable supply chain ecosystem that's supported by and complimentary to 3GPP, and other industry standards organizations. And again, the goal is to use commercial off-the-shelf hardware with virtualization software that enables abstraction in the form of virtual machines or containers to provide multiple hierarchical cloud development options. Next slide, please.

As we look a little bit deeper into the logical architecture, we recall that the RAN was typically traditionally built using specialized expensive devices, had a small number of vendors which really dictated everything about the RAN from cost of capabilities to upgrade schedules, and so forth. And when we move forward, you know, with 5G and beyond, that type of model really doesn't make much sense anymore. So what we want is to create open hardware specs that any manufacturer can build to use the software running on those devices from an open source community, an open source library, and powered by the principles of intelligence and openness and make the architecture the foundation for building virtualized RAN on open hardware with embedded AI-powered radio control. So we want to bring that intelligence in, have its software defined, AI-enabled RAN intelligent controller, which really gives the heart of this O-RAN logical architecture being that 5G RAN intelligent controller, or RIC as it's known. We move to slide 8, please.

So let's talk a little bit about security when we move to an open RAN architecture. Now, when we have this architecture, we do have a more modular design. We're going to have different suppliers providing different components in the network. And actually that can enhance security because it will allow operators to more quickly replace or address network problems including suspect equipment. A more intelligent RAN also will enable operators to deploy the security capabilities closer to the network edge. As we move the intelligence into the RAN, as we move the RAN into a more distributed and software-defined, we are able to deploy security capabilities out to the edge of the network. And that'll allow us to more quickly respond to threats and shift network capacity on demand.

Now, an Open-RAN also provides the framework for all stakeholders to align on a shared understanding of the security requirements so that we can tailor those requirements at a more granular level that has been possible before. Since we have a more modular design, since we're virtualizing the elements and components on the network and providing a focus on the security

requirements, we have the ability to tailor those requirements at that more granular level that we're doing.

A RAN based on open standards also helps both the users as well as network operators better understand to align on and demonstrate successful implementation of security requirements. And the other thing to keep in mind is, in the software development, we need to introduce secure software development practices into the software community. And that could be through vulnerable library upgrade practices, software composition analysis, security tests, and so forth. We want to treat the O-RAN as a zero trust environment. And O-RAN security would be defined following best practices such as those in the NIST's zero trust architecture.

Performing a risk analysis on both the CNS plane traffic to determine if the risk justifies the cost of adding encryption to the front-haul interface, and also investigate security use cases that will be core to O-RAN. And one that comes to mind, especially when you move to a massive IoT environment is signaling storm detection and mitigation. If we can move to slide 9, please.

So what has the O-RAN Alliance been doing? They've been doing a lot of work. They've published 23 new or updated specifications recently. There's a new white paper that came out earlier this year on use cases and development scenarios which is available on their website. And they also have been looking at cloud computing platform that can host relevant O-RAN functions to enable flexible deployment options in virtualized telco clouds.

Recently, they have the second release of the O-RAN software called Bronze. And this provides some new key elements of the O-RAN architecture and updates the alignment with the latest O-RAN specifications. So in here, we have the initial release of the A1 interface policy manager and an A-1 controller, which implements the non-realtime radio in intelligent controller architecture. The near realtime RIC is updated to the current E2 and A1 specifications with five sample x apps. And the initial controlling data, low and high speed contributions and support framework and integration between the DU and the RIC with E2 functionality and subscriptions support has been released as well as traffic steering and quality prediction use case leveraging the E2 interface data ingest pipeline. And finally, OEM use cases that exercise health check call flows in the near time RIC and it's O1 and A-1 interfaces.

I'd also encourage everybody, there's an O-RAN virtual exhibition, which has demonstrations of O-RAN-based technologies, and the link is provided on this slide. It's a good exhibition to get an overview of some of the O-RAN capabilities and further enhancements. Next slide, please.

Some of the deployment highlights, it's important to note that Open-RAN systems are already deployed. NTT DoCoMo and Rakuten, for example, have deployments in Japan, are very prominent examples, and major European operators such as Telefonica and Vodafone also have been active in the deployment arena. AT&T, we've conducted several demos and trials including working with CommScope and Intel to demonstrate a millimeter wave 5G Gnode-B an open fronthaul leveraging developments at O-RAN and hosted the O-RAN Alliance Plugfest where Samsung demonstrated multi-vendor compatible configuration performance and fault management capabilities of the O-RAN interface. Verizon is partnering with key suppliers to

conduct V-RAN trials as a move toward hardware agnostic solutions. And Dish just entered a multi-year agreement with Mavenir to deliver code native Open-RAN software for its 5G wireless broadband network. As noted here, 22 MNOs have announced intentions to deploy Open-RAN-based commercial networks globally. And operators, integrators and analysts indicate cost savings of between 35 and 49 percent as the main driver. Next slide, please.

The Open-RAN Policy Coalition was formed earlier this year as well. And what this will do is promote policies that will advance the adoption of Open-RAN networks as a means to create innovative- innovations for competition and expand the supply chain for advanced wireless technologies including 5G. Some of the policies that are promoted, including supportive global development of open and interoperable wireless technologies, taking on government support for open and interoperable solutions, US government procurements to support vendor diversity, fund research and development, remove barriers to 5G deployment and avoid heavy-handed or prescriptive solutions.

5G and Open-RAN security, really looking at next generation trust. The open interfaces defined in the technical specifications will provide a foundation in architecture for improving security. And of course, standards play a very important role in defining 5G security and an Open-RAN. Slide 12, please. So some of the key takeaways. Future RANs, again, are going to be built on this foundation of virtualized network elements, white box hardware and standardized interfaces. The O-RAN Alliance and other consortiums such as CHIP, they are developing solutions that are complimentary two standards promoted by 3GPP. They're not in competition with 3GPP, but using and building bond what 3GPP is defining.

O-RAN, to be treated as a zero trust environment, and O-RAN security will be defined to follow best practices. Open-RAN systems are already deployed. And adoption and interoperable solutions in the radio access network will help create innovation, spur competition and expand the supply chain for advanced wireless technologies including 5G. So with that, that concludes my talk for today. Thank you very much. And I'll turn it back to Melissa.

### 2.3.1 Technical Presentation: Q&A

MIDZOR: Great, thank you so much. That was very enlightening. I learned a lot about O-RAN and I didn't realize how many different organizations were involved. We do have time for at least one question. So this is from Pierre, who asks, going from closed proprietary equipment to the open disaggregated Open-RAN model things like switching from Apple to Android. But a lot of people love their Apple smartphones, so what is lost for one to make the decision? You're on mute.

DALY: Sorry about that. Yeah, I think it's a little bit more complex and going from Apple to Android, yes. Certainly, it's a jump in the architecture when you're jumping from, you know, a more closed, integrated solution to a more open distributed solution with potentially different vendors. I think the gains, you know, outweigh what is lost. I mean, certainly, the testing becomes easier when you have a single vendor solution. You don't have to integrate different

components together. So one can think of that aspect as being lost. But I think when you look overall, the gains that you get from moving to the open architecture far outweigh what potentially could be lost.

## 2.4 Panel 1: 5G Design - Resiliency at the Radio Layer

MIDZOR: Great. Thank you so much. I just want to remind everyone that came back to the breakout sessions at 2:30 if you want to catch Mr. Daly for more questions. So it's now my pleasure to introduce the moderator of our design panel, Dr. Tom Rondeau. He is a DARPA Program Manager that focus on adaptive and reconfigurable radios, improving the development cycle for new signal processing techniques, and really exploring new approaches and applications within the electromagnetic spectrum. Prior to joining DARPA, he was the lead developer of GNU Radio front. I encourage you again, all to use the app in the program to peruse the complete bio, not only Tom, our speaker, but also all our amazing panelists. And now I will turn this over to our moderator, Dr. Tom Rondeau.

### 2.4.1 Tom Rondeau: Panel Introduction

RONDEAU: All right, thank you. So I've got a few slides to kick us off here, just to try to frame the conversation a little bit, at the beginning here. So we're talking about resiliency at the radio layer. It's a fairly open-ended question in a lot of ways. And that's what I'm hoping to explore here is to provide some context for, or at least some way to conceptualize what this means.

So we just heard about O-RAN, which is a fantastic project that I think actually helps capture some of these thoughts that we're talking about here. And then once I go through my slides, I'll introduce—we'll go through in order to our speakers on the panel. And I think we're going to get some really interesting technical depth on the subject. So I'm going to keep it at the high level as much as possible. So we can go to the next slide.

This is, as I say, an oversimplification of the traditional, or the kind of pre-5G, sort of pre-4G cellular model where everything was very discreet. It was very nicely blocked off. You had the user equipment, which was a handset and our smartphone, you have the base station, you have the core. There's hiding a lot of details here, but it was fairly separable in a lot of the capabilities. Go to the next slide.

Another way to look at an oversimplification of what 5G and beyond cellular networks can look like. This goes back to what you heard from, I know Jeff Reed said it yesterday, Joe Evans said it yesterday, and I think Lisa said it this morning, that this is a revolution. This isn't just a small evolution from 4G to 5G, but it's looking at the world very differently. And what we're looking at here is a perspective of the explosion of opportunities from the instead of just having a handset now with the Internet of Things, this is really kind of coming to fruition. So all those different apps and services are now part of this whole space of the network. You've got multiple different frequency bands. We go from low bands and now we're opening up the mid band. We've got the high bands, millimeter wave stuff. We've got the virtual RAN. It's no longer just a box in a

base station. It's virtualized, it's much more and this is the O-RAN concept that we just heard about. And then you got the cloud-based core. So everything in the cloud is really, you know, the joke is that the cloud is just someone else's machine. But it's a lot of machines. It's a lot of virtualization of machine layer, doing all of the tasks that used to, you know, we used to rely on as, again, these individual kind of core siloed buckets here. If we go to the next slide, there's a huge opportunity.

And this is what's, I think, exciting about where 5G's going, is this growth in application space, and the demands that we're going to have for our network. AR/VR is a great promise, I love the idea. We haven't seen the killer app for it yet. But I'm sure we'll figure it out if the network is there to support it. The wearable world, again, kind of been nascent. But again, if the network is there to support us, I think we're going to figure out what wearables really need for us. Hyper localization, and I call this enhance auto, the vehicle-to-vehicle communications. All these are really cool ideas that the 5G and beyond network is promising.

Now, it does come with limitations, though. And that's the power performance scale on the y axis here. So the more that we push into the future of applications, the harder it's going to be to fit all that compute power into the power envelope of a lot of these systems that are going to be disconnected from willpower. So it's going to be a battery limited service. But what I'm trying to open up here is both this opportunity, but also this, this challenge of how much does the application space and the demands of our systems are going to come to play here. So let's go to the next slide.

This kind of brings us back to what I'm trying to propose here, which is, as we've go on through the generations of wireless communications, but you can see this very starkly in telecommunications world, we had discrete hardware components. Everything was just a brick that did something in the RF world and did, you know, process that signal. We then moved into RFICs, integrated circuits, or E6, to do a lot of the processing itself, very well - blackbox approaches still.

Now, their modems are much more software-defined. They're much more based on very complex, but very programmable, RF integrated circuits. And you've got the programmability of the modem and the radio layer. And as you push into the core, these two worlds are colliding more and more from where it used to be everything was specialized to the chip that were built very specifically for the core, to more that specialized cloud computing that that's been the past these generations or maybe generation-and-a-half.

But now we're talking about cloud processing, and again, this O-RAN as you just heard about, is starting to look more at commodity cloud processing. So now software-defined networking. So again, software is everywhere. If we go to the next slide, if you remember Mark Horowitz's, software is eating the world, well, software is still hungry. There's still a lot of space that software is coming into play here. And it's taking over more and more of our application space.

So the point of this, trying to set the stage here, if we go to the final slide here, what I just want to open up here is I like ontologies. Or this is more of a taxonomy with a little bit of an

ontological twist to it. I'm trying to think of this in terms of what we can look at when we think about resilience at the radio layer to really what is the radio layer anymore. We can go to the far left, the RF, the resilience at the left there. I'm calling them threats, which maybe that's a bit too of a DOD term, because there's more than just threats, there's just, you know, issues to deal with. But threats are intentional, somebody's actually actively trying to jam you. Or unintentional that's, you know, could just be interference, or poorly designed systems. But there's cyber threats, again, everything being software-defined these days, the cyber threats become more realistic.

I think I saw Dirk Grunwald in the audience here. So I'm going to quote him and the idea of an RF scripts kitty. But these are more easily accessible tools and devices, I'm partially to blame, having led to a new radio project where we built all the open source software to manipulate this type of stuff, you can build attacks very easily. But then you also have the professional and nation state attacks as well. What do those look like in a world where, again, the surface space is all on this programmable plane interacting with each other?

And finally, one of the things that I wanted to point out here is that hardware and software, as I said there, they're so intimately tied together and tied to 5G. There's issues with those that we have to deal with from the security perspective and to do with resilience, goes all the way back to the supply chain. Where are we getting our silicon from? Where are we getting our software from?

Configuration management is probably the biggest flaw of security in home networks, not configuring your Wi-Fi routers to have proper passwords and user locking down security configurations. So with that, I wanted to kind of use this as a way to scope what we're going to talk about because you're going to hear from our esteemed panel members, aspects and perspectives that cross this entire spectrum here, pun intended.

And while people are talking, I would really encourage—I'm seeing some questions coming already, which is lovely. I really encourage you to ask questions. You're going to get sick of me asking questions, if you don't. I really want to hear from you over the next roughly hour. So with that, Rachel, we're going to move over to Alex's presentation.

So our first panel member here is Alex Damnjanovic, comes to us from Qualcomm. He's worked a lot on cellular standards, prototyping of networks, leading Mac system design efforts. He's worked from 3G, 4G, and now he's really focused on the 5G new radio standard. And he's going to start us from the radio layer itself and from that RF aspect. So, over to you Alex. Alex, are you there?

DAMNJANOVIC: Can you hear me?

RONDEAU: Yes, we got you now.

DAMNJANOVIC: Thank you though. Do you see my slide?

RONDEAU: We do. You want to put them in presentation mode? There you go. Perfect.

### 2.4.2 Aleks Damnjanovic

DAMNJANOVIC: So, today I'm going to talk about 5G and resiliency at the layer radio layer with a focus on millimeter wave. The millimeter wave is mobilizing 5G. It's a new frontier for mobile broadband. The available spectrum is huge. It is 25 times more than what is currently being used for 3G and 4G. So, in terms of the available spectrum, which leads to higher data rates, millimeter wave offers great opportunity. We are talking about multi-gigabit data rates due to large bandwidth. We get much more capacity and because of the way from design, we also get a lower latency.

So, millimeter wave is giving us a lot of opportunity in 5G, but in order for millimeter wave to properly function or to basically provide robust performance, we need analog beamforming. So we need large antenna gain both at the transmitter side and the receiver side to overcome the path loss. So, that is considered potentially a weakness of millimeter wave because we have very narrow beam communications. And in case of high mobility, the question is if the communication can be robust.

However, millimeter wave release 16 now has proven to have—the test is proving to have a robust performance. All the beam management techniques that were developed are supporting mobile use cases. So the new opportunities that millimeter wave brings, those are the outdoor deployments and indoor deployments. In both cases, these millimeter wave deployments can significantly improve user experience. The other deployments is typically operator deployed and initial focuses on that sort of. In case of indoor deployments, we basically can complement existing wireless -services provided by Wi-Fi, and we bring superior speeds in cases like factories for AR/VR stadiums. So, overall, millimeter wave is creating value for the overall mobile ecosystem for operators, service providers, venue owners, implementers, device finance, et cetera.

So, millimeter wave is part of 5G. And in this presentation, I just want to point out that while one may consider that millimeter wave radio is not robust enough, actually, if beam management is done right, we actually have an opportunity to actually provide an extra layer of resiliency by using millimeter wave. And I'm trying to illustrate in this figure, millimeter wave due to analog beamforming actually has good jammer rejection, because of the narrow beams used for communications in this case, for example, between the g-nodeB and the UE, the millimeter wave can provide natural rejection of the interference. And this interference can be intentional or unintentional. It could be interfere or basically, could be spectrum sharing scenario, where basically, we have multiple operators operating the same end. And by utilizing analog beamforming we are able to suppress the interference and maintain the communication link.

So, in case of single beam communications, this suppression comes probabilistically with a high probability. We may claim that there will not be interference between two communications links. If, for example, we may even have a scenario where by chance, we have interference, just like

you'll see it in this figure. That scenario can be addressed with multi transmission point diversity. So, basically, if one link is interfered, a millimeter wave release 16 allows 5G—release 16 allows multi-TRP communications where a device can communicate with two different transmission points at the same time. So, this feature provides interference diversity and allows the user to maintain robust communication link with a network even when one of these communications links is jammed, either unintentionally or intentionally. So, this type of feature, due to analog beamforming, can provide the interference rejection from strong interference, because the interference rejection is that at the RF layer. Basically, we can see how these analog beamforming can be utilized to provide actually resilience in terms of spectrum sharing, where multiple communications links are active at the same time. And to conclude, this feature can also be utilized to provide additional degree of security at the RF player, because in terms of eavesdropping, it is much harder to eavesdrop narrow beam communications, particularly when we have multiple links with the network. And with this, I would conclude my presentation.

RONDEAU: Excellent. Thank you so much, Alex. So we're going to move on. I've got tons of questions for you, but I'm going to hold them until the end. I want to hear from everybody first. So next, we're going to move farther into the system design here with Andy Molisch, who's the Solomon Golomb, Andrew, Andrew and Erna Viterbi Chair and Professor of Electrical Engineering at the University of Southern California. A long history in the wireless world have focused a lot on wireless propagation and wireless system design. The research has been focused on that combination of the radio and propagation aspects of 5G and beyond networks. So Andy, if we can get your video up, and I was going to close your video down. Here, there we go. Perfect. All right. Andy, good with audio?

MOLISCH: Oh, yeah, I was still on audio. Can you see the full screen now or does it show you the preview?

RONDEAU: Yeah, we're good. Yeah, you're in full screen. Great.

### 2.4.3 Andreas Molisch

MOLISCH: Yeah. So, thank you very much for giving me the opportunity to being part of this panel. I wanted to discuss a little bit about the question of resilience in terms of problems that nature might throw our way.

And so far, Alex has already talked quite a bit about the specific aspects of millimeter waves. I want to look at it, as you said, a little bit more from overall system perspective, which includes the frequencies as well. And I guess the first question that arises is well, what is actually different in 5G compared to 4G? And even though 5G is viewed as a revolution O-RAN wireless, from a physical layer point of view, there are not really that many differences when we're comparing, for example, to LTE advanced. Big differences are really in terms of massive MIMO, as well as in the introduction of millimeter wave frequencies. So when we're now looking at the different possible error sources, we can ask, well, what is different from that perspective? But also, why

are we having such a big emphasis on resilience now in 5G? And that's really mostly coming from the applications.

So starting out with the possible sources of errors, I guess we all learned in our wireless courses textbooks about this small scale fading. And that, famous last words, I would say, is not really the main issue in 5G, as it's assumed that most of the theoretical papers also, because it can be handled fairly easily, mathematically, but there are so many small scale diversity sources, from antenna diversity to frequency diversity, temporal diversity, and so on, that this might not be the main emphasis right now. And particularly when we're looking at the impact of massive MIMO where we have channel hardening as a key effect small scale fading effects go a little bit the way, in terms of millimeter waves in particular when we have a lot of cyber-dominant components, the fading depth might not be as large either. And the biggest emphasis might be actually for the transmission of source packets can be more looking at the IoT applications, because we have a reduced frequency and time diversity there.

And we can think about physical layer techniques, which we need to circumvent that as well by, for example, going back to allow the spreading techniques in frequency entanglement. Now, the bigger issue seems to really arise from the large scale fading. I actually want to say that question of resilience, I encountered that at least 15 years ago when I was at Mitsubishi Electric research labs. And one of the big questions on factory automation was that the people building the factories wanted to have five to seven times reliability.

And so, the question of building ultra reliable networks to protect machinery that might be millions or hundreds of millions worth, that is really a big factor. And I think if with a single link, it essentially is impossible to achieve this level of reliability. I think this is something that we're seeing nowadays very much in 5G, something that Alex has also alluded to, that you simply need multi-base station, or multiple access point connections to our different- to the various devices, because the shadowing due to environmental objects, and so on, is going to kill us.

Now as we're going to higher frequency wavelengths in particular, body shadowing, by person or the robot holding the device is becoming very relevant, because now we're starting to look at the spatial correlation, or the angular correlation of the shadowing. And easily, if we have multiple access points, they might all be shadowed off at the same time, if there is a big object standing right in front of the device that wants to communicate. So this is having a major impact on millimeter wave systems. And also, we're becoming more sensitive to these effects in ultra reliable low latency systems because there is really no time to correct even if with a dynamic shadower, if the shadowing lasts for about the second part. You have a requirement that the packet goes through within one millisecond, then you obviously have some problems.

Possible solutions out of this dilemma are to go to multiband systems, where we might have, for example, a low frequency system that has maybe lower database but can easily distract around obstacles as a sort of fallback solution that can at least communicate the key data while millimeter wave from it might be shattered off. We are dealing with another source of error in terms of delay spread, which of course is caused by multipack, and which can be viewed as an advantage. But now as we're getting to data rates of 100 gigabits per second or more, delay

spread might actually turn into a drawback because we simply don't have the equalizers or don't have the processing capability for ODM to handle delay spreads of hundreds of similar durations long. Beamforming and analog equalizers might be some ways of how can get around this problem.

Another new noise source that we are encountering in particular millimeter wave systems is phase noise. And of course, Doppler also falling into that category of unpredictable phase shift. And so, this clearly becomes more relevant as we're going through high frequencies, we pretty much get a linear scaling here. And we have to think carefully about what are the possible countermeasures. That's really something phase noise has not been an issue that below 6 GHz has bothered us very much in the past.

Another challenge we need to handle in terms of robustness, this was already mentioned that, of course, beamforming is a very important part, both at high frequencies but also at lower frequencies when we're dealing with massive MIMO systems. And the question now is, how quickly can we adapt our beam weights as the transmitter or receiver is moving around? This might be partly a question of how often do we have reference signals? How fast can we do the feedback? How precisely can we do the feedback? But then also, when we have dynamic obstacles, then that might be blocking out certain directions, how quickly can we actually reconfigure and completely retranslate these into different directions because our beam has been blocked?

The particles that are foreseen in NR are a little bit on the slow side. We did some simulation work together with the some- to see how fast these things happen. And there is certainly still room for further improvement and research. It could be compressive sensing could be why it's like in machine learning, in order to get a better estimate of where to put our beams.

Last but not least, the question of interference within the system and coverage. So one of the key challenges we encounter, of course, in millimeter waves is that streets that have a particular orientation might be very difficult to cover, because the waves essentially would have to diffract into the street, and millimeter waves don't like distraction. So we could think about new complements, including 3D network deployment, so that we're essentially exploiting possibility of drones as temporary base stations for balloons or satellite to complement and fill out the blind spots that we might otherwise have on our coverage maps. And we also have to consider the question of interference, which of course, is becoming critical for identity deployment, where we are now looking at something massive MIMO will provide less interference and micro diversity.

So in summary, we have a number of new challenges for the resilience in 5G, which is probably coming from the fact that we are using different frequency ranges and larger waves, but also from the fact that we simply have more stringent requirements in terms of our quality than we had in previous systems.

Maybe one last point that I want to mention is that the analysis of how bad the situation is, is also very difficult, because we do have standardized channel models for 3GPP. But those are

really only suitable to compare one system against the other. If we want an absolute performance evaluation and say, what is the likelihood of an outage with the system, then the 3GPP channel models are not suitable. And you can just imagine that if you want that outage probability of 10 to the power minus 5, then you have to have enough channel measurement to actually assess how likely is it that then 10 to the power of minus 5 even is going to happen? And if you just say that at 100 points, I have 50 [inaudible] to it. And then I guess that that's also going to be valid in detail, where the 10 to the minus 5 power point lies, then you might not be getting a very good …

RONDEAU: Andy, I'm not sure if it's just me, but I lost your audio.

MOLISCH: I still see myself.

RONDEAU: You're good. You're back now.

MOLISCH: Okay. So maybe that was a sign from above that I should stop talking. But I think you saw my summary here now on the last slide, and I'll hand it back to you, Tom.

RONDEAU: Right. So thanks, Andy. And yeah, you actually preemptively answered one of the questions about the channel models, are they relevant for millimeter wave? And I think that is an interesting challenge. In fact, you know, one of my running jokes about 5G is that it's like Star Trek movies that only the even ones are good. So what you're posing here is a lot of questions about what, you know, there are a lot of questions that need to be answered, but they need to be answered based on the needs of the application space. So there's a lot of things that 5G is pushing out there that aren't necessarily based on needs from the consumer or from the market space that applications are going to be developed. But I think that they're going to go hand in hand.

We're going to develop those applications, we're going to developers' new markets, learn what they actually need, and then your questions become relevant as far as how fast do you need to have adaptive beam for? How many beams do you need to support? You know, those kinds of— and what the fading characteristics do versus those needs. So I think it's a fascinating way to frame the problem that I think really will help us- these are the answers that 6G is going to require from us. So thank you. So more on that later.

But let's move on to our third speaker, Kumar Balachandran who's a wireless communications engineer with Ericsson. He's got a long history of work in all areas of mobile communications stack, including the physical layer, signal processing, radio resource management, and spectrum sharing, protocol design, and systems engineering all the way from 1G through now 5G. He is also an active member with the WInnForum and serves on the FCC's Technology Advisory Council. So if we can get, Kumar, your video and audio up, I'll hand it over to you.

BALACHANDRAN: Yeah, can you hear me?

RONDEAU: Yes.

### 2.4.4 Kumar Balachandran

BALACHANDRAN: Okay, great. So I think to start with, we like to think of the entire problem of trustworthiness, you know, from a systems viewpoint, and to look at resilience as one aspect of what we need to consider going towards trustworthiness.

It might be a good idea to just step back and define what we mean by trustworthiness, right? In reality, a system's trustworthiness is really composed of a complex and holistic view of the integrity of the system. Now, the reality is that these views of system trustworthiness actually cover non-technical areas such as business processes, customer appreciation, the actors in the ecosystem, as well as regulatory dimensions. There's no doubt about it.

But it's very important for us to gain control over the technical aspects of the system that can solidify the attitude of the system with regard to specific requirements. So, the technical basis for trustworthiness in a system consists of those aspects of trust, that are derived from measurable or a testable evidence of compliance to requirements on aspects like security, reliability, privacy, availability, safety and resilience. And, you know, in the systems view that I have up on the screen, you can see that this is actually a process that spans all the way from development, which starts from standards development, to R&D, you know, and various aspects associated with it. Possibly regulatory requirements as well get into it.

The deployment and configuration or reconfiguration of the system, both of these are sort of related to each other by supply chain aspects, as well as continuous integration and continuous development processes. And finally, there's the operational aspect, which is really important, which is that you have to have enough observability in the system, by means of measurement, the ability to analyze what's going on, and to detect anomalies and respond to them. And basically, the idea is that now you have this threat and risk landscape that is acting on your system. And this is constantly changing. And you have to derive some sort of a composite idea of how your system is behaving at the top side.

Another way of looking at this picture really is using some sort of a trust stack, where you look at, you know, trusted nodes and products right at the bottom layer of the stack, and then you go on to a trusted network, followed by, you know, operational trustworthiness. And finally, you know, how much you trust the business aspects of what you're providing. We can go to the next slide.

So we really like to look at resilience as something that is derivative of the availability of the system on the network side as well as the result ability that you have. And this has implications for the physical layer just as well as, you know, other locations in the network as well as other layers of the stack. And, in 5G, you can look at approaches to this phenomenon that we call n-RAR using techniques like node pooling.

You know, one aspect that really comes out of this is the fact that, when we justify the development of a new generation, we're really looking at traffic projections, or use case

projections and then saying, "Okay, we really need so much spectrum to handle the number of users and then amount of data that needs to be carried in the system."

But while you want reliability and resilience, a lot of it depends on how much headroom you have. So it really depends on how much abundance of resources you're able to add to the system so that you can trade off coverage and system capacity towards establishing the kind of resilience that you require in your system, both to intentional as well as unintentional threats.

And of course, there are new 5G core features like network slicing and, you know, virtualized network functions and service-based architecture, et cetera, which each provide certain facilities, but the way you use those facilities to achieve the basic principles of enabling trust in your system and resilience in your architecture is important.

Now, a physical layer resilience is really aided by design for reliability. And this means you have to design for coverage. In 5G, we have this notion of a lean design for control and signaling channels. The robustness of the signaling, and control channels are much greater than what you have for traffic. We have the ability to deploy spatial diversity with MIMO, beamforming, densification of networks, et cetera. And these are all tools available, again, that you can use towards creating, you know, a resilient design in your system.

Now, of course, every time you add new use cases or new application, you create new threat or risk surfaces to your system. And every new performance requirement, in the sense, ends up being a potential risk. So, if you take 5G applied to critical communication needs such as industrial automation and so on, as one area then you can identify the reliability requirements and latency requirements for industrial applications as being a potential addition to your risk landscape. And you need to handle that in your design and deployment and operational strategy.

Now old risks still remain. The fact that you have to have backward compatibility with previous versions of the test standard means that you inherit some of the vulnerabilities that you have in previous standards. So for example, with NR, the fact that you're deploying NR in a non-standalone fashion initially, will definitely impact, you know, the attitude of the system with regards to the same vulnerabilities that you might be able to identify on the LTE side. And you know, new features in 5G, of course, they do eliminate some vulnerabilities. There's integrity protection for signaling since 4G that's been available since LTE. And then now with 5G, we have dynamic placement of signaling. And of course, now a lot of the signaling and control channels are dedicated, which means that you can apply beamforming to them and thereby, increase robustness.

And we have reduced the amount of dependence on broadcast and common signaling towards large groups of users. It hasn't been totally eliminated, but it's definitely been reduced. And then there are subscriber privacy enhancements. You know, the use of confidential physical layer identities, the subscriber concealed identifiers, SUCI, the independence of the paging identifier from permanent identities. And the fact that since 3G, we have had mutual authentication of

network access with the user and so on. These are all benefits that continue to improve the system. Next slide.

So, we might ask the question, you know, how robust is the 5G radiolink? And the answer to this is that, you know, physical channels can always be compromised with excessive interference power relative to signal power. And so, what does 5G provide that mitigates interference susceptibility? We have advances in channel coding that have been implemented, the use of LDPC in polar coding, for example, the use, and maybe even dependence on advanced antenna systems provides you with some flexibility. And then the signaling channels are really designed for good coverage. I mean, it takes incredible amount of interference to compromise a signaling channel.

And then the link budgets when you calculate it, they can provide you ideas about the coupling losses for each logical channel configuration, with the associated key performance indicators that are associated with it. So for example, some of the signaling channels will have greater robustness because you have access to higher antenna gain in those modes, versus other signaling channels where you made use of channel coding as a way of improving the interference resiliency, and so on. And, in general, you can also use system configuration to aid more robust design and deployment.

So, we have this, you know, we have a pretty strong recommendation to operators around the world to initiate identity handling with this concealed identifier that I talked about earlier. And for NR standalone, which I understand most operators at least in the US are very motivated to deploy quickly, network slicing can improve robustness by preventing fallback to 4G and prior generations, if the use case demands it, right? And there will be a certain compromise with coverage if you decide to do so. And of course, future releases will likely allow integrity protection for the data plane and that can be, you know, activated for certain new use cases if it's needed.

Now, there is some susceptibility analysis available in literature around jamming performance, for instance, Lichtman et al, I've given a reference in the in the slide set, if you get a chance to look at it later. One of the issues that we noticed over here is that this work really analyzes jammers operating in the energy limited region rather than the power limited region. And operationally, it's really the power limited operation that is relevant, mainly because of the level of flexibility you have in arranging signaling and in 5G that makes it very difficult for an adversary to figure out, you know, exactly where to put the interference. It takes a very intelligent adversary to do so. And in effect, the amount of power that you have to expend to completely compromise the signal is quite large.

But in reality, you know, you have to conclude the slides saying that mobile networks cannot be made totally resistant to jamming. Best we can expect us to increase complexity, improve diversity opportunities in your network and maximize energy consumption by adversaries to prevent them from compromising your operation. So for example, cross carrier scheduling and other aspects really come into the picture. The fact that you can operate over so many different frequency bands, et cetera. So to summarize, trustworthiness is largely derived from that part of

trust that originates from evidence of compliance to well-defined requirements and processes pertaining to security, reliability, privacy, safety and resilience. And physical layer resilience, especially, is derived from reliability and robustness. And it can also involve system adaptability as a mechanism, especially if you have access to a level of sophistication in the observability that you can introduce into various parts of your network. And additionally, it's achieved by a design that focuses on coverage, exploits diversity and redundancy, encrypts information and protects integrity, and generally, provides multiple diversity opportunities in the channels that you use. And it's important, very important to couple system observability through continuous measurement analysis and inference. This is an important area for application of, for instance, machine learning, because of the sheer volume of data and diversity of data available in various parts the network. I'll stop there.

RONDEAU: Excellent. Thank you, Kumar. I was with you for the most or everything up until kind of the end of the last of the previous slide. I think you're right, it's a system perspective, we have to look at the whole thing together. But I think you're overestimating the sophistication and intelligence required to disrupt the wireless network. I think it's a lot more susceptible than what you showed there. And we can maybe debate that a little bit later, give us more details, but that's one thing that that I picked up on that a few of us in the software radio worlds have lots of ways to cause havoc if we really wanted to. But otherwise, I think you saw Kumar kind of sits in the middle here looking over the entire stack. So let's move a little bit further into the system is in the core itself. We have to Pam Patton, and get her up. So she's a senior communications engineer at the Johns Hopkins University Applied Physics Lab, so probably should be referring to as APL. She's a technical lead for the 5G wireless communications lab, looking at networking architectures, virtualized cores. This extends from her previous experience with 4G LTE, both at the lab, and many years of experience in wireless communications for Department of Defense. So she's going to talk a little bit more about some of the key vulnerabilities that she's looking at for 5G.

### 2.4.5 Pam Patton

PATTON: All right, thank you for that intro. I'll just go ahead and go to the next slide.

So this is just to give you an idea of like where my brain is at and why I think about 5G the way I am, and some of the problems. It's mainly from the point of view of our customer set at Johns Hopkins University Applied Physics Lab. So we're a university of affiliate Research Center. And we have, you know, six pillars of focus in terms of communications within our asymmetric operations sector. The first three are nuclear command, and control communications. We look at satellite communications, and then cooperative engagement capability in data distribution systems. And then the next three is where we really look at it, this is where 5G comes into play is looking at the senior leader communications and how do we secure communications in critical missions? And cellular is very good tool for communicating on the move, and how do you make that more resilient and more secure?

We also have in the next pillar, special users. You can look at that tactical users military, how can you tailor cellular systems to meet the needs of those special users.

And then the last pillar is advanced communication technology development. And this is how we look at 5G from the point of view of software-defined radios, you know, looking at those new radio open source. And some of those custom software-defined radios and how do we use 5G in different ways or different parts of 5G to meet the needs of our sponsors? So this kind of gives you an idea of how I'm looking at 5G for this panel. The next slide, please.

So this kind of sets out in terms of, you know, our focus on RAN. So a majority of, if you look at the 3GPP standards and the technical reports that have been coming out for release 15 or early 16, a lot of those security features are focusing on the network side, rather than looking at the RAN side. They focus on integrity and confidentiality and authentication, which is very important.

But we also don't want to forget about the effects of interference, intentional or non intentional, that will affect the resiliency of – again, this is a whole system, right? So you affect one part and affects everything. In order to protect one part, you need to put security in all the different parts of that network. So how do you address that RF interference? Again, looking at those specifications, mainly 33.5, 501, is more on the architecture, looking at those interfaces between the F1 and the E1 interface and those are within the RAN. But that's more than on how do you protect the protocols within the RAN for your integrity protection, and against replay in confidentiality.

Then if you look at the technical reports, specific to release 16, there's a study on 5G security enhancement release against false base stations. And again, you know, that was mentioned earlier, this is a known problem since as long as cellular has been around, obviously amps. You just need an FM receiver. But once you got to GSM or 2G and above, you know, these false base stations are becoming more and more easy to reproduce. Now they're really cheap hardware and really cheap software. So you see a lot of the base stations, but pretty soon probably we're going to start seeing UEs that are going to be emulated on the software defined radios. And then how do you address a UE that you don't trust rather than how do you trust a base station that you don't trust? Let's go to the next slide.

So, I figured I would frame this around a specific use case. And like I mentioned earlier, that use case of an uplink or an untrusted UE. I'm glad Brian Daly went before me so he can describe a little bit more detail about those O-RAN interfaces. And what I have here with those blue arrows that are pointing up in between the central unit, distributed unit and the radio unit, that's kind of where that that E2 interface from that O-RAN diagram that has that near real time RAN intelligent controller or that near real time RIC. How that can be put into play to make this RAN over the interface more resilient by responding more quickly and autonomously rather than sending, you know, key performance indicators back to a centralized OSS or BSS, or some sort of management plane, have that base station, or that RAN radio network act independently, based on what they see at those different points.

So in this example, you have these rogue UEs machine type communications or IoT, that are flooding, maybe one or a couple of towers. You know, you see a lot of security papers about IoT, and you know, refrigerators being taken over and toasters taken over to take down Netflix, or some other content delivery network. But in that process, if those devices are geographically located in the same area, they can also flooded the RF with too many radio channel requests or like a rash attack type of scenario. And in that case, they're taking out not only, you know, the content delivery network that they're they targeted, but they're also targeting or taking out other users.

So how can you use that real time intelligent control plane to look at that data over time and do some, you know, analysis, whether based on like machine learning, or artificial intelligence algorithms, to look at this traffic, and then see at the RF level that, "Hey, there's something unusual happening," rather than waiting until all that data gets processed into IP packets and then sent back to the core that then you have to do your intrusion detection and filtering, when that data has become overwhelming.

So moving that threat detection to the front through the RAN can also make your network more resilient at the OTA layer. And this architecture doesn't rely just on O-RAN. If you look at most of the 5G radios that are coming out, whether they're separate cloud-based processing units, or they can be separate cards within a chassis, they still have those F1 and E1 interfaces, and you can still monitor the RF level or layers for traffic and anomalies at those different points within the processing chain. It might be within a backplane within a single chassis, or it can be distributed. So that was just a really high level, but I just want to put out, you know, a possible use case of how that O-RAN could be used for increasing resiliency on a 5G network specifically. And I'll hand it back over to Tom.

RONDEAU: Alright, thank you, Pam. What comes to mind with this one is, you know, you and me are coming at it from a fairly national security and defense perspective. Whereas a lot of the KPIs in the specifications are going to be commercially motivated. So your example here, you know, it's interesting to start thinking about what are the risk mitigations and the attack surfaces from the national security versus commercial, how do they intersect, where do they converge? And therefore, what's the role of DARPA, APL to help understand those if we're going to use this for national security purposes? So, fantastic way of thinking there. Okay, great. So we have one speaker left. Now we're going to bring him up now [Mr. Serge Leef] So, he is a career manager at DARPA's Microsystems Technology office. And I used to be in that same office together until I moved to STO. But so he joined DARPA from Mentor Graphics, where he's a vice president of new ventures. He's been running programs at DARPA related to supply chain trust and assurance. Also some open source design tools for better EDA, so basically, chip design and building. But he's going to focus on the supply chain and the 5G world for us now. So, Serge?

### 2.4.6 Serge Leef

LEEF: Thank you. Can you guys see me?

RONDEAU: Yep, you're all good. Just put it in full screen mode if you could?

LEEF: I'm not the one controlling that.

RONDEAU: Rachel. And …

LEEF: Maybe you should hit enable editing and then go fullscreen.

RONDEAU: Yeah. So, John's going to begin

LEEF: Yeah, yeah. Thanks Tom, for the introduction. So I focus on PDA and computer architecture type of programs and hardware security. Is my video up or not?

RONDEAU: Your video, you are up. I think we're still working on trying to get the slide presentation. But I encourage you just to keep going so we can start …

LEEF: Should I try to share my screen or?

RONDEAU: Yeah, why don't you go and try to share your screen. If it comes up quickly, we'll move.

LEEF: Is that visible?

RONDEAU: It's coming, perfect.

LEEF: Okay. Anyway, so, my …

RONDEAU: One second. It's cut off. It's not showing us the full thing. So I wanted to escape. You know what, if you can just minimize like the bar on the left, let's just go with what you got here. And then let's just keep moving.

LEEF: Yes.

RONDEAU: I think that'd be good, yeah.

LEEF: Okay. Thanks, Tom. So basically, what I wanted to talk about here briefly is the program called AISS, automatic implementation of secure silicon. And while the original plans behind this system were not specific to 5G, but the intent was to look at securing edge nodes in general.

So edge nodes, whether they connect to Bluetooth or Wi Fi, or 5G, are all sort of part of the scope here. And so, the objective of the program is to automate the inclusion of scalable defense mechanisms into chip designs to enable security versus economic optimization. So if 5G is truly pervasive, then it can be compromised not only at the network level, but obviously at the edge or in the data center.

And so, the chips themselves that are used to implement data center or the edge node is what we're thinking about how to protect. And so, in hardware security, there is not a single solution,

because all the security strategies come at different price points. To liken this to, you know, real life example here, sometimes putting alongside declaring our affiliation with a security company still is enough to dissuade attackers from hitting your house. And then in some cases, you know, even Fort Knox defenses are not sufficient to discourage those kinds of attacks.

So in a case, what we were trying to do is we're trying to come up with next generation design tools that incorporate security, or chips right into the design implementation flow. So there are three prongs here. One is on-chip security engine. And on-chip security engine is a component that we're adding to any chip that will essentially allow enrollment authentication provisioning, to ensure authenticity of a particular device. But we can also monitor execution and enforce security policies as the chip runs. We also are working on tools that would be used during the design process to secure the designs. We can obfuscate certain parts of the chip so that it is resistant to reverse engineering. We can watermark pieces of logic that are used to put the chip together or IP. We can try to do simulation of possible side channel attacks and other kinds of attacks. And we can analyze threats and vulnerabilities. And then, to put all of this together, there is the automated integration process that occurs. So which is essentially system synthesis.

Then here, we need silicon platforms, generators, interconnect and link to optimize all of those things together. So, you guys largely come from software, so if you look at my next slide, I'm sort of ignoring the software side threats, because it appears that more than enough effort and expense is going into those into addressing those threats. And the next level of cybersecurity that are more cognizant on my team is the hardware-software interface.

And there, DARPA in general, and MTO specifically, has activities in this area to protect the hardware-software interface. What I'm focusing on is specifically hardware security. And hardware security falls into these four categories that we're addressing. One is, side channel attacks. This is where an adversary tries to extract secrets from the chip using physical communication channel, harder than what was intended to the designer. And here, we're making relatively conservative assumption that attackers are actually able to listen to what our chip emits during execution. So in other words, this assumption forces us to build more protection strategies.

Reverse engineering is another attack surface that we worry about, which is extraction of algorithms from illegally obtained design representation. This could be a chip that's sliced into layers. And then we assembled using rather invasive techniques, or somebody simply walking out of some building with design files.

Supply chain attacks are a big thing as well. So here, we worry about cloning, counterfeiting, recycling, free marking of the chips, and then representing them as genuine articles. And here, the assumption we're making is that attackers can manufacture perfect products. That means our defense has to be robust enough to deal with that.

And then malicious hardware, this is also referred to frequently as hardware Trojans. This is another attack surface that we need to protect, and that is insertion of secretly triggered hidden disruptive functionality into the design. And here, we're making assumptions that the attacker

successfully inserted malicious function to the site. And so, our defense strategy sort of starts from there. So, why are we doing this? Why are we trying to help with this? So huge merchant cybercrime companies like Intel, Broadcom Qualcomm, they already have huge investment in hardware security. They have large engineering organizations that are working on this solving their chip level security issue is critical care about for them.

And then on the other side of the spectrum are the systems integrators. So people who create IoT edge devices connected to the web and deliver some kind of practical application benefits, so like security or fitness, or intelligent locking of doors. And so, those people really don't have any interest in security today, because we have a very short time to market, and it's not an in-house competence. Between those two are other constituencies like, let's say, semiconductor and system companies. And these are companies that recognize the existence of vulnerabilities, but do not have sufficient expertise or economic machination to do much about it.

And then there are defense contractors. They typically possess deep but limited expertise. They do it more as an art than science that is unevenly applied to those designs.

So with AISS, we target the latter two groups. And we figured if we solve their problems, then we can make a value proposition to large semiconductor companies that they don't have to spend quite as much effort to make their chip secure. And we can make an argument to system integrators, that inclusion of security, and this pervasiveness of the design comes with limited costs.

So, what we're trying to do here is actually do system synthesis. We're trying to automatically generate a chip that implements all the functions necessary for a particular application. And since the late 80s, we've been able to synthesize just like this, and optimize them on this performance versus size curve. And so, that's been approximately the technology that's been used from 1988 until roughly the present. With AISS, we're trying to add the notion of optimizing for power, and the notion of optimizing for security. And within security, we have actually four attack surfaces.

So in essence, we're trying to transition here from two-dimensional optimization to seven-dimensional optimization in order to come up with a design that represents an ideal set of trade offs, which is chip economics and security considerations.

There are some challenges here. Like for instance, we don't really know how to quantify security, we do not know how to rapidly estimate how one architecture is more resistant to attacks than the other. And of course, the multi-dimensional simulation is a significant scientific problem. So, the way that the AISS addition to the work is that the starting point is a platform, which is vertically-oriented aggregation of parameterizable IP blocks, and then the designer essentially supplies the importance readings to each of the parameters.

So how important is performance, how important is size, how important is power, and then how important is it to defend against particular attack surfaces? And then, what the system does is it goes through combinatorial optimization to explore huge architectural spaces. And for each

one, it estimates the level of goodness as expense measured against the cost function provided by the designer, and essentially optimizes for performance, size, power and security.

So, you know, how might one think about this? So you could think about this particular application that I listed as examples that, for example, lawn sprinkler performances really don't care. Size is sort of important if you're going to do volume. Manufacturing power is really important because you maybe want to run this for years on single battery. Security is like, who really cares if somebody knocks off the lawn sprinkler. But if you think more closely, below how to expand the security equation here, you could say, "Wait a minute, there is actually an attack surface here, which is a supply chain attack surface. Because if my design is successful, somebody could actually clone or counterfeit my chip. And so, no, I do care after all about supply chain attack surface. So I'm going to give it a nine. In response to that this system optimization, system optimizer will create a different architecture that has supply chain attack resistance capabilities."

Obviously, if you're thinking about guided projectiles, or routers, or automotive vision control applications, the cost functions are quite different. And in fact, for 5G clients, they may be dramatically different from what I have put into this example. And for switching and networking systems, that could be something else entirely.

So, anyway, I don't have an official summary slide, so I'll leave it right here and say we are working on security chips and these chips are going to end up in your ecosystem either the client or data center or network fabric, based somewhere. And so, that's—so, security of the chips in that whole chain is important. And we are trying to move the sense forward in this area quite a bit at DARPA.

RONDEAU: All right.

LEEF: Thanks for sharing. Yeah.

### 2.4.7 Panel 1: Q&A

RONDEAU: All right, so we only have a few minutes left, but I'm going to take a little bit more time before we go into our respective rooms afterwards, because only at least a couple of questions in here. But of course, this is just what you get when you have deep thinkers spending, you know, their time on trying to talk about a very complex subject. So first, there was the most popular question that we got, and I like it. The answer is easy. So, I'll ask it and then don't want to think about the depth of what the question is really asking here about how do we do it?

So with the behaviors of software-defined radio, cognitive radio, and then the new radio, et cetera, being increasingly controlled and perhaps dominated by software, there seems to be a need to revisit the equipment certification process, possibly expanding the process to address software. Any thoughts regarding reengineering equipment certification process?

I feel like the answers like we're all going to say yes to some extent. But let's try to dive into what does that actually then mean? And also some of us who went through the software-defined radio certification nightmare in the FCC about 15 years ago, and how bad that turned out, I would say. And the how ineffective it turned out to be, I think. So, do we have any thoughts on reengineering certification process given software as a dominant factor? I'm just going to keep opening it up to anybody in the—participating here?

BALACHANDRAN: My own view is it might end up being a lot more difficult than we imagined, because software demands to be very flexible. And if you want the flexibility of being able to change your features and functionality on a rapid deployment basis, then it becomes quite difficult.

RONDEAU: Yeah, as people maybe are processing this, one of the things that I forget who it was now. May have been Jeffrey that I was talking to. Somebody brought up the fact that, you know, hardware, eventually is limited by physics. Software is limited by theories of computation and numerical processing. We have the halting problem. So math is not complete, it's not consistent, and it's not decidable. From those three principles, software is by its very nature, dominated by the potential- potential flaws and flaws that can be almost impossible to sort out to the nth degree. So you're focusing now on this space that is this massive opportunity of processing and mathematics and how that translates itself into the physics of processing electromagnetic waves coming with all those challenges. Any other thoughts?

MOLISCH: So I would maybe argue that there are two separate problems. One is to make sure that the software that the system is doing what it would be supposed to be doing and functioning properly. And the other one is to avoid that it's doing something terrible. And that that maliciousness, at least when it comes to the RF emissions, because one could think about mandating certain emergency brakes, that could be tested in a relatively simple way, that there are interfaces that we're saying, "Okay, imagine somebody has hacked into the system, we're getting now the order to send out 100 watts per 10 MHz, 1 GHz bandwidth. Will the emergency brakes work properly to prevent that? And maybe that's a small enough space that that can actually test it. But I think if we're looking at all the millions of billions combinations of what could, in principle, happen in a base station and all the software that's running with it, and to ensure that every single possible use case, but tend to discover in such a certification process. I think not being a software person, myself, but it just seems to be a very difficult notion.

BALACHANDRAN: You can to a certain extent, I suppose, introduce traceability into the system to the extent that any software that you deploy is properly attested, and is, you know, associated through some chain of trust to a hardware route or something like that. The other aspect of it, of course, is that you can do the same thing for configuration changes that affect the operation of the system. So, if there is a command to get your radio to do something, you have a very clear ability to trace who did it and when it was done and how, you know, how it was detected?

RONDEAU: Yeah, I think interfaces is really interesting and I think the O-RAN Alliance and the work that they've been doing, and as we've even in the DOD, we've been focusing so much more on open interfaces. I'm a big believer in open for software, my background and everything,

but open interfaces are probably more important because it allows you to have constraints, you know, mechanisms built into how things communicate between devices. It's more of a pluggable architecture. What's happening inside of that could be opaque or you work on, but as long as you're kind of gatekeeping between the systems, there seems to be some value there as opposed to the huge problem of just trying to solve the whole software problem. So, I think one last question was a multi-parter, really, to Kumar, but I think other people will have some opinions, I think, Pam, for sure. This was about—it's about KPIs, key performance indicators. So, the operational system capabilities, we just talked about the names of 3GPP, standardized key performance metrics or KPIs. There's no coincidence that KPIs are used by wireless carriers to measure performance and keep their networks running smoothly. In a zero trust cellular communications environment, that is like a physical and virtual RAN of the core network, what types of KPIs describe trustworthiness? And is something called like, considers trust the unnecessary part of a wireless network?

BALACHANDRAN: So the short answer to this is, when I presented it, I didn't really intend for the KPIs to be limited to what 3GPP defines. And one of the aspects of what's happening with 5G and with the system architecture is that we are moving more from a telecom-centric approach to building systems to a more IT centric approach, if you want to look at it that way, because of all the virtualization and the separation of software and hardware, and, you know, the ability to centralize control and create action at remote locations, right? So, a lot of the wonderful work that NIST has done, for example, with all the cybersecurity recommendations and so on, they're still valid. And we really have to, you know, take our learnings from different sources, and try to integrate it into this composite that I talked about. So that you have an ability to continuously adapt and develop the system towards, you know, creating the right ability—you know, right level of trust that users and governments and operators can have in the system.

RONDEAU: Yeah, and I appreciated your presentation of the chart that showed that was basically a DevOps cycle. So that comes from having an IT perspective on all of these things. Pam, I do want to pull you into this because, as I said, you know, there's different motivations here between governments and DOD versus commercial and the KPIs. When you read their motivation, are very related to the labels of the commercial drives behind this. And they tend not to, they've lagged at least. I don't want to disperse them too much. But they've lagged in security and trust and the things that we in the DOD take, sometimes over seriously to the detriment of actually getting into solutions field. So, how do we balance this from your perspective?

PATTON: Yeah, that's a good point. Because, you know, with security, there's cost, right? And so, when we want, you know, a network to be really secure and really resilient for those edge cases where, you know, those machine-type devices go crazy, or some, you know, some sort of flood signaling or flood attack happens on that network, how often does that happen, right? So the probability of these events happening and how do they affect the overall economics of that network, is it worth investing on a commercial network? Obviously, for a government-owned network and private networks, it's like, "Hey, let's throw as much security as we can at it." But

also in terms of the KPIs for trustworthiness, I've never actually thought of it that way. Because I always think of key performance indicators as something real time telling me what's happening right now. I'm getting this many RRC connections failed, this mini-handovers are failing. So in terms of trustworthiness, I think of that in terms of design requirements or key performance of the design or key parameters of a design that would make something more trustworthy? I'm not sure if during the operation of a system, could I say it's more trustworthy right now than when it's loaded with traffic? So I'm not quite sure how to answer that question in terms of KPI trustworthiness. But yeah, there's definitely a balance in terms of security, cost and usability too, right? If your algorithm starts detecting a flood of traffic and thinks it's an attack, and it's actually just a bunch of people stuck in traffic, and they're all trying to make phone calls. Now, they've all been denied, unintentionally, by the system. So, you know, there's all those trade offs between security and how you apply that. But I definitely see in those private networks in those government-owned networks, that the security is going to be much higher and much more flexible. The commercial networks, again, it's that, you know, what's the likelihood of it happening? And then what's that cost?

RONDEAI: Yeah, I think it's a really provocative, thought-provoking. It's thought-provoking question about what does trustworthiness mean, what does trust mean? So, I'm not surprised we didn't have an answer. But good thoughts, at least, from the discussion. I want to wrap up, but I think right now, so we can get on to our breakaway, whatever they're called, breakout rooms.

But I do want to wrap this back to Alex and put you on the spot for a second because I thought the way that I bookended our discussion here was starting at the RF layer and going back into the hardware in the supply chain with Serge. But the thing that always strikes me, and I've talked to the folks at Qualcomm a lot about what you're doing in the millimeter wave, it's fascinating, how much more though, as even though I posed it as an RF problem, the nature of the network, in order to manage the beamforming, and the multiple base stations required to maintain that connectivity. It is again that merge of the radio physics and the antenna physics, but with the networking control and the algorithms required behind there. I think it's a wonderful opportunity to start breaking outside of our boxes, as I were taught, as electrical engineers, you do information theory, it becomes theory, you know, to thinking about this as we really have to be thinking about the whole system. So can you give us more about what Qualcomm is thinking about in terms of aligning itself with the networking functions to solve some of these physics problems?

DAMNJANOVIC: Well, I agree that it's a complex problem, and it has to be looked at, not just from the physics point of view, but also the network, as to it's a critical component of millimeter wave system beamforming. So, what analogue beamforming provides an advantage to basically compensate for the path loss, the beamforming is critical to actually to be maintained—the beamforming has to be maintained during the ongoing communications. And mobility plays here a significant role, where we can kind of get in and out of coverage fairly quickly, and we get blockages and so on. So in that regard, very fast and robust beamforming together with diversity that we talked about multi-transmission points. So we should be able to connect to

multiple points and to densify the network so that the UE always has, basically, a point in the network to connect to and to minimize latency when we hand over from one beam to the other.

So, millimeter wave can actually work pretty well. It can provide huge data rates. But one has to be very careful about the beamforming and the ability to achieve diversity in this network. So that will make millimeter wave more useful, because of that potentially provides for high data rates. And on top of this, it will have network sharing—I'm sorry, spectrum sharing. So basically, because of the robustness that millimeter wave offers, we can now maybe deploy multiple operators—allow multiple operators to deploy on the same spectrum in the same area, and just like on beamforming for simultaneous communication. So that's yet another layer of efficiency that millimeter wave can bring.

RONDEAU: Great, thanks. Yeah, if we were in person I would we get there sort of whiteboarding some thoughts here about really trying to nail like get into the depths of the questions here, that really the math problems that are presented with all of this. But unfortunately, I do, I'm going to close this out right now.

I want to leave us with two questions. We don't have time to answer them. But I want to kind of prep them for maybe the breakout sessions or just to get people's thoughts. I think they are interesting. The first one was specifically to Serge. But I think it's a general problem that we just talked about in the KPIs. So, how is trust security measured for a circuit design? So, I think we already were talking about it from the trust in KPIs but also trust in circuit design. Just trust in general, is an interesting metric that we can think about.

And then another question was, are companies already making 5G-related chips, keeping security functions in their design criteria as delivery here? So again, I'm not going to ask for an answer for that one. But I think, you know, just kind of thinking about it. Serge, maybe since you wanted to speak, I'll give you 30 seconds, and then we'll wrap it up.

LEEF: Yeah, Tom. So basically, there are metrics associated with each attack surface. And so, it's not a simple answer. This is the security of this chip equals excellent security of x chip equals y. So, for example, for reverse engineering attacks, how many combinations of G's would it actually take to crack particular logic application, logic blocking scheme? You know, is it 10 to the power of 27, or 10 to the power 45? That's a metric. In such attacks, also the degree of emissions visible outside the chip is a metric, as well. As to whether 5G makers are employing any of these techniques, I would say that, at this point, the truly advanced on chip security methodologies are only used in the very, very largest merchant semiconductor companies. And just about anybody outside of those two or three, I would say, is not using the most advanced technology available.

RONDEAU: All right. I appreciate that. A wonderful discussion, everybody. I really appreciate all your thoughts. It's a very complex surface here. Cyber, what is cyber, what is security, what is trust, I think are really interesting questions that we're all really getting into. But we'll leave it there. Thank you to the audience for putting up with me taking over 40 more minutes of your time. And I'll end this. I'll pass it over to Melissa and she'll lead us out to the breakout rooms.

>> So thanks, Tom. Great panel, you guys. I was really hoping to see sort of a dust-up between the two different camps on how effective beamforming was at resiliency and protection. I'm hoping, Andy, I would love to hear your comments on that in your breakout panel. But for now, we will all go out to the breakout panels for one-on-one interaction, and O-RAN speaker. Remember, you can use either an app or there's also links in the confirmation email that you received. And I will see you guys over in the breakout rooms.

# 3. DAY 3: AUGUST 12, 2020

## 3.1 Andrew Thiessen: Introduction of Technical Presentation

THIESSEN: Welcome to the third day of ISART. We really hope that everybody's enjoying the conference so far, especially given that we're trying to come as close as possible to a face-to-face experience, given the situation I think we're all in. So we appreciate your patience and your participation.

Today, we have two segments that we're going to cover. The first is covering the technical side and policy aspects of securing and making more resilient, the technical side of 5G system during the deployment process. And the second is how monitoring and data collection can and should improve the valuable input and feedback into the design, deployment, and operations to improve the resiliency of the same network.

Please note FCC auctions 105 and 904 are ongoing. As such, participations—participants in the meeting may be subject to the FCC's strict anti-collusion rules. So accordingly, these discussions—during these discussions, there can be no disclosure either directly or indirectly, of any of the company's auction bids, or bidding strategy, or post-market auction structure—post-auction market structure.

So some logistics. Our virtual ISART 2020 as you know is structured into two, two-hour blocks each day. The organizing committees work hard to find ways to incorporate the tools for the real-time interaction among the panelists, with in-depth plenary talks, high interactive Q&A, and opportunities for networking and conversation in the breakout rooms. Please feel free to ask questions online during the presentation of panels. Remember to spell out any acronyms please. Also, look at the questions already in the Q&A section on the right side of your screen. And please vote, if you'd like to hear an answer to a particular question. The moderators will work hard to pool questions based on the interest level and will also work to try to take the unanswered questions throughout the breakout rooms, so that everybody has an opportunity to hear an answer to their question. The last half hour of each two-hour block is reserved for those breakout rooms. We hope the breakout rooms, basically what we're trying to do is we're trying to build the same experience that you'd get if you could go chat with the panelists during a coffee break. So kind of keep that in mind. We're really looking for a kind of casual interaction there.

So as I said, after each panel concludes, the panelists and speakers from that session will exit the BlueJeans events platform and head over to the BlueJeans meetings platform for their breakout room. I'm reading Melissa's notes yesterday, and she says, "Fingers crossed." So there you go Melissa, fingers crossed. For those of you able to download and access the brand new ISART app, we encourage you to do that. All the information and links needed for the breakout rooms are in the app. For the non-app users, the ISART confirmation email sent this last Friday has quick links that contain the link and the phone number for the breakout room. Room hosts from the conference will be there to help if needed. So if you run into any kind of problems, reach out

to the conference services staff listed in your confirmation email. A quick technical note, the code to access the main sessions on the BlueJeans event platform is the same each day. So if you do have issues with the link, please try the next comparable link. But also, again, the ISART app will also allow you to reach out and connect with each other. By default, the only information that anyone will see on the app is your name and affiliation. So if you're open to chatting with others, networking, exchanging virtual business cards, please remember to go into the app and add whatever information you think is relevant. Again, we encourage you all to use those interactive tools to ask questions and talk with your panelists and presenters in the breakout rooms. Because again, you know, we're trying the best that we can to replicate that face-to-face experience for you.

So with that, I'd like to introduce our first speaker professor Alenka Zajic, from Georgia Tech, where she's the professor in the School of Electrical and Computer Engineering. The professor has completed her BS and MS degrees from the University of Belgrade and her PhD in electrical and computer engineering with Georgia Tech. Her research interests span electromagnetics, wireless communications, and computer engineering. Professor Zajic is going to give us a high-level overview of supply chain verification problems and possible solutions offered by EMSI channels, including RF detection of malware. Please remember that you can submit questions during the presentation. And if there's time remaining after professor Zajic finishes, then we'll see if we can work through some of those questions. And so now I'll turn this over to our first speaker, professor Zajic.

## 3.2 Alenka Zajic: RF Detection of Malware through Side-Channels as a Solution to Supply Chain Verification Problems

ZAJIC: Thank you Andrew for the introductions. Hear me?

THIESSEN: Yes.

ZAJIC Hopefully, you can.

THIESSEN: Yes.

ZAJIC: All right. So I want to bring attention to side-channels, analogue side-channels in particular and how they can help us with supply chain protection and verification. So next slide.

When we say supply chain protection and verification, it implies different things to different people. So what I want to bring together is verification of the hardware. And this is one example of allegedly China using a tiny chip to infiltrate motherboard of this computer. So that's one of the things we want to check against. And the problem is that when you get fully finalized board, then it has so many components, how do you look for the intrusion? Slide three.

The second problem is firmware verification. That is the software that is activated when you are booting the system. And every phone has it, every computer has it, every equipment that you

are using in the power plant has some sort of boosting software that says, hey, okay, this is what we are supposed to do. And apparently that is not verified in any way. Slide four.

And the fourth problem is obviously intrusion of the malware or any other intrusion that happens over the network. And this is one example of how the ports were crippled by the malware that took over their network in under one minute. So how do we solve all three problems together? So the next slide.

Well, we propose to use side-channels. And the side-channel is a means of obtaining information about the software execution outside of the program intended communication. Next. So what does that mean? Can you click all of them? Thank you. That's good. So what is a side-channel? It boils down to you are not supposed to consider X as a source of information and that's what I will refer as YWNS. The next slide, six.

So the side-channels can be timing side-channels where you can obtain information about the performance of the code by observing how long something took to execute. It can be cache side-channels, whether you're looking at the micro architecture, trying to deduce something about program execution. And then analog side-channels and they can be power, EM, acoustics. You will see the new side-channel we found out. We call it backscattering or impedance side-channel. They can tell you a lot about physical aspects of the implementation. And then you can use the bus snooping or the DRAM freezing, if you are allowed to open the system that you are observing. Next. The seventh slide. And you can click all of them.

So the Bell Labs discovered first wireless side-channels in 1943. So they have been around for a long time. And they discovered it by building the telegraph. They told military it's perfectly secured. And while testing it, they realized that on the other side of the room, on the oscilloscope, they can see the—some activity that is related to the messages they are sending and they dig deeper into that and found out that they can actually decode the message. And when they told it to military, they said, "Oh, we don't believe you." So they actually put them in two different buildings and they were able to reconstruct the message. And what happened is they put a [inaudible] on it. Said, "Let's never talk about it." And it has been like that for a long time.

And then they popped up again in the cryptography community around 1980s, where the concern was about reconstructing private-public key encryption and that can be broken via side-channels. And side-channels have are very well-known in this community for a very long time. And they were mostly focusing on the hardware such as the microcontrollers that are usually new credit cards that you're using on a gas pump and things like that, where they really don't want you to get exposed. Slide eight.

So about 10 years ago we started looking into this problem and where the starting point was, can you get any emanations from the modern systems, like, you know, laptops, desktops, cell phones, IoT, and so on? And can you extract any interesting information and how far away you can do that? That – those were the first questions Milos Prvulovic and I tried to answer when we

start looking into side-channels. The other questions we try to answer is what is physically driving this behavior and how it can be used in various ways?

It turns out is that yes laptop, desktops are complex, but information still can be extracted and it can be extracted from the significant distance. So collecting all this knowledge over 10 years, so what we propose is we can help supply chain verification in three steps. On the left side, you have this called RFB analysis, which means RF backscattering analysis that we use for the hardware Trojan detection. Then we are using EME analysis for the firmware verification. And then we can also use EME analysis for the real-time monitoring of the system in the field. And today I will talk about, a little bit about all three parts and how side-channels can be used for that. Slide 10.

So let's start with RFB analysis. Still how do Trojans they're particularly nasty, because they are tiny and they're usually not activated until certain event happens, which means you need to find them—either you know the combination, how to trigger the behavior, or when it's triggered you can detect it, but it might be too late because your drone is going down. So power, EM, acoustic side-channels, they all depend on the current that needs to go through the circuit, which means circuit has to be activated in order to find it. And what we certainly call, what if we look for the impedance? That's something that doesn't have to be active and it's always attached there.

So how do you get the information about impedance? Well, you use the backscattering. You send the unmodulated signal and the state of the inverter usually has two different impedance states. There are tiny differences, but when you have a lot of transistors, you can actually detect them and the modulated signals comes back. And that way we can tell that something additional got attached to your original circuit and that we would try to detect the hardware Trojans. Slide 11.

So we looked at the AES crypto processor on FPGA, we looked at Trojans that are in a trust hub that everybody looks at, where the size of the Trojan is about 1.7% of a circuit and so on. And we try to detect those. Slide 12. And what is the idea here? The idea is that Trojans trigger circuitry small, but always active. It's much, much smaller than overall Trojan. And that Trojan connections to AES circuit changes impedances to the original circuit. Hence, we might be able to detect that through the backscattering. Slide 13. Oh, there's more on this slide.

And the—what we are trying to detect is a subcycle temporal granularity, which means you have a really fast clock. And within that clock, some things change. And for that to detect, you really need a large bandwidth that can observe many times the clock rate of the capture change. And by looking things in the frequency domain, we actually look at the harmonics of the clock and are able to defend that. Thirteen slide.

So this is the picture of how we would measure it. We are using the electric probe to inject the sinusoidal signal and then we are using the magnetic probe to collect the signal so that we don't have interference between the two signals. Slide 14. And this slide, what I want to show you is how much backscattering performs better than EM and the power. And we're detecting both dormant and activated hardware Trojans. And you can see that the green line of the power and

the dormant performs the weakest, then EM performs a little bit better, but it still has a lot of false positives while the backscattering can detect both dormant and activated with 100% accuracy. And the reason is really that we are detecting is something physically attached to it or not and we don't need the currents flowing through it, which helps a lot solve this problem. We can detect down to 32 gates, just the trigger part of the Trojan, which means we can detect really, really tiny changes. Slide 15.

We can also detect the counterfeit designs, which means if the layout changed in any way but the components are the same, we can also detect that with really high confidence. Slide 16.

So that was the RFB analysis for testing the hardware Trojans. You can do that once when the manufacturing is done, it arrives to your system, and you can do this X, Y, Z positioning and find things. People would say like, "Oh, but you need a golden example for that." Yes, and we are working on solving that problem without a golden example. One way is the modeling of these impedances. And the other one that we came up with is I can measure a large number of boards and actually cluster them into two groups of infected versus uninfected. I may not know which one is which, but I can destroy only two boards and actually do reverse engineering that way and figure out what's going on. So there are ways to solve the problem of not having a golden exam.

So let's talk about now firmware verification. Slide 17. So this is an example of the system, SEL-351S, which is often used for power systems, actually many military systems it is used. And here you have a huge metal box and you want to verify is the firmware correct? And what we discovered in testing many of these SEL boxes is that actually firmware changes without anybody notifying you. On the right side, I'm showing you the spectrum of the firmware and these lines that you're seeing here are actually the loops in the code. So even if the hardware is different, I can still say this is the effect of the software not of the hardware. Slide 18. And here we're showing you a different firmware on the same SEL box. And the results show that you can quantify them and actually you can visually see that the spectrograms of these three devices are different. So these side-channels can be used for protection of the firmware system. Slide 19.

And the last piece is the EM-based software verification in the real-time. Slide 20. The key problem here is how quickly I can detect that my network is under attack. And here we are showing the medical device, syringe pump, get something that is hard to monitor in traditional ways. Slide 21. Slide 21. We're basically we're showing the spectrogram on the left side of normal behavior and then on the right side, it's when it's attacked. And we're showing also the fact of the—they have a very specific features that are different than when the malware is actually attacked. And to make a point here, we're actually reusing the same core, then we change the things only into instruction. So these are very, very tiny changes that we are easily—we can easily detect. Slide 22.

Here we are testing it on various devices, typically IoT devices and we are showing the detection of latency and they are all under 1.5 milliseconds and we have zero false positives and 100% accuracy. So this is a very, very efficient way of detecting things. Now if you go to slide 23, I want to show you the spectrogram on the left side, you have a DDOS attack like me, right? And

on the right side, you have a ransomware. And on top of that, you have content switching between the ransomware and the application we want to run. And visually you can detect them they're really large changes. So the things that are really hard to detect on the network level because they are tiny, here when they start being executed on the processor, they're very easy to observe using side-channels. Slide 24.

So to conclude, analogue side-channels are not always bad. And understanding physics behind it really can make it as a powerful tool. There are new side-channels to be discovered and leveraging them for a firmware verification, malware intrusion, hardware Trojan detection is very, very powerful tool. And I have other applications where the side-channels can be used. Slide 25. I want to thank you for listening and thank your government for funding this research. I'm open for questions.

### 3.2.1 Technical Presentation: Q&A

THIESSEN: Thank you very much for that, professor. I appreciate that. Let's see. Let me go to my special Q&A thing here and see if we have any questions. I have one. It is, can you discuss countermeasures to side-channel monitoring, such as random emission generation?

ZAJIC: The main problem with—like if you want to really fight side-channels, you need to use asynchronous circuits, because as long as things are caught using the same power plan, there will be side-channel. You would need to make every circuit have their own power source and being clocked with different ways and with different timing and so on. And as you can imagine, that is very expensive way of doing things. The other way is to fight emanations by reducing emissions in the first place, making voltage regulators more wired so that the process of clocks more quiet, spending less power and stuff like that.

THIESSEN: Thank you very much. Brushing my question pool again. Does anybody else have any questions for professor Zajic? I'm not seeing any come in. Thank you, professor. I really appreciate that. Okay. I don't think we have any more questions. So I think what we'll probably do is we can switch over and prepare for the next panel. So again, thank you very much. I appreciate it. Okay.

So our next panel is a great collection of different backgrounds and skill sets. It's going to dive into both the technical and policy sides of 5G while looking at zero trust through the lens of deployment in government. Our panel monitor here is Drew Morin. Drew Morin currently serves as the Director, Federal Cyber Security Technology and Engineering Programs for T-Mobile. He's responsible for identifying emerging and cyber security trends and regulatory policies to improve security programs. Also, please keep in mind that the slides will be available in a few days and recordings in a couple of weeks. And so now I'm going to go ahead and turn this over to our moderator for the first panel of the day, Drew Morin. Thank you.

## 3.3 Panel 2: 5G Deployment – Implementing Secure and Resilient Solutions

### 3.3.1 Drew Morin: Panel Introduction

MORIN: Hope everybody can hear me fine. So starting off today, I want to just basically, first of all, thank you all for coming in to see what we have to present today. We're very excited. I've got a great—we have a great set of panelists here cover this topic. We're going to cover from a broad perspective. So I'm going to kind of jump right on into it and just start with a few opening comments and then each one of our panelists will have some opening comments as we go. And then in the backend we'll take questions and we'll discuss as we proceed.

So, first of all I wanted to just kind of note that what we'd like to take a look at what we're dealing with here as a carrier, we're obviously dealing a lot with licensed spectrum. And spectrum itself I mean, is just basically a bunch of frequencies. But in the licensed spectrum, represents an exclusive right to use a set of frequencies. And of course that's going to be subject to interference, power levels, and other types of constraints.

So the objective for us is to minimize the potential for interference between different spectrum allocations, that's to help ensure the availability of optimal use of spectrum bands. It's also one of the things that we do to ensure that we're monitoring what's going on in the spectrum, so that we can identify other potential interference and work with industry and government partners to mitigate those types of threats. There's also non-exclusive spectrum allocations, the idea of shared spectrum. And they have a slightly different set of rules of the road. I'm not going to go into that much detail. So I'll just—our panelists may want to cover some of that more information. But, you know, the unique challenges they're going to represent is things around the allocation of the shared spectrum, once again, there's interference and the ability to release a spectrum up for others to use when you're sharing it. So there's a lot of technical challenges around that type of spectrum as well.

When we look at 5G and when we're deploying 5G right now, one of the key factors we're taking into account is that 5G expands the amount of bands that are available and how they're going to be applied, and really how they're going to be applied to support additional use cases. Not every use case works with every band efficiently. So when we start going through that, we start looking at how we're going to deploy the spectrum. We want to ensure that we're taking into account a lot of the different aspects of threat. And specifically, we're looking at things like a jamming threat, the idea of road base stations, even the physical attack on a cell site, as well as looking at things like supply chains, we just heard about. Those types of our equipment and firmware can come into the radio side of things and the radio access network, and they can cause additional potential avenues, and vulnerabilities, and threats. So we're going to talk about a lot of different perspectives related to what we mean when we're talking about the resilience and the security in 5G deployment.

And we're going to be talking as Andy said about policy side, as well as about the actual technology involved with this. So what I wanted to start with is to basically identify that our

speakers, we've got folks who are basically within equipment OEMs, we have wireless carriers, we have industry associates, and we have government policy makers here. So this diversity of opinion is really going to hopefully help to paint a broad overview of the challenges and what has been done and what is being done and hopefully identify for you all, some areas where from a spectrum perspective, there may be opportunities for forward-looking research. And we'll be talking a little bit hopefully about some of those things as well.

So I want to open the discussion describing some of the work that T-Mobile in partnership with industry, in partnership with government, and with academia, that we've pursued specific to these various threats to the 5G networks. Many of these activities that we're associated with our primary security resilience, are further up the stack than typically the RF side and the data link layers. Examples of that are supply chain risk management. And that's where you're talking about the overview of ecosystem and how you're going to be able to mitigate 5G threats to the components and provide assurance to the components that are actually deployed within the network. Some of the examples of what we're doing today in supply chain risk management is a partnership with ADIS and the Department of Defense. We're co-chairing a working group that's looking at assured 5G as an example.

We also work with our industry and government partners in the Department of Homeland Security on the information communications task force of the supply chain risk management. There we're looking at everything from information sharing to actually threat evaluation and other types of policy and technology actions associated with identifying suppliers, and products, and services, and how to evaluate those risks to improve the overall supply chain ecosystem.

Finally, the industry and government, we also are representing various working CSRIC groups. CSRIC is the cyber security resilience and interoperability council of working groups that are hosted by the FCC and focusing on 5G. I think it's important that we …

THIESSEN: All right, Drew. Drew, I think your audio has dropped. Hey, Drew. Can you see me? I think your audio has cut out, we can't hear you. Can you try? We can—I can hear you now. Okay, we can hear you, okay. Yeah, we got you. We got your back.

MORIN: Okay. So I was—my mouth was moving and nothing was coming out. That's standard fare, I guess. Okay. So I could tell from the data that I am still being heard. Okay. So I'm assuming that we've—I was talking a little bit about the CSRIC, but I blanked out.

Just basically, CSRIC is a partnership between government agencies and industry to look at emerging trends and to try to get ahead of it and identify different ways of dealing with the resiliency and the interoperability of these networks. And one of the things we're working on in the current CSRIC, in both a stand standalone as well as standalone deployments, is there's a lot of focus on what I would call the data link, which is that connection, that authentication and activity that happens at the radio access network to the user equipment. So that's one of those areas where we are working as a public-private partnership to identify where those threats are, what are the mitigations, some of the things that are built into the specifications and standards,

and how we can improve that overall experience and overall resilience of the network going forward.

Now I want to drop into a couple other things that T-Mobile is doing specifically in 5G threats and mitigation. And one of those areas is the road base station. The idea of putting up a cell site that's an artificial cell site with the purpose of impersonating legitimate cell towers to intercept traffic for some kind of nefarious purposes, whether it's to compromise privacy information, to insert malware on devices, and other types of bad actor activities, if you will.

One of the things we did in partnership with the University of Washington and the Department of Homeland Security are the national infrastructure protection plan, security and resilience challenges, we proposed and executed a research project focused on capturing networking event logs, including control, authentication, attachment data between the UE and the base station. The UE being user equipment. The objective here was to look at this flow of data, capture the legitimate traffic, and also capture how a road base station would operate, and see if there are signatures we could identify and develop to basically create an algorithm for detection of road base stations. That research paper I'll make sure is available for your post show to be able to look at. And it may be an area where some of the researchers here might be interested in pursuing additional activities in that area.

Road base stations are a continuing threat to the attachment of the security of networks. And we need to continue to if you will, it's almost like spy versus spy. We need to continue to improve our ability to detect and mitigate those quickly in the network.

Another area of public-private partnership is the current ongoing work at ADIS around wireless emergency alert. And this was actually a weird exploit. It was uncovered by a university of research, University of Colorado researchers. And they brought this up to—wrote up a research paper on it. The FCC convened a workshop with participants from industry and from academia to discuss this vulnerability and develop an action plan for mitigation. A working group was established in ADIS and it has been working towards addressing the potential risks around this with vulnerability with report expected to come out by the end of this year.

So those are some of the examples of where T-Mobile, as well as industry public-private partnerships, have been executing to try and address threats and vulnerabilities within the wireless environment, specifically, most of them around the ORAN side of things. So I hope that that gives you a little bit of a baseline of some of the activities we have going on.

Now wrapping up the opening comments, I anticipate you're going to see today that the vulnerabilities in the RF domain, definitely an area of emerging focus, represents a tremendous opportunity for continued research to improve the security resilience of this emerging network, especially these emerging network generations beyond 5G, as we become more dependent on this wireless connectivity and the ability of these networks to touch our lives continuously all around the world.

So with that, I'm going to turn it over and introduce our first panelist. Jaisha Wray is the Associate Administrator for International Affairs at the Department of Commerce's National Telecommunications and Information Administration. In this role, she formulates telecommunications and information policies that promotes these in international forum. Jaisha will lead off our discussion on policy by addressing the following questions. What is the administration's approach been on ensuring secure, resilient, 5G networks? And how is the administration working with industry and industry national partners on these efforts? Jaisha, turn it over to you, please.

### 3.3.2 Jaisha Wray

WRAY: Great. Thank you for that introduction, Drew. I am very pleased to be able to join you all for discussion on a key area of focus for this administration, securing the supply chain and infrastructure for 5G in the United States. Today, I will provide a high-level overview of the U.S. policy efforts that underpin the implementation of secure and resilient technical solution, which I'm hoping will set the scene for the discussion with the carriers later in the panel. I'm also going to discuss some of the areas of cooperation with both industry and our international partners.

Then in my last position I worked on 5G policy and cyber cooperation on the National Security Council staff. And I was lucky that my time there overlapped with Anita Patankar-Stoll, who you'll be hearing from next on this panel. Now while on the NSC, Anita and I worked on the development of a national strategy to secure 5G, which was signed in March of this year. And as Doug Kinkoph discussed during his opening remarks on Monday, this strategy serves as our overarching strategy for the security of next generation wireless communication systems and infrastructure. And it frames how the United States will secure 5G infrastructure at home and abroad. The strategy outlines how the United States will facilitate the domestic 5G rollout, assess and address 5G security risks, and promote responsible development and deployment of 5G infrastructure globally. It also outlines how the United States will come, continue to work with our partners and allies to lead the global industry as 5G standards, technology, and applications evolve. NTIA is working closely with the National Security Council and a range of other departments and agencies to develop an implementation plan to ensure that the goals of the national strategy are met.

Now there are also a number of complimentary presidential and legislative actions that represent a holistic multifaceted approach by the administration and by Congress to work to ensure secure and resilient 5G networks. I'll go over some of those examples now.

One example is the Federal Acquisition Supply Chain Security Act of 2018, which creates a unified whole government approach to protecting federal systems from supply chain risks. It established the Federal Acquisition Security Council or the FASC and it enables government-wide exclusions or removals of specific products determined to pose unacceptable risk. Another example is section 889 of the 2019 National Defense Authorization Act, which prohibits federal agencies from procuring or contracting equipment or services using telecommunications equipment from five covered Chinese companies. And as of August 13th, 2020, which is

tomorrow, it will prohibit federal agencies from contracting with any entity in using such covered equipment or services as a substantial component of any system. Another example is the Secure and Trusted Communication Networks Act of 2019, which prohibits certain federal subsidies from being used to purchase communications equipment or services posing national security risks. It also provides for the establishment of a reimbursement program for the replacement of communications equipment or services posing such risks. And my colleague from the FCC will be discussing this act in further detail later on in the panel. In addition, in May of 2019, the president signed an executive order on securing the information and communications technology and services supply chain or the supply chain executive order. Now this executive order will prevent foreign adversaries from exploiting vulnerabilities in the ICT supply chain and protect the vast amount of sensitive information being stored in and communicated through the ICT products and services. And then finally in April, 2020, the president approved an executive order formalizing Team Telecom, a committee that assesses foreign participation in U.S. telecommunications and assist the FCC in its public interest review of license applications. The committee also reviews applications and licenses for risk to national security and law enforcement. And given how interconnected our networks are and will be with 5G, the USG understands that we cannot undertake these efforts to secure our 5G networks alone.

NTIA continues to work hand in hand with industry to secure our networks. This is why NTIA launched the Communications Supply Chain Security Risk Information Partnership or C-SCRIP, which is a program to share supply chain risk information with trusted providers and suppliers of communication services and equipment. Now this program will focus on small and rural companies that may not normally have access to this information. NTIA is also working directly with industry players on adding transparency to the software supply chain, by helping those who write, purchase, or operate software to understand potential risks in the software supply chain. So when a new vulnerability or risk is discovered, a software bill of materials can help any organization realize whether they or their customers might be at risk.

Our international partners are also critical to this effort, particularly as we look to promote vendor diversity in order to reduce or eliminate reliance on untrusted vendor equipment. We are seeking to enhance vendor diversity by accelerating the research, development, and deployment of open-interfaced, standards-based, and interoperable 5G networks across the country. Through international cooperation, we believe we can accelerate the global transition towards an open 5G network architecture and build a diverse 5G ecosystem. So these activities are just a few examples of the administration's efforts. We will continue to work closely with our international partners in the industry to ensure 5G surfaces can be accessed both safely and securely. Thank you very much. And I look forward to the discussion.

### 3.3.3 Anita Patankar-Stoll

MORIN: Thank you, Jaisha. That's a lot going on there. That's a lot for us to take in. So I hope everybody captured all that information. I certainly was typing like a crazy man. So next I'd like to introduce Anita Patankar-Stoll. She's with Verizon. She serves as the Public Sector Counsel in

Verizon's Business Group, public policy, law and security. In this role she supports public sector compliance in various areas, including supply chain risk management, cyber security, Universal Service Fund, and program implementation.

Anita, when we consider the anticipated meteoric growth of IoT that will be facilitated by these 5G deployments, would you be able to comment on some of the issues this may cause and possible mitigation strategies around that? And as well, not only the technical issues, but are there possible policy considerations for government to weigh in that could be impactful in a positive way for these 5G deployments? If you could address this, I'd appreciate it.

PATANKAR-STOLL: Great. Thank you so much, Drew. Thanks for the opportunity to sit on this panel with my esteemed colleagues. And I have to say thank you to Jaisha for the callout. I recently left government and I'm recently at Verizon. So now I get to see sort of how industry takes a look and tries to implement policies and works hand in hand with government.

So Drew, this question that we've posed here is a huge one. And of course we could take hours talking about it. So I'm going to focus here my comments on sort of spectrum issues around it, but obviously there's a whole discussion around IoT and cyber security and some of the things you mentioned in your opening remarks about authentication and that sort of thing. So just looking at the spectrum and looking at that RF link to make sure that it is in fact secure and that sort of implementation is occurring, the 5G world really does provide us with a new and exciting world of things that we can employ like dynamic spectrum sharing for example, is one of those which will allow us to effectively, and accurately, and reliably coordinate the Gs, the 5G and 4G spectrums that carriers set of. I think that's one of the ways that spectrum management will continue to change and evolve. We've basically gone from manual efforts to automated and hopefully now to dynamic.

The new—these new efforts can really—are exciting because they can automatically shift lanes in the road as needed and leverage the spectrum and enhance consumer experience. I think that there's just going to be a massive number of devices that do different things. Some IoT devices will do very little networking, other devices will do more complex solutions like AR, VR, that require massive computing capabilities on the edge of the network.

So we have a challenge. Operators have a challenge to get the right size, their network resources for the various use cases that we will have in the coming future. We also can think creatively about ways to leverage licensed and unlicensed spectrum in a way that doesn't cause interference to the licensed spectrum use. I think it's really a critical time for industry and policy makers to collaborate to ensure that the explosion of IoT use, new uses in bands doesn't cause new, also new, sources of interference to the established regimes that we have.

Of course from a technical side there have been and will be continued use. You will—operators will continue to use technical methods to deal with in-band and out-of-band interference issues. So we have everything from, you know, considering distance to frequency separation, using filtering, using case restrictions for the band side issue. All of those will continue. So from 4G to 5G, you know, there's a lot of making sure that we've learned from what we've done before and

continuing down the same path. Operators will continue to resolve interference issues. We have thousands in my new place of employment. We have cyber security professionals and employees who and engineers who are monitoring our networks to identify and respond to threats. We get regular reporting about the data, about reporting and data about the network. Engineers can look at patterns of interference and closely monitor caller data process failure rates, they can look at the frequency bands and the type of impact that is occurring and draw conclusions. We can keep track of products that are known to cause interference issues.

Alternatively of course we are in hurricane season and nature could be the cause. And so there's a lot of, you know, analysis that will, that goes on and will continue to go on. This of course can pose challenges depending on the size of an operator. And I think my colleague on the panel Carrie, will probably give us some insight into sort of what rural providers are faced with. And so it may be that some carriers really do rely on customers to notify them that services is degrading or calls aren't going through, that sort of thing.

So, you know, we have to work with all of that. And of course if interference is particularly bad then operators of course will utilize the FCC's Enforcement Bureau. This is actually where I started in FCC's EB and go to them for assistance of course under the Communications Act section 333, which states, "No person shall willfully or maliciously interfere with or cause interference to any radio communications of any station licensed or authorized by, authorized under this chapter."

Of course there are a number of ways FCC can't—can act to address interference issues. The number of regulations around marketing radio frequency devices prior to equipment authorization. And you're dealing with devices that need to be certified by a telecommunication certification body. And so all of that will continue to go on. I think that, you know, in the future turning to your question of, so what can policy makers keep in mind?

I think we continue to need good policies that are driven by technology and advances. We don't want dirty devices deployed in the U.S. So device certification may be an area where we have to start thinking a little creatively. I think the first presentation from the professor, I was taking notes, very interesting. You know, thinking about software, thinking about how software can change the operation devices and cause a device that didn't cause a difference before to now start causing devices.

Actually, the FCC's EB had issued an advisory in 2019 about devices containing—that should contain security features to protect against modification by unauthorized parties. But then the question in my mind becomes what happens when software is used, is, you know, deployed by an authorized party and somehow it inadvertently causes the device to operate in a manner inconsistent with the device's equipment authorization. There's this, it's kind of a new world of dynamic change and how do we grapple with that, both on the government and the industry- I think policymakers should continue to work with large retailers to make sure that devices aren't permitted to work and sold here in the U.S., though a part for 15 devices have their challenges. You know, I can go online right now and buy some devices that are—shouldn't be used in the U.S. So, you know, we here of course a lot of challenges in the sort of old days, right? With baby

monitors, and badly placed routers, and microwave ovens. But I think, you know, there's going to be—we achieved, worked on that well in the past. We'll need to continue to do that in the future.

There's of course a lot of good examples. Years ago the FCC held a workshop to develop technical and testing requirements for lighting devices. They would know LED lighting caused a lot of interference. Industry and government came together and that was a success story. There's other success stories around boosters and repeaters, where again, industry had come up with a consensus proposal and taking it to the FCC and was able to work hand in hand in instances like that. So I think that some of those things that we've done before, we should, you know, policy makers should continue to leverage and just keeping those conversations going. I think one of the as I had mentioned EB issues advisories, I think those were very helpful to just act as a reminder of the rules of the road and recognize that, you know, those are helpful to a number of different—to all operators and in particular, perhaps smaller operators that don't have so much resources to sort of, you know, digest all of this. It's really helpful to have those advisories.

So I think overall we need to have rules that provide predictability to licenses. That really enables operators to plan accordingly in their current and future development and deployment. And so I'm looking forward to the continued work in this area and continued discussion on this panel. And I will leave it at that for now and turn it back over to you.

### 3.3.4 Charles Mathias

MORIN: Thank you, Anita. That's a lot to wrap our heads around. All the information you provided, that was very, very broad coverage. We really appreciate that. I guess since we have the opportunity here, the FCC has taken a policy leadership role in infrastructure protection associated with supply chain risk through the rip and replace program, as well as other activities, as you'd mentioned they needed the idea of the FCC Enforcement Bureau advisories, the CSRIC, and other types of activities and programs like that. Here to provide some comments, insights into some of the FCC activities is Charles Mathias. He is the Associate Bureau Chief in the Wireless Telecommunications Bureau at the FCC. And I'd like to turn it over to Charles to provide some comments for the audience we have here today. Thank you, Charles.

MATHIAS: Right. Thank you, Drew. Can you all hear me? It's a pleasure to be here and it's a privilege for me to be able to give you an overview of what the FCC has been doing in this area.

While the FCC is an independent agency, it's a full partner in the government's efforts to secure our networks. And so what I'd like to do is walk you through the FCC's role, what we've been doing over the past several years, how that interplays with some of the executive orders and congressional action, and then tell you where we are today.

So first, the FCC's role is defined by the Communications Act of 1934. And it includes, as one of the reasons for the FCC's creation, the purpose of the national defense in promoting safety of

life and property through the use of wire and radio communications. The commission assesses national security and foreign policy concerns in reviewing applications to transfer a spectrum license, a cable landing license, or telephone lines, among other things, when an applicant has a reportable foreign ownership. We work closely with other federal agencies that have additional expertise in these subject areas. And the FCC previously has denied an application from China Mobile upon the recommendation of executive branch agencies for international section 214 authority to operate on national security and law enforcement grounds.

As Drew mentioned, we have the CSRIC, the Communication Security, Reliability, and Interoperability Council, which is currently reviewing among other things, mechanisms to best design and deploy 5G networks to mitigate risk to network reliability and security post by among other things, vulnerable supply chains. Managing security risk in the transition to 5G and managing security risk in emerging 5G implementation.

The action that we've taken began concretely in November, 2019 in the report and order and further notice to propose rulemaking. In this action following an NPRM that was a notice for proposed rulemaking, which was issued in 2018, the commission released a report and order adopting a rule, a new rule, which was 54.9. This provides that no universal service support may be used to purchase or obtain any equipment or services produced by or provided by a covered company, posing a national security threat to the integrity of communications networks or to the communications supply chain. Specifically, USF recipients may not use USF funds to maintain, improve, modify, operate, manage, or otherwise support such equipment or services in any way, including upgrades to existing equipment and services. This applies, this new rule applies to eligible telecommunications carriers or ETCs. And a covered company is a company designated by the FCC as posing a national security threat to the integrity of communications networks or communications, or the communications supply chain. The report and order initially designated Huawei and ZTE as covered companies for the purposes of the rule.

What is the rule impact? It applies to any and all equipment or services including software produced or provided by a covered company. USF recipients must be able to affirmatively demonstrate that they have not used any funds obtained by USF to purchase, obtain, maintain, improve, modify, or otherwise support any equipment or services. The prohibition applies to upgrades and maintenance of existing equipment and services, because the item found that a blanket prohibition was the best way to promote national security.

Vulnerabilities can be difficult to discover as we've already discussed this morning and malware can be designed and built directly into communications equipment. The rule does not prohibit USF recipients from using their own funds to purchase or obtain equipment or services from covered companies, but USF recipients must be able to clearly demonstrate that no USF funds were used. Existing multi-year contracts to acquire equipment or services from a covered company are not exempt from the rule and ETCs must certify that they have complied with the rule.

The designation process for future companies has a number of steps. First, the commission will initially designate a company as posing a national security threat. Upon publication of the initial designation in the federal register, interested parties will have 30 days to comment on the initial designation. If no party opposes the designation, the commission will issue a public notice following a 30-day window, announcing a final designation. If a party opposes a designation, the commission will review the record and release the final designation no later than 120 days after the release of the initial designation. The commission may extend the deadline, but will endeavor not to do so in order to provide certainty to all impacted parties. The final determination will be based on all available evidence.

On June 30th, 2020, the federal communications commission's Public Safety and Homeland Security Bureau released orders formally designating Huawei Technology Company and ZTE, their parent subsidiaries and affiliates, as companies that pose a national security threat. As a result of these designation orders effective June 30th, 2020, funds from FCC's Universal Service Fund are no longer able to be used to purchase or maintain the equipment as I described earlier. The designation orders found specifically that Huawei and ZTE are highly susceptible to influence and coercion by the Chinese government and military. It found further that the Chinese government exercises strong control over commercial entities in their sphere of influence and then China has a notorious reputation for persistent industrial espionage. Huawei and ZTE equipment also contains known security risks and vulnerabilities.

The designation orders are informed by actions of the executive branch and other branches of the federal government as well as similar assessments from other countries. There the 2019 item also included an order requiring ETCs to respond to an information collection. And Carri will probably have a perspective on this.

The goal of the information collection is to determine the extent to which potentially prohibited equipment existing in current networks and the costs associated with removing and replacing it. It was focused on Huawei and ZTE equipment and all equipment and services from these companies that are used by the ETCs and their affiliates. It—the information request seeks to answer certain questions including, do carriers own the equipment? What is the equipment? What would the cost to purchase and install replacement be? And what would be the cost to remove?

The—there was also a further notice. And I apologize for going through a litany, but I think it's important to sort of give you a sense of where we are because—and this is also a window for those of you who are not familiar with it. This is the way the FCC works.

There was a further notice that proposed to require as a condition upon the receipt of any USF support, the ETCs not use or agree to use communications equipment, they would be required to certify to such to receive USF funds. And they would be proposed—it would propose to require ETCs receiving USF support to remove and replace equipment from their services. It also significantly proposed to establish a reimbursement program to offset reasonable transition costs and propose to make the requirement to remove covered equipment services, pinging on the availability of a funded reimbursement program. It proposed to make available reasonable

replacement costs for equipment and services and propose to seek a congressional appropriation, rather than relying on current Universal Service Funds.

Now as Jaisha mentioned earlier, the Secure and Trusted Communications Network Act of 2019 created a further role for the FCC. The act was signed into law in March of 2020. And section 2 of the act requires the commission to publish by March 12th, 2021, a list of covered communications and equipment services informed by determinations from either an intergovernmental agency with appropriate expertise, a depart—a specific determination made by the department of commerce, a list of covered equipment and services as pursuant to section 889 of the 2019 National Defense Authorization Act or specific determination made by an appropriate national security agency. Section 3 requires the commission to ban the use of any federal subsidy as discussed before. Section 4 requires the secure and trusted communications network reimbursement creates the secure and trusted network reimbursement program.

And in April of this year, the commission sought comment on incorporating the Secure and Trusted Communications Network Reimbursement Program into the FCC's ongoing supply chain proceeding. The rulemaking for this must be completed as well by March 12th, 2021.

Although section 4 creates a reimbursement program, it's important to note that Congress has not yet appropriated the funding. Section 5 requires each provider of the advanced communication services to submit a report to the FCC on whether the agency has complied with the requirements. If the provider does not have equipment that's covered by the law, then they don't need to provide the certifications. If it does, they have to provide a detailed justification of what they have and why they're using it. Section 7 covers enforcement. Section 8 requires my colleagues at the NTIA in consultation with the FCC, FBI, DHS, and others to establish an information sharing program.

And finally, we are getting to the end, in July of 2020, the FCC adopted the Secure Networks Act declaratory ruling and further notice to do what we had proposed, namely to integrate the provisions of the Secure Networks Act into the commission's ongoing supply chain rulemaking.

We found that by adopting the prohibition in 2019, we complied with section 3 of the Secure Networks Act. We also sought comment on implementing various aspects of the Secure Networks Act, including proposals to maintain the list of covered equipment providers and services. A proposal that would prohibit the use of federal subsidies, such as USF, a proposal to require all providers of advanced services to submit their annual reports, and a proposal to implement enforcement penalties. The comments and reply comments are due on August 31st and September 14th respectively. But here ends the lesson. Thank you very much. I'm happy to answer questions as I can, but I would note that as this is an open proceeding, I might not be able to be as forthcoming as you might like.

### 3.3.5 Carri Bennet

MORIN: Thank you very much, Charles. And thank you for your honesty for setting it that way. And we understand that there are brakes on what you're allowed to say so. So as Charles kind of noted, the information around the Universal Service Fund, the Secure Networks Act I think, you know, while we're looking at the smaller carriers are facing significant hurdles as they move to deploy their own 5G networks, as well as some of the challenges being around supply chain risk and around some of the suppliers that have been identified as, I guess we'll just say some of the suppliers that have been identified as problematic. So here to speak on the subject of the rural and small carriers and specifically around their challenges and how they're addressing these 5G deployments is Carri Bennet. Carri is the General Counsel for the Rural Wireless Association and they represent rural telecommunications companies who each serve fewer than 100,000 subscribers. But Carrie, if you'd like to take the mike.

BENNET: Thank you, Drew. Hello everyone. I want to follow on what Charles laid out so beautifully. And I don't have to talk as much because he laid it all out, but I'm going to tell you the real-world dilemma that these small carriers are in.

About a fourth of the rural wireless association members have deployed Huawei or ZTE in their networks. And I want to back up about seven, or eight, nine years and explain why that's the case. Back in 2010, 11, or so, the FCC started proceeding to disburse money called Mobility Fund Phase I. And it was $300 million to help build out 3G and 4G in rural and remote areas where the areas are. So in trying to make the best use of that money, which is very limited and it was done through a reverse auction, where the lowest bidder got the money to serve a particular area, ZTE and Huawei had been in the United States trying to sell equipment and services. And they came in and undercut the market and made it very, very lucrative for the carriers to participate in these reverse auctions, because they could get the equipment at severe discounts from what they would buy from the traditional carriers like Erickson and Nokia. So that's how we got to where we are. And now we're there.

And since they deployed 3G and 4G, none of them have deployed 5G fortunately and that's a good positive thing. But now we're in a predicament where, you know, things have changed or information has been learned. And we're trying to this, you know, these companies are trying to figure out how they pay to get the equipment out of there. A lot of them are ETCs they're eligible telecommunications carriers that Charles mentioned, that get universal service support. That support got cut off on July 1st to use anything to support the Huawei, ZTE networks, maintain it.

Some of the money can be used for other things that don't necessarily pertain to the network that might pertain to customer service, backup generators, things like that, that are not purchased or used or from Huawei or ZTE. But going forward, since they can't spend universal service money under the Secure Networks Act on rip, I don't want to call it rip and replace, we like to call it replacing and removing or replacing and removing the equipment, because you have to replace the equipment before you can remove it.

So, in complying the order, and I think I'll get back to last June when commissioner Starks held a workshop called Find It, Fund It, Fix It, the FCC is in the process of still finding it through the data collection. The Secure Network Act is going to make us go beyond the scope of just ETCs that have to report in. There are a lot of ETCs that have also deployed Huawei or ZTE equipment that were not covered under the FCC's current data collection process that will be under a new data collection process.

So once we find it, then we still have to fund it. And Charles mentioned that we can't fund it with USF, we have to fund it through an appropriation from Congress. And that's what we're in the middle of trying to get money appropriated for that now. On the Senate side, with the COVID Relief Act, there was a provision in the McConnell Senate bill that was proposed to include funding under the COVID relief fortune for up to a billion dollars to fund this replacement. The house has already passed during the price part of the regular appropriations process for fiscal year 2021, which begins October 1st, a billion dollars. Chairman Pai has indicated early on in April that it may be $2 billion that we need. Fortunately, the Secure Networks Act got a blank check book, but the FCC has to move forward. Once they know the information and how much it's going to cost, they can come and ask Congress for more money in different years to be appropriated.

It's a process, it's not going to be done in a year. It's going to be, we're estimating a 3-5 year process and get the resources to do it. You have to remember Verizon, AT&T, and T-Mobile- do the tower building and citing and all of that. So it's a little challenging to then try to get those resources put together for rural areas to do the replacement and removal of the equipment. RWA has been working very closely with the veterans who are being trained. There's a whole program called, what they call it? The Warriors 4 Wireless, where they're taking veterans who have left the military and retraining them to help build out these networks. I think that's something that maybe T-Mobile might be involved in as well. But we're trying to get resources so that we're ready when the money is appropriated. So there's a lot of challenges that the rural carriers are up against.

The other thing that's interesting, because this is a 5G focus group, some of the equipment that we'll need and software to replace the 4G and 3G equipment already has 5G baked in. But there's some question before the FCC on whether you can use the money to buy 5G because that's not what you're replacing, but it would make sense to buy some 5G and have a secure network with this money, instead of going back to some old technology and replacing that. So that's something that we want to have further discussion on with the FCC, and NTIA, and the administration.

But we're all, I think rowing in the same direction and working really, really hard to just get this done really fast and to try to do the best with the least amount of money. But we don't want to repeat concerns that were brought up, because we were being cost-effective before and we ended up buying equipment we shouldn't have bought. So some of the challenges that our members have going forward, especially when they start looking at deployment of 5G, is we don't want to be in this situation again.

And we'd like to shift the burden of the cost of any future replacement that Charles alluded to, because we don't know if there's going to be other equipment vendors or software providers that we'll have to remove later on down the road. RWA would like to see the burden shifted to those companies so that if you buy equipment from companies and then later you find out that they have problems, that the cost is shifted to them and not to the carrier. So that's going to require—I am a lawyer. I'm, you know, making sure when you do your equipment contracts and your service contracts that you shift that burden to your supplier.

And then the part that I think that I think I wanted to have an off side conversation with Jaisha Wray at NTIA is these small carriers don't have the resources. The guy who's putting the antenna up on the towers, the guy cutting the grass, you know, around the tower and doing the maintenance on the tower and, you know, he may also be the one that, you know, is getting the cow away from something that the cow shouldn't be chewing on. So we're just letting you know that, you know, little, few resources, but very smart people out in rural America who make do with a little, and they make do very well, and they serve this country beautifully. So we want to continue to make sure that happens.

We—also I just wanted to address one other thing besides the security issue. On that, on that side of this. One of the things that our members have said to us repeatedly is, why can't we monitor the networks? Why isn't there a better monitoring program? Because how do you stop, you know, how do you stop something if you don't even know it's in there? And it seems like some resources should be placed more on monitoring as well, going forward. And they would like to be able to take advantage of that if the government is willing to try to put those programs in place and push monitoring of networks further down the chain. So I'll leave it at that because I think we're going to have a lot of robust discussion and I'd like to make time for that. So I'll turn it back to you, Drew.

MORIN: Thanks Carrie. Much appreciate it. So our final speaker for this morning, before we go into Q&A is Mike Murphy. Mike is the CTO for Nokia North and South America. He's responsible for aligning Nokia's product roadmap with the needs of customers in the United States, Canada, and Latin America. Mike, we've opened this discussion with a broad coverage of 5G deployment security activities about carriers, government policies, unique challenges, the small rural wireless carriers. I love the comment that Carri made about monitoring the network, and detection, and what can be done in those areas. So as a provider of end-to-end 5G networks and services, what can you tell us about security challenges of securing spectrum and these 5G deployments and how can we continue to advance technologies to mitigate these breadths? Mike.

### 3.3.6 Mike Murphy

MURPHY: Okay. Thanks, Drew. If you don't mind, I'd like to start with kind of telescoping start at the top level, then move down to more detailed level. So at the top level, I guess our view is that 5G is inherently, you know, on a path to being less secure in the sense that the attack surface is much greater.

So in 4G, which was dominated by partially smartphones, you know, we've used 5G as extending into vertical industries. And what comes with that as well as different areas, is potentially more catastrophic impacts of intrusion or bad actors. So, you know, if you have a problem with your smartphone, it's not necessarily catastrophic, but if you have a problem with your electrical utility or robotic surgery, that's pretty catastrophic. So the attack—we say the attack surface is bigger.

However, on the positive side, you know, this was well known in advance. And so there's been many levels of improvement in the definition and also now in the execution of 5G. So standards are a lot better. As a vendor, you know, we put a lot more emphasis into the product elements. Our customers are doing more on the network side. So there there's a lot of improvement versus 4G. Despite all that, we still say that, you know, the really the final, you know, the final proof of trust is in the supply chain. You need to trust your suppliers. So, you know, we agree with the FCC's stands on this.

Now getting a little more detailed, so on 3GPP, the standards for 5G, it's done a great job. Things are a lot better than in 4G. A lot of the interfaces that weren't encrypted before are now encrypted. Some of the old problems like MZ catching, those are, you know, close to impossible now. Even the fundamental architecture of 5G is better. You have things like CURUD is split, which breaks up a base station into multiple parts. Some of it, for example the part that resides near the antenna, doesn't even have any access to user info now. So you can kind of isolate that part. A splicing allows you to have vertical and even physical separation. So you can have different boxes that support a slice or a virtual part of the network that gives you a physical protection.

But despite all that, 5G is still vulnerable. There's still messages, there's still control channels that are not encrypted, but the good news there is that these are slowly starting to be addressed. So there's the standards, there's a document called TR33.8.9. It's been going on for two years now. And it more or less lists all of those problem areas that I mentioned. Then step by step, you know, there's going to be solutions to those.

That being said, you know, they're—not everything can be solved. There's sometimes technical hurdles to execution of some of these solutions. Okay. Continuing on a different plane.

So that was the standards plane. On the vendor plane, for example, a company like Nokia at the very highest level, we put a lot of emphasis on ethics, just mandatory training for every employee. I just finished mine a week ago. We're part of the Ethisphere subscription to looking at the world's most ethical companies. We're a four-time honoree. I think we're the only telecom infrastructure vendor in that as a world's most ethical companies. We're also involved in the NIST 5G security, FCC, CSRIC, as you mentioned.

Like coming down to the product level, we have on the call design for security, where we look at every single thing we make, hardware and software, from supply chain to software development, and we assess it for security threats. And that includes third-party software by the way. So we

look for things like hard coded passwords, backdoors, and make sure those are removed before we deliver them to a customer.

And we also have something what I think is quite interesting is even after you do all of that, you're deploying networks, you're still going to have a problem. So we have something called a threat intelligence lab that looks at over 70 networks worldwide. And a couple of interesting statistics there. So since COVID, the monthly rate of infections in the network has increased by two times. And since 2019, the infections by IoT devices has increased two times. But this is definitely a growing problem. And the last report we did say that the monthly average infected devices in the U.S. is about 2.3%. So if you calculate that out, that's about 700,000 infected devices today.

That's largely smartphones. I mean, there's some portion that is IoT. But as we move towards 5G and the IoT side starts increasing dramatically, we would expect that to increase exponentially almost. And another interesting statistic is that from our threat intelligence lab, we observe that once an IoT device is connected to the network, it takes about three minutes before there's an attempt to infect it. So it's a big problem, but on the other hand good things are happening to resolve some of the problems.

Coming back to the more, one of the questions was asked for this session was about interference and jamming. So that's kind of inherent in anything that's RF, because you can't block the airwaves. So once it's in the air, you can look at monitoring it, hopping it, and repeating it. But there's a lot of things that are good in 5G to help against that. So, you know, just at the very, very highest level, 5G is higher frequencies, which makes it on the bad side, it makes outdoor, indoor penetration more difficult. On the other, on the positive side, you know, if you really wanted a highly secure system indoors, you could use millimeter width indoors and the external propagation outwards will be fairly low. Also beam forming is very directional, that makes replication more difficult. So there's some good things happening even on this interference jamming topic.

So in short, you know, we think 5G has more threats than 4G, but there's also more action that's been taken at 4G and continuing action. So that's kind of my quick summary here. Now, Drew you asked me you said, "Hey Mike, can you end on a controversial topic so we have some good dialogue here?" Well, I'll try and do that. But my question, which I know it will be controversial, is as we move to more open ecosystems and O-RAN as a foundation for that, so we have more suppliers of different sizes at necessarily a consistent to draw some of the things I mentioned that Nokia does. Will that actually increase rates?

### 3.3.7 Panel 2: Q&A

MORIN: That's a doozy. Thank you very much Mike. That was great discussion, great set up on the technical side of things and a wonderful leading question. And I know that essentially, because we have a lot of folks here who are dealing with the open RAN and really opening interoperable networking configurations. And it's interesting, because I'm of two minds of it.

I understand the premise that by opening up and expanding the supply chain ecosystem to new entrants and to other entrants through opening up these different components within the network, that there's a theory that could help the U.S. have more U.S. suppliers, U.S. centric suppliers and therefore, that's going to improve supply chain risk management. I understand that argument.

I also look at it from the standpoint that anytime you're opening up and adding more platforms and more interfaces, and you mentioned in terms of the 5G network, the idea of the CU, the DU, the RU, which the radio unit, the distribution unit, and the control unit. And if I'm going to separate those three out and have different vendors and I'm going to have different interfaces across those, every one of those interfaces becomes a new attack surface, right? That right now is pretty much enclosed within a more proprietary architecture. So you can see that on both sides there's going to be arguments for and arguments against. So it's definitely a loaded question. So, I think, you know, my perspective is that a supply chain risk management, the idea of specific countries that are problematic and suppliers from specific countries that are problematic, is a concern.

But there are ways to manage that threat. And I think one of the things within the Department of Homeland Security supply chain risk management task force and I'm a member of it, Nokia is, as well as Verizon, as well as NTIA, et cetera, and FCC. And so when I look at that, when we talked about some of these threats, we evaluated somewhere, I actually co-chaired the threat evaluation working group. We went through and did a survey and got around 300, 400 some odd threats that we then categorized into different areas. And one of the things that we found is that to just say, well, if it's a foreign provider, that's a threat, that's not necessarily true. What—there's a lot of different criteria that you take a look at and it's if the provider is subject to control by a nation state and that nation state is a threat, that's where that threat really originates.

So there's a lot of things that we have to be a little bit more mature about and we are. I think from the public-private partnerships that we're having right now, we're getting a much better handle I think on both sides of the fence, as far as supply chain risk management and how that feeds into the enhance—the security and resilience of our moving forward networks. So that is one person's view of it. I'd like to open it up. Somebody wave if they're interested in adding to it what their views are on supply chain risk management and specifically around the radio side. Anybody? Yes Anita, please.

PATANKAR-STOLL: Well, I agree with what you were just saying, Drew. I'll just add that, you know, I think going back to my lessons learned, let's learn from the lessons of the past, so we've done this in the core already, right? I can like defer to you for the engineering analysis there. But, you know, learning from the lessons of the past and using those in the new context of O-RAN, open doesn't have to mean insecure. So let's make sure we're baking security in as we're doing that.

I think the challenge is that there are challenges, right? There's the idea that you can open the marketplace, but this isn't the kind of thing that just anyone can do, as you well know. Like you

need good engineering experts that are developing the software that goes into the boxes. This is not if, you know, it's like a colleague of mine said, "You know, it's like if Verizon were to open a restaurant, well, our Wi-Fi might be great, but our food might not be that great." So I think that's the challenge and operators that are currently in the deployment phases, it's a challenge because we need stuff now.

And then not only, you know, you need it now, but then you also need the deployment is a challenge. You have thousands doing it in the U.S. right? You'd have to switch out thousands of boxes. And so there's challenges there. And then of course we can go into, what are we all dealing with right now? COVID. And the ability to actually get boots on the ground to do that is, can be challenging. So I think, just as Drew was saying, you know, the sort of open access, the arguments that you hear from sort of government side or sort of the economics of it, should be weighed with enabling devices that are in software that's secure and deployable. And so I think those are just some of the thoughts speculating on this.

MORIN: Thank you. And actually, there was—okay, Carri wants to weigh in on this. I also have a way I'm going to tie it in with one of the questions that have been raised. But Carrie, you first, please.

BENNET: No, I was just going to say from my members' perspective, because they're about to be in a position to have to deploy brand new networks. They're very, looking very hard at these open interfaces and open RAN radios and whatnot. Because to them it's like we get this money, we have to make again, good use of it. They're very conscientious of this. They can use it to upgrade through software and that would be really important. And so these deployments in these areas I think as long as this is secure and our understanding isn't another. I'm a lawyer, I'm not a technical person, that the open interfaces, because they're open you can see into it. They're not proprietary, they're not closed, you can't see the bad stuff that maybe you could see and what we, you know, suspect the government has suspected has been going on with Huawei and ZTE. So that to us is exciting. And to future-proof networks by being able to upgrade like that would be very, very important. So and, you know, do it once and then the lift going forward into 6G and 7G, which I'm hoping I'm retired by then, will be a much easier lift. So that's our comment from the rural's perspective. So.

MORIN: Thank you. Any other comments and thoughts around the idea of these open networks and open interfaces? And if not, I'm going to actually try and tie this in a little bit to one of the questions that came in. Since we have been talking about this in the context of supply chain risk management, one of the questions that came for Jaisha was around that the NTIA seems to be or the administration, it was more of a political question, seems to be almost exclusively focused on supply chain risks. And the question was, what about all the other threats to the security and reliability of 5G networks? And I know NTIA has a lot going on in this. So I think it'd be great for you to kind of open up that conversation on it please.

JAISHA: Sure thing. Thank you. So, and I see where that question came from. A lot of my remarks were focused on the supply chain aspects and I think that is one of our key focuses, because we are recognizing that adversaries are trying to steal information, exploit these

systems for intelligence collection and surveillance. And so what better way to stop it than by focusing on the supply chain. But of course our 5G strategy is multifaceted beyond the supply chain. We are looking at enhancing U.S. participation, U.S. leadership in standards, bodies, we are looking to promote R&D testing, evaluation of new technologies. So I would encourage you to take a look at our 5G strategy and the implementation plan which is being developed now. We'll offer even more comprehensive approach on the U.S. actions that we are taking to really face the threats to security, reliability of our 5G networks. But yes, a lot of it is focused on supply chain.

MORIN: Yeah. Well, it's interesting because building on your comment and Carrie's comment before about the deployments and the news comes about deployments now, what we have to do today, one of the things I know we've fed back into and a lot of the folks in the industry talk about in our conversations with NTIA around the next generation and what the future research plans are and to this community that's on the call here.

You probably going to find this also very interesting because this is one of these research areas, is how do we start looking at those next generation 6G or next G, whatever wave forms? How do we look at the different, if we started to look at terahertz frequency? What are the different things we're going to be able to do there? And are there improvements now that we see what's happening in the 3G, 4G, and even in the 5G spectrum and spectrum efficiency, some of the benefits of beam forming, as Michael commented on and things like that. You know, are there ways for us to look at that spectral protection and kind of field it in to that next generation research, that next generation 6G and beyond?

So I mean, I'll just put that out there as a challenge to the audience because I'm assuming there's a few academics out there who are looking at this problem. And we'd love to hear it, I'm sure NTIA would love to hear what you all are working on, because we're really—we'd like to drive and this fundamental research that needs to be done for that next generation of technology, which is another way that we can actually have a U.S. led, get back into the infrastructure lead that we've had in our country over the past decades for the, you know, 3G and 4G beyond. Okay. So that was one of the questions. I see that Jaisha would like to comment some more and so would Anita.

JAISHA: One thing to add on that is, I know Doug Kinkoph also holds everyone who submitted comments on our request for comments on the national strategy to secure 5G implementation plan. But this was a topic we certainly heard about there. We really welcome feedback from all of our stakeholders and really encourage everyone to continue this discussion, because as you mentioned this is a critical focus.

MORIN: Thank you for that. And Anita, I saw your hand was raised. What would you like to add?

PATANKAR-STOLL: Well, I was just going to echo, join the chorus there in terms of research. You know, you guys at T-Mobile have a lot going on, we have a lot at Verizon in terms of lots of labs and opportunities for collaboration, businesses, and universities, and that sort of thing. And of course, I'll put a plugin for ITS and Andy and the group. I think that, you know, that's where it's

going to come from. And, you know, I was also going to mention on this question, you know, other threats about security and reliability, I think we're seeing it in the government from other places too, right? So a lot of us are thinking about the upcoming cyber security maturity model coming out of DoD. And so clearly, you know, that effort is a large one and is focused on more than just supply chain. It does include of course supply chain and references to NIST 80161. But there are definitely broader efforts afoot. I just wanted to throw that out there.

MORIN: Thank you, Anita. Thanks for bringing that up. One other area that I'll—and Mike, I want to kind of lean on you in this one, hopefully, and that has to do with both Anita and I mentioned the idea of dynamic spectrum sharing, you talked a little bit about it as well. But one of the questions that was raised is that is when we talk about enabling the Gs and all of that, there's a little, the audience is saying that there's a bit of confusion about dynamic spectrum sharing in terms of how applicable it is for sharing in a non-exclusive spectrum environment. So the question has to do about could anyone elaborate on scalability of dynamic spectrum sharing for use and shared spectrum machines. And I know Nokia has got a dynamic spectrum sharing platform product. Maybe you could talk a little bit about what it is, how it works, what it is anticipated to achieve in this type of an environment. That would be very helpful I think for the audience.

MURPHY: Okay. Well, I mean, dynamic spectrum sharing is a pretty simple concept. So you know, you have two choices, not to share, so not dynamic spectrum sharing. So then you basically have your 4G spectrum, it's used for 4G, 5G is used for 5G. In fact, the Sprint's first deployments 5G were done using this what we call split mode 4G/5G. Dynamic spectrum sharing is just saying, okay, you know, I want to use some of that 4G for my 5G—for 5G. However, I don't want to dedicate it, because the fact is right now in the United States you don't have that many 5G devices out there. So I don't want to give up 4G spectrum completely allocate it to 5G where there's not many subscribers. So how can I do that in a dynamic way basically based on request? Well, if there is somebody 5G device in that particular geographic area, you know, that spectrum can be used for 5G, but if there isn't, it's used for 4G. So it's kind of a way of smoothly transitioning from 4G to 5G. So it's very, very important especially in the United States where 4G capacity is kind of at its maximum. So it's not like you can just steal away spectrum and hand it over to 5G. You know, you still have the subscribers needing it. So this is an elegant way of doing that. Does that answer your question?

MORIN: Thank you. Anita, you wanted to weigh in on this as well, please? You're on mute Anita.

PATANKAR-STOLL: Sorry. Can you hear me now? To quote an old commercial. So agreed. And I think from a policy perspective, I think there's challenges, right? Like, so the technology may be there, but then in my mind, I wonder, how is this, you know, this question is asking non-exclusive spectrum environment. I have a question around, well what about when we're talking about government and industry sharing, what does that look like? And, you know, I think that there are challenges in there aren't rules in the road yet for, well, who gets prioritization. Like, okay, well, if I'm doing it for, you know, if an operator A is doing it for operator A's customers, then operator A has full control over where and how much and, you know, the movement, the dynamic use and efficient use, and can monitor that, and, you know, all of those things that

come along with spectrum management. So, but then how do you do that when you're introducing a couple of carrier A and carrier B or introducing carrier A DoD? Well, for—that's where I think we need some good dialogue and good industry, you know, not to be, not to sound too repetitive, but that collaboration. The government got that right. Otherwise, it's be as, it won't be able to be used as well as it could be. So.

MORIN: Okay. Thank you, Anita. And Mike, I see that you've got an additional comment you'd like to raise or it is another inflammatory question? Just kidding. So go ahead and unmute, Mike. Mike yours.

MURPHY: Very specific technology. But there's something completely different, which is just sharing spectrum, like CBRS. And, you know, going forward we know that a lot of spectrum is still used by agencies and it's difficult to free up easily. So then we have to get into a shared spectrum, something like CBRS. And it is true, you know, it can get a bit tricky depending on the particular usage of it. So in CBRS, we know it's used by radar on postal lines of course. And I was talking with my colleagues there's something in CBRS called the ESC, environmental sensing capability basically tries to detect radar. If radar is on it switches you off. But on the other hand, it's actually pretty easy to probably replicate such a signal and basically turn the operators off. So almost certainly, I think the broader context of sharing between different parties, whether they be different operators or government agencies, you know, commercial business. Big topic and it brings with it more questions about how do you make it secure?

MORIN: That's from our perspective one of the concerns we have raised is, if I'm running commercials, traffic, and there are other providers radar for example, or other types of devices in there, now you—the idea of a road base station goes out the window. Because if it's in the shared spectrum anybody can be in that spectrum, whether they are legitimate or whether they're nefarious. And so it changes the dynamic tremendously. And this is not a simple problem and it's going to be with us for a while as we try to figure it out collectively. And I think that that's an important thing to note in that regard.

Carri, one of the questions that came up, I want to direct to you, is the question was about the RWA members and any potential impacts or experiences they've had related to security vulnerabilities in the existing Chinese equipment. To what extent has existing equipment proven to be insecure, caused any outages, breaches, malware, espionage, hacking, and others really? Has there been any that you're aware of? You don't have to name names obviously, since your association is good. But have there been any instantiations of these threats, vulnerabilities in a material way or even in a non-material way that you are aware of within the rural community?

BENNET: Flat out, no. That's why, you know, in the beginning and I think there was some reticence on all of this when this first, you know, launched. But, you know, they understand that they trust the government that there is problems and they're ready to move it and get it out.

MORIN: Okay. Short. Asked and answered. So another question came up and I'm going to just open this up for the broader community here, is that it has to say, they were talking about—we talked about 5G supply chain security, they're talking about, has any thought been given to the

unknown unknowns in 5G security, supply chain security? Which I think is a kind of an interesting way of asking it.

And my initial perspective on this would be from the standpoint that the supply chain risk management task force did look at these 300 somewhat, categorize them into nine broad categories, as far as the types of supply chain risk management, because they weren't just about a supplier actually intentionally putting things in. But we incorporated economic threats, we incorporated insider threats, we incorporated a broad spectrum of threats in that. And that is something that has been published at Department Homeland Security, cyber security information security agencies website. You can dig that up.

I can also share it with folks who organized this, Andy and team to get it published out so you all can get access to it. It probably answers that question fairly clearly about, yes, the thought has been given and industry and government have worked together in that particular one to address some of those challenges and concerns about supply chain security.

Let's see here. Just want to make sure we kind of—one of the other questions was raised up about end-to-end the 889 guidance from the federal within the National Defense Authorization Act and some of the guidance there concerning integration or use of telecommunications equipment and services from prohibited providers. Along those lines, one of the questions that was raised and there were a couple, there were variations of it. But I'll just kind of drive into one aspect of it, which is the idea of interoperability between North American operators that are covered by this and international operators. Because we do have roaming scenarios where a foreign person comes to the U.S. and is roaming in the U.S. and we have to interconnect with their home operator and vice versa, where a U.S. person goes to that foreign. And the general concern or question was, you know, how do we ensure that there's, I don't know, I guess, the idea of protecting and does the indie—does the 889 restrictions actually apply to this type of a scenario? So we've got a couple people here who've got a legal background, I'm not one of them and this would seem to me to be more of a legal. So we'll start with Carri who's got her hand raised. And I'd like to, you know, if any of you all would like to add into it, I'd love to have, you know, you all participate. Carri.

BENNET: I was going to say after the NDA 2019 was passed, I think Congress or some members of Congress immediately realized what they had done. And that it did cause a problem with our, you know, our foreign service offices overseas, our military bases, and the government contracts that those Huawei networks and ZTE networks are deployed in different parts of the world and there's not a way to not be on them. So I think that initially caused some problems and immediate violations. I don't know what they did to fix it or, you know, take care of how to deal with it. I just know that they identified it as a problem.

MORIN: Thank you. Charles, if you could add some context for, that would be very helpful, most appreciated. You're on mute, Charles. Charles?

MATHIAS: Yeah, thanks. First, thank you. The precise interpretation of ADD9 is a DOD- is sort of arcane. And I don't know the precise answer for that, but a related question that I saw was, what

would happen if you had international networks and you had prohibited equipment outside the U.S. and you got USF money? And I can tell you—and Carri would have a perspective on how many of her members, because I think that might be the group that would be most impacted by this. If you—the way I think we would interpret it, if you have prohibited equipment and you bought it and put it overseas, that would be a problem for us. But if—but we're really concerned with just the network that you're responsible for. And if you have to interconnect internationally, that's not something that we're looking at. We have a narrow approach.

BENNET: And I would just follow up and say that my members aren't doing anything overseas. I mean, they don't deploy anything overseas. But I think what the concern is, is like if you have a government contract and you're using Verizon, or T-Mobile, or AT&T, one of the bigger carriers and they have—and you have to take these phones or you have the, you know, serving the military bases overseas or the, you know, the diplomats overseas and they have the contract with Verizon, or AT&T, or T-Mobile, and then they're interconnecting with these networks, then how do you stop that from happening? And what—and I think that's the part that I think is about to go into effect tomorrow. And that's where that interim role is coming through. And I think that that could be problematic. But I think it went into effect for that purpose like almost immediately and then they realized after they passed the law like, "Oh, we just put ourselves in violation of the law." And I don't know what happened. I was told that by members of Congress and I never knew what the resolution was, because it's outside the scope of what I do. But that's where it is. I think it's the government contracting aspect.

And I think the other problem is from the rural carriers perspective, a lot of these rural carriers who have these networks in place are along the borders of, you know, Canada. And Canada has Huawei equipment deployed and there's roaming that goes back and forth between the Huawei networks on this side and our side of the border and on the Canadian side of the border. So it's problematic in that there's a carveout for roaming on third-party roaming that is in there. But where we're finding a big, big problem is the way it's being interpreted under the interim rule, is that if Verizon is roaming on this- government con—that's government, federal government folks, roam on these third-party networks that are my company's networks, then that's okay. That's covered under the exemption, that there might be an interpretation that they can't let their own customers, Verizon's own customers that are not federal customers roam on this network.

THIESSEN: And with that …

BENNET: That's where we have an issue I think.

MORIN: I think Andy is pulling out the hook.

BENNET: Okay. Sorry, it's very complicated.

THIESSEN: I want to get my gongs to hook and reel us back in.

MORIN: Andy, just real quick. I hate to interrupt, but would you also mention to folks, you know, we're going to provide documentation, things like that, some of the things we've mentioned, there have been some questions about that. So if you'd address that please?

THIESSEN: Right. Yeah, so for everybody out there, I know that a lot of the references that Drew mentioned, you know, we knew coming into this, that there's going to be interest bubbling up on those. And so we will work on making sure that those references, you know, to all the documentation that we talked about today is posted. So with that, you know, the transition now and so I think this is a good segue into the Q&A that you'll have with each one of the panel members and professor Zajic as well. So let's see, I have to read my part here. We're now going to go into the breakout room. Remember, the information on the breakout rooms is in the ISART app or on the email that you got for confirmation. And for our panelists remember to close this and then re-click on the link to jump into your breakout rooms so we don't get any crosstalk between the panel session and the breakout room. So with that, I look forward to seeing you each in the breakout rooms. Thank you.

## 3.4 Andrew Thiessen: Introduction of Technical Presentation

THIESSEN: Welcome back, everybody. Good afternoon from Colorado to the afternoon session of day 3 of ISART. This afternoon, we're going to be focusing on monitoring. So we're going to start with a technical talk on spectrum monitoring, and then we're going to move to a panel of experts and we're going to explore options for effective and efficient spectrum monitoring and how to obtain usable data. And basically also what that usable data is looking at that as the nexus of the feedback loop between design deployment and operations, right, in an obvious key to securing the 5G radio layer. Remember that at the end of the panel, we're going to move to the breakout rooms where you'll have the opportunity to interact one-on-one with your panelists, again to coffee breaks. And not just the panelists, but also the technical speaker that I'm going to introduce next, so let me get right to that.

Our next speaker is Doug Boulware. Doug has been a fixture at ITS since 2017. He's a project leader and a senior developer for the Propagation Modeling Website, and he's a senior software developer for the Spectrum Characterization Occupancy Sensing. Spectrum monitoring system, that's a mouthful developed at ITS. But Doug is absolutely deep in the bench of subject matter expertise on spectrum monitoring. So, let me go ahead and turn this over to Doug.

## 3.5 Doug Boulware: Spectrum Monitoring

BOULWARE: All right. Thank you, Andy. Oh, just lost slides. OK. Good afternoon, everyone. Thank you for this opportunity to share some information on what I believe is a very exciting project in spectrum monitoring within NTIA's Institute for Telecommunications Sciences here in Boulder. This project is led by Mike Cotton. He's the division chief in our theory division. And once again, my name is Doug Boulware. I'm a computer scientist and software engineer and I oversee the software side of this effort. Next slide, please.

So we're going to begin and get into the motivation that drives this work. And then we'll go into some of the details on a real world research and development environment that we were—that we're establishing known as Boulder Wireless Test City, then we'll hit on some key points of a heterogeneous distributed and persistent monitoring capability that we're developing within the Boulder Wireless Test City. Next slide, please.

So many in the audience are probably aware, ITS has a long storied history in measurement and monitoring going all the way back to 1927. So you can see in these various pictures the evolution of our measurement monitoring vehicles through the years, and we have a more modern version of these even today. Now, while the technology has changed over the years, the basic concept has remained the same, and that is that we assemble laboratory grade measurement equipment into one of these vehicles. We'll take it to a fixed location for some duration of time, perform some measurements, bring the data back to ITS, analyze it, and report on the findings. Next slide, please.

Now, increasingly, though, we're being confronted with some challenges. We all acknowledge there's increasing demand for finite spectrum. And the concern is that as we move forward, and particularly as we enter into more dynamic usage of the spectrum, there's concern that there may be increased occurrences or opportunities for unintended interference and degradation in our systems. And on top of that, as we heard a little bit yesterday, advances in technology have now made it far easier and cheaper for people to jam systems or cause intentional interference in RF systems. Then compounding that issue, the fact that, you know, really, wireless security tends to lag behind traditional cybersecurity. You put all this together and you begin to sort of come to the conclusion that perhaps our traditional approach towards monitoring doesn't scale to the current and future challenges that we face. In addition, even within ITS, there's some debate on persistent sensing or monitoring. But within, you know, this group, we believe there's value in persistent sensing.

And so as an example of that, I mentioned that several years ago ITS deployed sensors out of four coastal locations and ducked long term occupancy measurements in the CBRS band. So these charts on—or these graphs in the top right are showing monthly occupancy levels through the course of a year at each of these four locations. What they're able to show over this long term monitoring activity is that sharing in this band actually may be viable. In addition, having these sensors out at these locations, collecting persistently also presented additional opportunities.

Recently, there was some concern that emissions from Mexican wireless carrier could bleed across the border and cause interference, potentially, for our FirstNet communications. We were able to use the data that was being acquired from our San Diego sensor to investigate this issue. You can see in the graph on the bottom, the blue highlighted region, the far right side, does that—we actually were able to see emissions or the downlink from this Mexican wireless carrier coming over into the FirstNet uplink band. Now, all of our experience in this area over time has also led us to the belief that in order to develop these new monitoring capabilities, and the broader suite of advanced wireless technologies, we need a real world research and development environment to support that technology evolution. Next slide.

So we're actively working to bring about a new future for spectrum monitoring. We're trying to fundamentally change the way we perform this monitoring. To do this, we've established a real world research and development environment known as the Boulder Wireless Test City. And we're using that environment currently to develop a distributed persistent and automated spectrum monitoring capability. This system is built upon heterogeneous sensors that utilize standardized and open source software, and provide common metadata for the measurements and uses automation for security and scalability. Next slide.

With the Boulder Wireless Test City, what we've done is we've distributed sensors throughout Boulder and up at our Table Mountain field site and radio quiet zone. This map—Or the map you're seeing has pins of different colors. So the green pins are showing sensors that we have currently deployed and are up and active. And then the yellow pins are showing priority sites that we've identified for our next deployments. And then red and blue pins are showing sites that are sort of under additional consideration. What we're trying to do here is deploy these sensors throughout a broad area to offer several different RF environments.

So our radio quiet zone up at Table Mountain has long been valued asset of NTIA and ITS'. It allows us to perform very controlled experiments. And now within Boulder Wireless Test City, we're able to expand into new and interesting environments. So through—By placing these sensors throughout Boulder in the wider region surrounding Boulder, we cover not only different terrain, but also areas that feature different spectrum activity. So down in downtown Boulder, we might have something that's more similar to an urban environment. And then as we move out, we encounter more suburban.

And then going even farther out, we get into sort of world spectrum environment. We're doing this with an ongoing Cooperative Research Agreement with CU Boulder. This allows us to deploy RF sensors throughout their campus. We're also actively working or engaged with the Volta research and administrative network to identify additional locations and negotiate fiber access at their locations. Each of the sensors that we're deploying within the Test City are also outfitted with our Spectrum Occupancy and Characterization Sensing or SCOS software that will go into some more detail on an event. Next slide.

So, one of the things that we're trying to support within the Boulder Wireless Test City, and more broadly as a monitoring capability, the notion of heterogeneous sensing. But the idea here is that we can actually just customize sensors to suit the monitoring task at hand. So certainly, there are situations that require more expensive sensors or sensing equipment. So an example of this is the sensor that we've deployed out to those coastal locations and within the Boulder Wireless Test City, diagram in the lower left. This was a mid-range commercial sensor that we then outfitted with a custom pre-selector to allow more sensitive sensing in—or measurements in a noisy environment.

Now, on the flip side of that, the diagram on the right shows the—our inexpensive sensor that we refer to as the Greyhound that we've been experimenting with. And so we've built this sensor off of inexpensive commercial SDR and minicomputer. But the idea here is that across both ends or, you know, both ends of the spectrum pun intended, we're using cots, components that are

interchangeable, and then we surround those with repeatable and automated processes that allow us to calibrate the sensors as we go from lab to field. Next slide.

Now, if we're talking about supporting heterogeneous sensors, right, we need—we still need a way to interact with those sensors. This is where our SCOS sensor software comes in. The SCOS sensor software essentially just establishes a universal language or API with which to interact with these different sensors. So this API allows us to interrogate the sensors and scheduled tasks on them, regardless of the underlying sensors, capabilities, or manufacturer. We've built in or integrated support within this framework for two commercial SDRs. We've also open sourced this software in an effort to hope—to encourage others to provide additional integrations for support for additional radios.

The key to understanding what SCOS provides is a notion of discoverable sensing actions. An action is really just some sort of operation that the sensor can perform. But the thing to note here is that it's more than just the technical parameters of the sensing. Actions allow you to also encode additional post processing on the data. So you can push processing of the RF data out to the edge of the network, and this has several advantages. One, you can reduce the amount of data that you're required to send back to the central repository. And then also, you can reduce the amount of sensitive data that you may be sending across the network.

In addition, these actions then also serve as sort of a research transition path. So whether you're an researcher that is internal to ITS or an external researcher, that you may be interested in signal processing or machine learning. So you can focus in on your algorithm development and then it sort of packaged that as a action using our SCOS sensor API, and now you have a means to distribute that capability of sensors in the field. Each of the sensors also features an onboard scheduler. So interacting with the API is really just as the simplest, interrogating the sensor to find out what capabilities it has or what actions it can perform, and then scheduling those actions at the desired time for the desired duration. Next slide.

So our SCOS sensor software allows you to interact with an individual sensor, regardless of those underlying capabilities. But what we're after here is interacting with entire distributed networks of sensors. So we've developed a SCOS manager software that provides centralized command and control over the entire network of sensors. This allows you to manage sensible—sensor schedules across the entire network, search and download archived arc data, and then also perform analytics and visualization over that data. Similar to how SCOS sensor features actions as kind of a specialization or injection point for new capabilities, the manager also features a well-defined analytics API that serves as a similar function for both internal and external researchers.

We're currently working on obtaining what's referred to as authority to operate that will allow us to host these capabilities off our ITS network and establish a website. It will be available for authorized federal users, we hope in the first quarter of FY '21. Next slide.

So one of the key things driving all of this is that we're trying to encourage both interoperability and reusability, and we're doing this on two fronts. So the first is through standardization. We're

working within the IEEE 802.15.22.3 working group to establish an IEEE standard for the API's that's used by both the sensor and the manager. So this working group is chaired by Apurva Mody. I believe he's in attendance today. And I think the draft eight is currently under circulation and we have hopes that it will go to the IEEE review committee in September. The other front, on which we're thinking this, is through establishing open source and common metadata for the broader community to use. Within SCOS, we've embraced the SigMF JSON metadata format that we've established nine additional SigMF extensions, and have pushed those out to a public GitHub repository.

And I should note here that, you know, these aren't just out there for others to, you know, kind of view and consume. Being in GitHub allows other people to file issues or submit pull requests for changes or offer up additional extensions as well. Next slide.

The final thing I want to hit on within this distributed and persistent monitoring capability is scalability and security. So we feel that automation is actually the key to both of these. So we're actually automating the provisioning of the operating system and the software, as well as the maintenance of that software throughout the system's lifecycle. So we're using foreman to automatically deploy the operating system to all of our edge devices, and then also perform status and monitoring. We have also used puppet to establish different essentially kind of configuration environments that allow us to pin the devices in those environments to different versions of the software. So as we mature the software, we can automatically push, upgrades to sensors in different environments.

Finally, with regards to security, and more specifically confidentiality and integrity, we're currently working to implement the security controls identified in this Special Publication 800-53. And then here, too, we're using automation, that we have Ansible, automatically deploying security hardening scripts to the edge devices after the operating system has been deployed to those devices. In addition, each of the sensors in the network are outfitted with a calibration and sensor definition file. And then these files are used to populate the metadata that's supplied with every acquisition or sensing operation to sensor performs.

Finally, there's one aspect to your actions that we didn't mention before, that's an advantage. So the nice thing is that we can develop an action and we can actually put that action through lab verification, established that, you know, we've verified that it's providing the data that it should, and that we have confidence in that data. Then once we've gone through this process, we can actually push that action into configuration management so we can have faith in that data as we go forward. Next slide.

So I'll wrap things up here and just highlight a couple points. We've talked about how we've established Boulder Wireless Test City. Now we're using that environment to mature this spectrum monitoring capability. The point really here that I want to drive home is that we're not sort of doing this research for research sake. The idea is to establish this environment, the Boulder Wireless Test City, that allows us to mature this capability so that we can then push it out and have a national impact with it. So we've currently established the ability to perform edge processing as well as coordinated sensing within this environment. As we move forward

over the course of the next year, we're hoping to dive in to really characterizing the RF environment within Boulder in the surrounding area. And then more broadly, as we go further down the line, we believe that Boulder Wireless Test City could be very useful in additional propagation model development and validation. And then further down the road and compliance validation as well as enforcement methods. We realized that these are challenging issues that we're investigating that we know that will only succeed through partnering with industry, academia, as well as other federal agencies in the development of these advanced spectrum technologies. And with that, if there's time, I'll open it up to questions.

### 3.5.1 Technical Presentation: Q&A

THIESSEN: Thank you, Doug. You have one question. It's, can you repeat the full frequency range capability for SCOS?

BOULWARE: Let's—So that's, I guess, dependent more on the specific sensors that you have. So, Mike may want to correct me on this in our breakout afterwards, but the cheaper inexpensive Greyhound sensor, I'm not sure of the total range, but that one we've outfitted has been focused on monitoring 700 MHz bands. That other mid sense—mid-range sensor that I talked about, I'm not entirely certain on this, but I believe it goes up to close to 6 GHz. I would check with Mike Cotton afterwards, though, on those details. He handles that side of things.

## 3.6 Panel 3: 5G Monitoring and Data Collection - The Feedback Loop

THIESSEN: Fair enough. Thank you, Doug. So thank you very much for that talk. And remember, everybody, Doug will be in a breakout room following the next panel for additional questions. And I think that's the perfect introduction to the next panel on monitoring and data collection. Our moderator is Dr. Ashley Zauderer, who's the program director in the Division of Astronomical Sciences, with him the director for mathematical and physical sciences at the National Science Foundation. Her primary responsibility is electromagnetic spectrum management, where she works to represent the scientific interest for protection and use of electromagnetic spectrum, both within the United States and internationally. So Dr. Zauderer, you're a very busy person and I think you're a great person to moderate this panel. And so with that, I'll turn it over to you.

### 3.6.1 Ashley Zauderer: Panel Introduction

ZAUDERER: Great, thank you very much. And welcome, everybody to the third panel, monitoring and data collection. We're very excited to have today, five experts that combined have more than 125 years of relevant experience in data monitoring. It's very important as we think about securing the 5G layer that we get the feedback that we need from data, ongoing decisions related to design and deployment, in problems with ongoing operations, whether it's interference, that's intentional or not. I wanted to note that on this panel, it's great, we have representation both from academia, government, and private industry. There's DARPA spectrum

challenge winners, those who are a member of IEEE with many, many publications, and then also experienced both within the United States and internationally. So as you hear the talks from these experts that you see on the screen, I would encourage you to type questions. And if you see a question you like, make a note of that and I'll be watching so we can ask questions to the panelists. So then, we will move to short presentations by each panelist, and then we'll have some discussion afterward.

So we'll start with Mark Gibson. Mark is responsible for developing domestic and international business opportunities for CommScope. He has over 36 years of spectrum management experience. He leads both technical and business development efforts for numerous wireless and spectrum related products and services. And it's also important to note that he's led efforts to address spectrum sharing between the federal government and commercial users, and also have significant experience and leadership responsibilities with regard to the CBRS efforts that have been ongoing. A member of CSMAC, he also has been a co-chair of working groups related to spectrum sharing and data exchange issues. And I also think it's really interesting to note that he is also a pilot and when it comes to collecting data, he has experience actually collecting it from his airplane, which is exciting. So with that, I will pass it over to Mark for his presentation. Thank you.

### 3.6.2 Mark Gibson

GIBSON: All right. Well, thanks, Ashley. And I thank you for that introduction. What I'm going to do is kind of give a background on a project that we worked on and we worked really closely with some of the folks from ITS back in AWS3, which was about seven or eight years ago, where we did some airborne spectrum monitoring that helped inform some of the spectrum allocation policies. I write—Spectrum allocation is probably a little strong, but at least a spectrum sharing policies related to commercial federal sharing of AWS3. So next slide, please.

So the premise going into the discussion is really bate—regulatory databases are really insufficient to fully characterize spectrum usage. You know, we find that, you know, all the regulatory databases that we use in commercial are usually the FCC databases, and then federal folks use the GMF, which is the Government Master File. You know, these are regulatory databases. They're not necessarily engineering databases. And so not only do they lack the information needed to do spectrum and characterization, they also sometimes contain errors. And so, you generally need to get out there. And from Doug's presentation you saw earlier on spectrum monitoring is really the way to do that. We find that spectrum occupancy measurements and usage measurements can help inform decisions on how to use and share the spectrum and that's what this presentation is supposed to show. And then I'll show you how we did this for AWS3. So next slide, please.

So the idea behind this, this again, goes back to the AWS3, if you remember the AWS3 is the 1.7 and 2.1 gig band. The 1.7 is the uplink band, which is the lower power portion, and that's what you see there in the diagram to the right. And so this got pulled into under the Commerce Spectrum Management Advisory Committee at the time to study how you could share spectrum

with the various what they called equities at the time, they were using that band, I believe there were a total of five different categories of those types of systems. We were dealing in this situation, actually, with airborne one. And so what happened was CSMAC was formed—formed these working groups and there had been work done initially by NTIA. And then there was also additional work done within the context of the CSMAC work to characterize the facility for spectrum sharing, at least in the uplink.

And we found that through the course of the discussions and interaction, that the assumptions that we were using were really worst case, so—or highly conservative. So what we wanted to do was to get—And actually, in these worst case assumptions led to very large exclusion or protection zones around the systems. So what we wanted to do was to find out what real world measurements indicated. And so that's what we did, is we did some real world spectrum occupancy measurements at an airborne approach, mostly because we wanted to characterize something what UE power looks like at an altitude that could approximate an air combat training system. So next slide, please.

So what we did was we did a series of airborne measurements over D.C. I apologize, the diagram in the upper right is the same as the diagram in the upper left, I just noticed that. But basically what we did is we flew arcs around the D.C. area with a spectrum monitoring system outfitted to the aircraft up to and including an external antenna. We use the CRF – CRF SRFI node. And I don't have a picture in this presentation of that, but I can certainly show people if they're interested. And we do develop test plans to fly the circular arcs at different altitudes just to characterize UE power at altitude.

And these altitudes, if you can see in the lower diagram to the left there, the altitudes were at 1,000 foot increments between 3,000 feet, and 10,000 feet were possible. As most people know, the D.C. is a complicated airspace. We also flew in Norfolk, and the idea behind that was to sort of de-correlate any multiple activity we saw from UE powers in D.C., because at altitude, especially at 100—at 10—at 10,000 feet, the radio horizons about 120 miles. So over D.C., you're seeing Philly and other areas and we flew down in Norfolk, you wouldn't be seeing that much.

And so, frank—basically, what we were trying to do was to characterize UE power at these altitudes so we could get a sense as to what effects clutter might have. And also, we put a source in the D.C. area, transmission source, so we can also just characterize propagation loss. And we worked with the folks at ITS to do some of this and we were able to confirm from the test measurements that we collected that propagation kind of follows along RF77, which is an error on propagation, might actually follow very well, so that was good. And so if you go to the next slide, that really states the results.

So basically, the results indicated that the UE powers and altitude were less than predicted by the propagation models that were used for the original analysis. That ultimately does work on shrinking the protection zones for either a combat training system. So, if we had only relied upon calculational methodologies to determine these zones, we would have been restricted on spectrum use, and so that's basically that shot of this.

The other thing is we found at altitude, given that you can see very far, we saw some rogue signals. So that blue line there you see in the spectrum plot is a rogue signal, which we found interesting. So speaking of which, I have one more slide that's not part of this, it's a CBRS. Can you go to the next slide, please? So, we were curious early on in CBRS to see what the spectrum looked like in areas where there shouldn't be any radar operations. Or if there were, to see what radar operations look like, so we did a little flight. As Ashley said, I'm a pilot, so we outfitted an aircraft with the measurement gear and took a short flight, about an hour and a half down to Richmond, we didn't land, we turn around and head back up. And we had the CRFS gear going the whole time measuring between 27—or 2,900 and 3,700. And what we saw was if you look at the spectrum plot there, it's also the waterfall, we saw basically was radar signals and bands where there should be nothing.

We don't know what this is. We thought—And in fact, I sent this around to several folks, sort of off the record, just trying to find out what could be going on. And so, this basically just underscores the value of spectrum monitoring. But not only that, but spectrum monitoring, you know, above the clutter. You know, again, we were 11,000 feet, and so the horizon distance at 11,000 feet is 150 miles, so we can see a far piece, but that was the intent of this effort, because we wanted to see if we could receive radar signals. But instead, we saw a lot of what you see in that upper—that spectrum plot, which was rather confounding, given that there shouldn't have been anything there. So if you go to the next slide, this summarizes my conclusions.

So again, reliance on spectrum databases and regulatory information is insufficient. It's really important to get out and do some good measurements using good metrology and, you know, working with the folks at ITS, that is the best metrology you're going to see. It also informs allocation consideration, especially sharing is being considered. We're thinking perhaps that could be used in the new allocation for 3,450 to 3,550, and that's basically it. We also think spectrum measurements can be used, obviously, for interference detection. We do a ton of that but, you know, there's not enough time to get into that. So with that, I think I'm done. And so thank you very much. And I think I can handle a couple of questions. If not, we can do them in the panel discussion. OK, great. Thanks.

ZAUDERER: Great. Thank you, Mark. Any questions from the panel? I have one question on—you mentioned a little bit the comparison of the observations of the data, comparing them with models, and also the question of interference and occupancies. So what do you find to be the biggest challenge? Were there some discrepancies between the data that was collected and the expected models when you compare that or is it really more important in terms of trying to understand the occupancy and interference?

GIBSON: Actually, that's a great question, Ashely. It gets to the crux of the effort. What we did is we worked—This effort was done on behalf of the wireless carriers. And what we did is we worked with them to back out proprietary per KPI data on the operational parameters of their systems, which when these initial analysis were done, there was no way to do that. And so all they had, I believe these were analysis done through CSMAC work, all they had was the data that's typical for, you know, these handsets that are published by the manufacturers. When we actually applied real KPI data, in terms of busy hour usage and that, we were able to actually

correlate that to the measurement data and determine the impact primarily was the application of KPIs. So in fact, handset powers had a time duration, duty cycle and whatnot and other power limitations, and those are things that we actually saw in the data. And I should mention, we had about four and a half million data points with all of this, so there was tons of data. That was the main thing we found.

### 3.6.3 Michael Schwab

ZAUDERER: Great, thank you. I'm sure we'll come back to this discussion as we move through. So the next talk is by Michael Schwab. And it's a great segue as he is a vice president and partner at umlaut, over 25 years of experience in electrical engineering, wireless communication, systems engineering, and interference mitigation as well as business development. He has a degree in electrical engineering, and he has been at umlaut for more than 18 years, since 2001, and in the United States since 2010, working on benchmarking, for networks, also hunting mitigation for interference, and recently with telecom security and cybersecurity. So with that, I will pass it over to Michael.

SCHWAB: Hello. Thank you very much for having me on the panel and the kind introduction. So I'm coincidentally pilot too as Mark as he just announced. And I'd like to spend a few minutes on the data collection and monitoring to focus on two aspects of PC interference and interface security.

The network carriers are collecting a huge amount of network performance and spectrum information. The data is typically used for regular monitoring of the network to identify performance issues, outages, and also capacity issues, as an example on cell level or wider geographical area. The data can also be used for network optimization and troubleshooting. The availability of so-called network counters depends on the run vendor, as all have their own understanding of standards and implementation. Moreover, it depends on the radio access technology, software releases, et cetera. And the maturity of the deployment also plays a role.

Vendors initially focus on the most important information and roll out more later on. As we transition to my next slide—Well, second slide already, I'm just still forward, networkers have the ability to monitor the spectrum and on an aggregated level on PRB level for LTE as an example. This is available for all frequency bands use by several carriers. In contrast to this, spectrum information is not available in down direction, as the handsets of opposite different capabilities and a much smaller compared to big base station. The downlink information is recorded by the network, but also by crowdsource data providers such as not to further use the data for optimization. Next slide, please.

The capability of spectrum monitoring, the network carriers has also the possibility to identify external interference. Operators spend billions of US dollars to license a few MHz of spectrum and want to assure that they can use the spectrum properly. In the field spectrum related to performance degradation, but the network operator licenses spectrum, the frequency band is neither clear of interference, not previously legally operator devices. If you look at the rather—

recent 600 MHz addition, similar devices are causing problems as for the 700 MHz spectrum deployment 10 years ago.

Just as an example, a lot of wireless microphones are still operating in the 600 MHz spectrum. We found a lot of these in short respect and now again. There's a tendency that low bands are much more often external in the field, the live bands and higher frequencies. It will be interesting to see which kind of devices will be active in the upcoming CBRS bands. Limiter base bands are much cleaner, though. Patchy requires a clean RF spectrum compared to LTE and UMTS to achieve higher spectrum efficiencies. Hence, there might be an additional need to clear the spectrum, which was doing fine for all the radio access technologies. Our third dimension wireless microphones, intention radiators, a lot of external interference problems caused by non-intentional radiators in the band of interest. Picture on the right shows you one of the most common offenders harming 700 MHz networks since more than 10 years and are certainly also interfering the 600 MHz band. The cable TV equals—issue allocation also depicting 850 MHz bands, which are used for UMTS, LTE, and just recently used for dynamic spectrum sharing between 5G and LTE. Cable TV equals problems are very often caused by that installation quality and questionable influence. In the picture, you can see a cable TV amplifier, the gray box in line and several corrector splitters, including huge amount of loose cables connecting to the splitter. You can—Imagine it's only a matter of time, wind, whether, wherein so to the TV signal is irradiated.

Other very frequent interference devices for cellular networks are cell phone boosters, wireless phones, designed for foreign markets with tech phones, but less cameras, light ballasts, and light fixtures as well as baby monitors. So this fits nicely to the list that Sanyogita of Verizon shed in an earlier session today. Network monitor interference are the only addressing fraction of the interference issues if performance degradation is really very bad. Most major carriers in the US are certainly far more than 1,000 export interference problems annually. They certainly have interest to further analyze the available data to estimate the actual amount of interference problems and impact on coverage. Defense mitigation can be lengthy and costly process, especially if offenders are not cooperative in the SSB needs to be involved. The offenses can become costly for the offenders as well. The vast majority of interference problems are- can't-cannot be solved with the support of the culprit, without any financial impact on the culprit. Next slide, please.

I'd like to jump to a different topic, interface security to start to connect to the two topics of this interference. There are plenty of measures in place to reduce and limit the possibilities of impersonation, deception, and tracking except for users in place. 5G will further enhance possibilities. However, the setup is also becoming much more complex, especially in the non-standalone mode, with three or even four radio access technologies are running in parallel. This opens new tech vectors. 5G will not yet entirely overcome the possibility of the interface security concerns caused by fake base stations.

Come back to the interference topic, intentional interference can be used to jump with 5G connections. If certain 5G frequencies are uneven, or unusable and the fake base station is best available to cell, the handset may use the fake base station. Especially in older radio access

technologies, there are easier ways to actually—to set the traffic and be the man in the middle. For a few hundred dollars, you can build such fake base stations, with some knowledge, of course. Network carriers may need to establish additional monitoring and also use top source data to localize more 'stingrays', so called, which another name for fake base stations. Earlier today, we learned from Drew Morin of T-Mobile about the efforts of the T-Mobile carrier about fake base stations. Umlaut does a lot of traffic testing globally. The data allows us to analyze the radio information in regards to security concerns. Not all carriers, we observed, have the same interface related mechanisms in place. Default configurations for other misconfiguration may be an example to reduce the usage of that's available in production. I would like to stop here, because my time is over, and hand it back to Ashley. Thank you very much for your time.

ZAUDERER: OK. Thank you, Michael. We have one question from the participants watching. Can you quantify or elaborate on the statement that was made one of your slides that 5G requires a cleaner RF spectrum compared to LTE and UMTS?

SCHWAB: Yes, certainly. So this was already the case when you compare UMTS versus LTE, so the technology support lowering those flaws. And if certain criteria are not fulfilled, then higher modulation coding schemes cannot be applied, which is the effect for high throughput as an example and higher performance.

### 3.6.4 Bob Baxley

ZAUDERER: All right, thank you. Any questions from the panelists? Yes, Kaushik. Can you try again? I think you're still on mute. OK. You are still not coming through, so if you can hold that question and we will come back to you. OK. So with that, let's go ahead and move on to the next panelist, and hopefully we'll get the audio worked out with that. So the next panelist, it's really interesting that we discussed unintentional interference, but then there was a little bit of a move to the intentional interference, so that's a perfect segue to the next speaker, Dr. Bob Baxley. So he's the co-founder and the chief technology officer of Bastille, which is the first cybersecurity company to detect and mitigate threats from the Internet of Things. Prior to starting Bastille, he was the director of the Software Defined Radio Lab at the Georgia Tech Research Institute. So he has expertise in signal processing, machine learning, radio frequency projects, and it's also the inventor of 27 patents related to radiofrequency wireless signals. So with that, I will pass it over to Bob for his presentation. Thank you.

BAXLEY: OK. Thank you, Ashley. Thanks for having me. So I thought I'd give a little bit of context about what we're doing in Bastille. And for do that, at the very highest level, we built a software defined radio system that detects submitters in enterprise facilities. Let me motivate that from this, if you click to the next slide. And one more.

So, the highest level, there's billions of emitters out there, there's billions of cell phones, billions of Bluetooth devices, billions of Wi-Fi devices, and then billions of IoT devices. And of those IoT devices, the vast majority of them have radio interfaces. These radio interfaces, they're not all just those kind of big name protocols you've heard out there. They're things like Zigbee, there's

proprietary protocols, long—low power run protocols like LoRa and SigFox. There's a whole bunch of protocols and spectrum and these devices end up in your corporate facilities, and the federal facilities, and they create a new attack surface for your cybersecurity perimeter. If you go to the next slide, please.

In addition to the phones and the Fitbits, and things that you know about, laptops that run on Bluetooth, and Wi-Fi, and cellular, they've also got covert wireless in enterprise facilities, things like DECT headsets where maybe confidential conversations are being had. IoT devices like light bulbs, audio visual systems, and boardrooms, and meeting rooms. On the upper right is a thermostats, so building control systems like that. And thermostats these days tend to be Linux boxes on your wall with multiple RF interfaces associated with them. And then even computer peripherals, like mice and keyboards, you might not know that—know this, but most mice and keyboard manufacturers roll their own 2.4 GHz protocol to push the data between the dongle and the mouse and the keyboard, some don't use Bluetooth. So what this means for corporations and people with sensitive data is you've got this big unmitigated attack surface. Next slide.

And maybe to make that a little easier to think about, you can think about what enterprises do to protect data on their wired network, corporate networks. There's a whole industry of intrusion detection systems, network access control systems, firewalls, advanced persistent threat detection systems that cybersecurity firms sell to big companies so they can monitor the network traffic in their facility. But beside Bastille, there's no—unless you have Bastille, you probably have no visibility into all the RF networks in your space. And you may not even realize that some of your devices, some of your industrial control systems have RF interfaces that aren't being used that have default credentials or maybe you have other unmanaged RF interfaces that you don't realize. So what do we do with Bastille, we help you understand what those devices are in your space so that you can adjudicate them. So two slides.

So what do we do? We deploy software defined radio sensors in your facilities. So they're this this device on the right, it's a little bit bigger than a Wi-Fi access point, and you're deploying them in a similar kind of density as your Wi-Fi access points. On that software defined radio sensor, we're doing digital demodulation of dozens of protocols across hundreds of channels, and that lets us see the L1 and L2 traffic, the unencrypted traffic from emitters in a facility. We see those emissions from multiple sensors, which lets us geo locate the each device inside a facility.

And once you can do that, we have packet information so you can get things like MAC addresses, you can understand manufacturers, sometimes you can understand the model, you can understand which devices are connected to each other in the volume of data flowing between devices. And with all those—all that information, you can set your device policy rules for your facility. Next slide.

So what is the sample policy rule that is popular with our customers is a Bluetooth pairing policy. So you may—We have customers who have policies where Bluetooth emitters are allowed as long as they don't connect to anything, because that connection may imply the data

is moving back and forth. So if you have a really secure facility, maybe you don't want any devices in your facility that have a network connection, and this constitutes network connection. So what may happen is you have a facility where phones outside the facility in a locker, which maybe allow Fitbits to come in, and a user has no idea or maybe doesn't know that the Fitbit is still paired with a phone or with the headset that has a microphone and still paired with the phone. With Bastille, we can see both ends of that connection localize both ends and understand if there is a connection, both the device is no longer connected to the phone. And then our users can use that data set to have alerts. And if they see a violation, they can send someone into turn off the connection. Click.

So another example is cell phone. So we can see cellular emitters, UE inside the space, and localize those and we see them distinctly so we see a dot per phone. As I'm sure all this audience knows, cellular devices have really ephemeral identifiers like [inaudible], so we don't have persistent identity, but we are able to tell you there is a phone here and this is approximately where it is. Next slide.

So with all that data, you can have policies like these devices are allowed. You have policies around your network connections. You can have geo fence policies. These devices allowed in a room, this device isn't. And then with our APIs, you can connect those policies to automated actions. So if a policy alert is tripped, you can have an incident response system, create a ticket and alert IT security person via phone, email, SMS. You can use agents on devices, so MDM is an agent- agents on your computer. And if those devices go into the wrong area, you can disable them. Or you can wire up Bastille's alert since your physical security system. You can, for instance, slew a camera into a room where a device policy violation has just occurred. Next slide.

So how do we do that? We do that by—with our sensor arrays. So our sensor arrays have two software defined radios in them, we've created them from, you know, from scratch. They've got integrated antennas. Their power over Ethernet, we've got their passive, so the FCC certified, there's no emissions coming off of this. And so, we're not having to interrogate devices. And with—All the demodulation happens in FPGA, most of it, which lets us see, for instance, all 79 Bluetooth channels all the time simultaneously without having to jump around and try to follow the hopping pattern or frequency hopping emitters, like Bluetooth, which is low in energy and Zigbee. Next slide.

And then there's an enterprise security system. So the setup is you deploy sensors to your facility, maybe you have many facilities across the world and at each facility, there's an on-site appliance that the sensors talk to. That's called a concentrator and your concentrators are talking back to one central fusion center. And ultimately, you have operators, wherever they need to be, who can see the user interface that fusion center is exposing, and they can use that user interface to decide where dots are, and adjudicate device policy violations. And so that's the—that's what we're doing the best deal. I'll pause there and turn it back over to Ashley.

ZAUDERER: Great. Thanks Bob. We have a question if you could answer, how many monitoring sensors are needed to geolocate? And what is the signal energy level that is needed to detect, you know, how close in proximity do the cell phones or the problem needs to be? And then

secondly, if you could just speak a little bit if this type of technology could be expanded, you know, outside of a building? If there's some interesting applications to geolocation of interference on a larger scale?

BAXLEY: Sure. So the number of sensors we use, you need multiple sensors to see an emitter, you need at least three—we'd like to have five, our deployment model is we put a sensor every 50 to 70 feet. It's hard to peg down exactly how loud an emitter has to be before we see it. It kind of depends on if there's processing gain—coding gain that we get when we demodulate the signal. And it also depends on how far away that device is from an emitter—I mean from one of our sensors. Yes, so for larger scale spectrum monitors, so this is a kind of application spectrum monitoring, except it's not analog monitoring. It's digital decoding. And we're really only looking at specific protocols, what we know devices are. We do have the ability to do spectrum monitoring. We measure power and bands, but most of our customers aren't that interested in that. As far as scaling it out, you know, if you could deploy as large of a best deal network as you wanted. And, you know, one thing we've thought through is, it may be that customers could expose their best deal data in an anonymize way to, you know, government agency, so that you can get distributed monitoring without having to pay for all the distributed sensors, piggyback off investment that companies are already putting into their local spectrum monitoring installations.

>> Great. Thank you. And before we move to the next speaker, I wanted to do a quick audio check because she comes back with us.

>> Yes, I'm back. Can you hear me?

>> Oh, perfect. Thank you.

### 3.6.5 Jim Arnold

ZAUDERER: And we move on to our next speaker. I see there's a few more questions that we'll return to after all of the presentations are done. So our next presentation is by Jim Arnold. He works for the Department of Transportation where he has served as the senior spectrum manager and spectrum lead in the office of Positioning, Navigation, and Timing since January 2014. But he has more than 30 years of experience in research before transitioning to more policy work. And he has his master's of science in electrical engineering from the Florida Institute of Technology. So with that, I will pass it over to Jim for his presentation.

ARNOLD: A little bit different—OK, now I'm unmute, I'll talk. So from a—thank you, Ashley and good afternoon everybody in the—on the session this afternoon. So I do—for Department of Transportation, we take a slightly different perspective on and how we communicate. Can we go to the next slide please?

So, transportations uses may different types of communications for many different use cases, uses different by geography, population density, and different types of traveler's needs. As our mission comes along we expect automated vehicles and infrastructure to also integrate various

types of indications as you'd expect to be a part of these different use cases. And we will have to approach 5G in a way that probably nobody else does from a communication perspective. Or visit the extra vehicle to everything communications, predominantly non network. I provide critical transportation services such as of highly tailored for communication that we use for machine to machine in a rapidly moving environment. And again, look at the intersection here at the bottom center, you've got a lot of different vehicles, lot of things go in different directions.

They often—But they- everybody else is going. We don't have time to set up the network to get access to the network and communicate through that network. So we do it in a broadcast method. All devices in the area from an ad hoc mesh network of sorts out to approximately 300 meters. And that's to be able to vehicle side of it. Then we have big infrastructure which obviously ability to do a form of edge computing. We've got a lot of different things coming into play here. Next slide, please.

The standard communication allows us to address crash conditions in real time and move toward a zero crash transportation environment. As in this respect, such direct communication offers game changing enhancements to vehicle safety mobility. The ability communications where we have messages that are broadcast from each vehicle at a rapid rate roughly 10 times a second, depending on the application and through—and receiving vehicles use that information to determine if there is a potential for collision. For you to warn the driver in the future, they want the vehicle to take an evasive action.

We have infrastructure. We have the roadside devices used to wireless to provide travelers. We have traffic signal information, but we call signal phase and timing, works on locations, lane closures, other roadway anomalies, to both enhance safety and reduce congestion. But we really trying to move from a different—we're trying to give the vehicles more situational awareness so they—that they can avoid crashes and make more efficient use of the transportation infrastructure. Next slide please.

Because our signals are—is predominantly a broadcast signal within an ad hoc network, there isn't a way to really monitor the spectrum and adjust with the devices. However the devices are capable of monitoring or their own spectrum use. We look at the channel busy ratio and things like that. And adjust power levels, address transmission rates, you know, 10 times a second is probably too often you're sitting in a traffic jam. So we reduce that a little bit. It's pretty important in places like Los Angeles for highways with over a thousand vehicles, moving faster forming these ad hoc networks as they go.

By—As they go nearby each other, they're going over arterial streets. You've—There's a lot of complicated interactions there. When you look in New York City where you've got roadside units that are located at potentially every intersection less than, you know, a hundred meters apart. How do you manage those in power and channel usage? They have to be able to do that in real time on their own.

Additional considerations for measurements include naturally occurring ground bouncer [inaudible], urban canyons, Doppler effects, foliage and building reflectivity, and other divisions

of transportation environments across the nation. We are—As a vehicle moves down the highway, it's – the vehicles it's interacting with are changing, the environments operating changes from an urban area to a suburban area to a rural area, and both urban and natural canyons. It's quite a diverse environment, that we have to work through. Next slide, please.

So, one thing we do is rather than go out and actually look at spectrum, we set up test systems that reflect the conditions in order to collect the data that clearly reflects the radio performance and how it accounts for all these various … variations in the environment. To set up our tests we use a variety of data visualization that capture equipment most notably with the Institute of Telecommunication Sciences in Boulder we created our own command and control system allows us to monitor all devices under test at the same time.

We have an upcoming test for the LTE cellular field to everything, where we putting out some 250 different devices. We're going to monitor each one in real time. See what goes on to pull the data back and do some further analysis in detail. And we can see all the over the air exchanges as they're happening. And again, post processes broken into more detail. As 5G is modified to work in this mid-band spectrum ranges and modified to form the ad hoc networks for vehicles, or devices and [inaudible] based broadcast. We also use self-statistic methodology to see how it works make sure that can form progressive ways to deploy applications in a wide variety of challenging transportation environments. And I will note to the graphic is not done to scale but it gives you a general perspective on, what are test configuration might look like. Next slide.

And we're moving towards zero trust environment. From a transportation perspective, we actually broadcast everything in the clear, but we have a certificate to whoever, to a message every so often. And that certificate allows us to verify that the sender is actually within the—is operating within the constraints of the open network. With a—For misbehavior—misbehaving devices we have misbehavior detection and we also have a very strong privacy protections. We're set up at this point so that our—we actually changed MAC addresses, every—let's say 75 to 50 seconds. So, you really—it is nearly impossible. As far as we can tell you, it is impossible. It actually track a single vehicle traveling down the road, because it's always changing. Yeah. Those are the—and that's it. Back to you, Ashley.

ZAUDERER: Great, thank you, Jim. One quick question, I wanted to ask you, you need a dedicated system or can you use the 5G system and kind of related to that someone in the Q and A asked will DSRC be separate from 5G? You know, will the base stations be used for the vehicle communications in a DSRC spectrum? If you can address that, that would be helpful.

ARNOLD: So depending on the application, you can use a 5G network system, you can use an LTE system, you know, there are systems out there today there that are in use. I think of—some of the Google applications where you're going from point A to point B and using that. From a safety standpoint, you know, we're sending messages at this point, 10 times a second, that's every 100 milliseconds. And you've got to find for the vehicle that receives that that calculates potential for impact. Often, it's a fairly quick solution, you're too far away, nothing's going to happen. Or, you know, there's a greater potential for impact. You've got to be able to—those

systems had to be on the same—essentially the same channel. It has to be pretty much dedicated system. You have two different systems so you're trying to translate between them. If you're trying to go the infrastructure associated with that radio network and going back with vehicles, it takes too long. We've actually done some testing with—this was several years ago, so I don't know if it still applies but we were trying to measure the time it took to associate with a network connect and data into the network and get back. It was taking something of just over a second, which from a crash imminent perspective is way too long. For 5G base stations we use for V2X communications to DSRC spectrum. That's a very good question. We've—We're looking at how we would transition from one communication technology to another and there really aren't any good answers just yet. We know that whatever which is chosen today will not be available in 30 years. So there has to be a way to transition. How we do that? This is still a question.

### 3.6.6 Kaushik Chowdhury

ZAUDERER: That's great. Thank you, Jim. And I'll read one question for you to start thinking about as I transition to the final panelist, is Department of Transportation considering the vulnerabilities when you move from a controlled test environment to the real world environment? So you can be thinking about that and the reason I want to transition our final speaker on—he has a lot of experience with on spectrum emulators and modeling and also real world so I think it's something he can still be addressing a little bit and then we'll return to that question in the panel discussion. So our final panelist is Dr. Kaushik Chowdhury. He is a professor in the electrical and computer engineering department at Northeastern University. And he seems to wear many hats as he's also a director in the Institute for the Wireless Internet of Things, a faculty fellow, and he's also co-directing the Colosseum RF/network emulator, and also involved with the Platforms for Advanced Wireless Research projects office. He's so very active. He's won numerous awards early in his career from four or five different agencies, including NSF and DARPA, and the Office of Naval Research. He has his PhD from the Georgia Institute of Technology. And has research interests that span a breadth of areas including deep learning applications in wireless spectrum sensing and spectrum access, networks, robotics, and also wireless RF energy harvesting. So, a lot of really interesting topics. So with that, I'll pass it over to you for the final presentation. Thank you.

CHOWDHURY: Thank you, Ashley. Right, so I'm going to talk to you about a way in which we can obtain this data that, you know, will be heard so far about how important data sets are and, you know, by proper monitoring of these data sets, you can find people who are the legitimate users, people who are intentionally or perhaps unintentionally issuing undesirable emissions in the spectrum. So the question now is, do you think this is important? How do you collect them? And what are the tools and methods that you have as a researcher, as an academic, as an industry person, or as the government to get access to these data sets? And I'll talk about some of these experiences that I've been involved in, in this brief talk. So please, if you can go to the next slide.

So here are the four main focus areas where I feel that these are the sources of five key data sets. So you already heard about the institutional data sets that the NCAA has been collecting—there's a vast repository from NIST as well. So these are—So some of these are publicly accessible, some of these are not. So one of the things we need to do is to build relationships and make it easy for governmental agencies to share these data sets with the rest of the community. So that's something that we need to do.

On the right hand side, you see the importance of crowd source data sets. Now, here's an example FlightAware, which tracks airplanes using the signals that they transmit is a crowdsourced sort of a data set. But you can already see the value of this data set. Now if it takes like a couple of $100 for someone to set up a base station and make a spurious RF signals into the environment, then a similar few $100 could be used in a crowdsourced mechanism to involve concerned citizens where they can become part of the spectrum monitoring process.

So what are the incentives that could be made available for a crowdsourced spectrum sensing environment? This is to me, I think, is a fundamental problem and I'll come back to it towards the end of this topic. But what I probably am going to focus on these two kinds of data sets that we can collect, right. One is the experimental data set and I'll focus a little bit on the power platforms. And the other one is emulated data sets in which you can have repeatable virtual worlds, but you can test things without going into while. And that will go to the Colosseum. To next slide, please.

So, I've been very fortunate to be involved as part of the power project office. Now the power program is $100 million cash and in kind contribution program, which is led by the NSF as well as consortium of industry companies. And what they do is here we are tasked with—as a public project office, we are tasked with collecting and then overseeing the operations of city scale or community scale like experimental platforms, which really push the boundary to something which you can do over the next 5 to 10 years, which you cannot do inside a small lab. So these are real experiments in the wild. And so these are the three platforms that are being afforded so far. And these different platforms are in different stages have their operational capability and that being developed as we speak. So here's some ideas on what kind of data sets that you can collect.

So from the powder data set in Salt Lake City, Utah, you can collect data sets related to software-defined networks, fully programmable stacks. You can actually run a 5G stack on—in the real world on the cloud platform. You have the massive one or MIMO base station that is currently deployed as a country to element base station and they're higher order 64 element base stations are coming. There's COSMOS which has deployments in New York City in which you can experiment on millimeter wave and full duplex data sets is airpower, where you can now mount base stations on UAVs and have base stations on polls and then have interesting 5G dynamic connectivity and testing in a real mobile and aerial mobile environment. And here are two additional rural broadband platforms that are upcoming. You will hear more announcements on this towards the end of this year.

So these are resources for you to go ahead and perform experiments and obtain this data from actual devices in the wild. These are this again scale over the community. So you can actually see the effect of interference of mobility of human actions or vehicular traffic in the wild. So these are the power platforms and the takeaway message is, we need to use these more to reduce the time from experiment conception to data set creation. So you really don't need to invest the time in going to a place. You can just log in remotely and obtain these data sets. So next slide, please.

So, the next one is emulation. So often that experiment are perhaps collecting a data set activity is not mature for the wild yet. So in these cases, you want to have an emulated environment where you can create a virtual world and you should be able to test a variety of different protocols, transmission parameters, configurations in a perfectly safe environment, which is repeatable.

So here comes the Colosseum. The Colosseum was used for the DARPA spectrum collaboration challenge. And after the challenge was over, it has transitioned over to Northeastern University. And at core, it's a massive channel emulator. It can perform a full matrix that is 256 into 256 channel emulation. You—They can be 128 programmable radio nodes. And each such radio node is an extra 10 USRP, which has two data boats in it. So you can imagine it's a pretty large scale system. And on each such software-defined radio video, you also have compute resources such as an FPGA, GPU and other CPUs to run as a host. Now, the takeaway message here is that because you have such a system, you have to be careful about what data you want to focus on and be conscious about the scale of the data. For example, Colosseum generates more data than there are say, bits in the Library of Congress per second once if you operate all these assignments at the same time.

So here is it, what do you do with all this data? You get swamped with it, unless there's a plan to take only what you need. So, next slide, please. You can go next slide. Yeah. I think—Sorry, there was—I think—can we one back. One more back. Oh, anyway, all right. So let's go forward one, maybe it got skipped somehow. OK.

So one of the things that even if you collect these large scale spectrum data sets, the question now is how do you share them? So we are a big proponent of standardized language for sharing. And so one of the things that—and you heard this being spoken earlier is the SigMF format. Now this format is something that—no not that not just NTIA uses, but also we used ourselves when we create a data sets. So what we do is, we can collect and save them in a format that makes it easy to share. There are a number of different parameters of code, the transmitter systems, the frequency, the bandwidth, and all these different features that you can compare to the present in a metaformat. So, here's an example of a SigMF presentation. You can download this data set. It's for other fingerprinting, basically, amateur detection, and you can freely download this that we have collected ourselves. But just to show you that whatever we create, we should be able to share them. And we need a standardized way for this kind of information sharing. So with that, I think I'll stop here and then we can have more discussions.

ZAUDERER: Great, thank you. When you talk about the need for standardized data sets for usable or existing data sets when you try to access and do studies, can you speak to that?

CHOWDHURY: So there's always going to be a problem on what existing data set can you use as is. Now, when we went back and we tried to look at what data sets are available, you will often find that it may not be very relevant and current in the sense you may not find that I've saved 5G NR waveforms that have been transmitted over the air and you have collected these 5G NR waveforms and the receiver in an interference environment. That data set may not exist publicly at least for an academic to use. So I will say that it's—I'm not very—what I believe is that we need a spectrum aggregation or a data factory, as you may call it, right? If we are in the data revolution today, then what's going to drive which is a data factory, and we don't have that. So that's what we need to create. And we can do this through these power platforms, Colosseums and other data sets that are available.

### 3.6.7 Panel 3: Q&A

ZAUDERER: Great, thank you. So that brings me to a question that was asked, and if a panelist just raise your hand, if you'd like to address it, given the focus on the benefits of expanded monitoring, what precautions do operators of the monitoring equipment need to be aware of to avoid violating the nation's wiretap laws, and generally making sure that it's anonymize appropriately such that you're able to share these data sets? Any comments? I know, Michael, for example, you've done some work on, you know, specifically for wireless carriers. But your company also does some more generalized work. What is the difference there in terms of, you know, when you collect data that you release and publish more broadly versus when you're doing, you know, work that's private?

SCHWAB: I mean as long as we've collected data for measurements that we do ourselves, I don't see a big issue. It's more the passive data collection, where you collect spectrum or the—if you only collect spectrum information, you may not—certainly not able to easily decode. So there's—you can only identify this some usage. But I'm also not in the legal domain, power cost data collection certainly, there are a lot of rules to follow similar things that the FCC experienced back then when they collected their own data or code data program as well. So there are, of course in Europe GDPR regulations to follow and I think there's a strong one also in California, some of you might answer.

ZAUDERER: Do you have other comments on that question? OK, seeing none. I'm going to return to the question that was asked on just after Jim Arnold's talk, whether the DOT is considering vulnerabilities to the intelligent transportation systems when you move from a test environment to a real world environment, and then what else be great if any other panelists wants to weigh in on challenges or vulnerabilities that you've seen on—in the real world environment for maybe things that were not expected when you model a system? I will start with you, Jim.

ARNOLD: Thank you, Ashley. Yes. So I will start out by saying the transportation officials tend to be very risk averse. They really want to make sure things are working very, very well before they introduce them to the public. It's a really quite surprising how long it takes to from a final product to deployment. And as part of that process, yes, we do some very one-on-one control testing. We do some larger field testing where we have multiple vehicles in a very controlled environment. And then we do a small scale or even a larger scale, model deployment. It's in those smaller planes we tend to do run across issues that we wouldn't see in the smaller tests that we have to resolve. And that is well before it goes out to the general public. It's—That's one of the reasons it takes so long to move things from a—from concept to deployment and transportation arena. Now, like I love the example of the digital detectors for intersections. We used what we call loop sensors. Wire is buried in the road to detect vehicles going over for years and years and years. And back in the late '80s, early '90s, there was the development of a technique vehicle that could detect whether or not there was a vehicle in the air entering the intersection. And it took 15, 20 years for that technology to become widespread. And that was a fairly basic thing. But we didn't want to—we want to make sure that the—that folks didn't—there was a pull up to the traffic signal, they were actually detected. Because we all know when we set a traffic signal to or we go to patient, I know I do. So, we want to make sure that that type of able to recognize. But that's an example. So we do, in fact, look at the larger scale model deployments. And even after that, we continue to collect data to make sure that the deployments. What we're using is effective and meets the needs.

ZAUDERER: Yeah, Mark.

GIBSON: Yeah, you know, so it's an interesting question. We have often been called to do interference detection measurements. And so in situations, and I think somebody mentioned the track—the typical, you know, light ballast case. But there—it's interesting. So there's one situation, we've had another situation we have in CBRS, as a Spectrum Access Service—System provider or SAS. We had to work closely with the Enforcement Bureau to address the line between their responsibility and the census responsibility for interference identification. As most people know, the FCC has sort of decimated the Enforcement Bureau to some extent through cost cuts. So this is going to happen in six GHz with the automatic frequency coordinating system. So the one bright—lightweight line we have here is we're not at all collecting data sufficient for evidentiary proceedings. So, you know, if the misbehavior is related to just somebody really being an active rogue operator, the—we're not collecting that data, at least we aren't—we do our measurements and we're pretty clear about that. But if we're out there trying to do a troubleshooting measurement where, you know, all the—if the parties, all they want to do is resolve the issue and actually, that was a question that came up earlier too, how is that information shared? And you know a lot of it depends on who owns the data? And that's a big question we deal with often. But for the most part, the people we're dealing with are willing actors and they're—they want to resolve the problems. And I don't know, with exception, maybe one or two situations in my entire career, where we're going to actually had to get law enforcement involved. And those are because of people using jammers which they are—and I remember specific situation which we won't get into where somebody was using a jammer and we actually found it and actually had to call the local law enforcement to have it removed. Again,

that's an edge case. So like I said, most of the data we collect is not- is really used to resolve the problems and it's resolved among the actors.

ZAUDERER: That's helpful. Any other comments on vulnerabilities you've seen moving from, you know, a test environment to the real world.

BAXLEY: I'm not sure about test environments in real world, but I can speak to some of the airborne vulnerabilities we've seen, and that have been released in the security research literature. So, there's lots of people who have demonstrated various forms of malformed packet injection. If you've got a digital communication system, and you send a packet that the parser is not expecting, you can do simple things like have the system restart, you can get the system to deadlock, where it doesn't restart. And people have even demonstrated over Bluetooth and Bluetooth Low Energy, for instance, being able to inject carefully crafted sequence of packets to take over machines. So they get remote code execution on the whole constellation machines, Linux, Android, Apple, and Windows boxes. So I think and really, it comes down to whoever wrote the protocol decoder on the system on chip that's doing the decoding, there's some corner case that didn't get taken care of very well. So that's certainly a security issue when you're thinking about these things. We're probably all maybe we remember back to—when the Tesla was hacked at Black Hat a few years ago, they were able to exploit some problem in the WiFi credentialing of Tesla's so that you can connect to the Tesla and take over it and have it start driving without authorization. So it's definitely a very tricky space. And there's no real easy answer, except visibility of your interfaces, and then pen testing and then quick patching when you find a vulnerability.

ZAUDERER: Yeah, Kaushik.

CHOWDHURY: Just one quick follow up part here. When we started to look at this, you know, we realize this problem as well. One approach that we could use to address some of this is perhaps to do something like an RF fingerprinting on trusted devices, and do that at the physical layer. Even before bits are formed and sent up for processing, could we identify an amateur as a trusted one versus maybe someone that masquerading or just an unauthorized transmitter? So could it be that the legitimate transmitted is just going off because its power amplified is off? Or is it because someone new has come into scene? So we could do that using RF fingerprinting. It could be one approach.

ZAUDERER: One question I wanted to ask that they came in. There was a number of questions about if you restrict with Bastille on the well identified bands for cellular service, or if you scan from 25 MHz to six GHz inclusively, and kind of related, do you plan to expand the frequency range from six GHz up to 7.125, that that band is opening up to WiFi and other unlicensed devices?

BAXLEY: Sure. Great questions. The – our scanning schedule is configurable. And you know, there's some opportunity costs because the front ends, they can't see that entire range all the time. So if you're looking at one band, you're not looking at another. We have some default configurations that we deploy for people and most customers choose to just look at the bands

where they know traffic will be—and then occasionally scan bands where they're not sure if there will be traffic there. So, that—there's a there's a little bit of a science to understanding when you scan, where you scan, and it depends on your use case. Ah, yeah, with the WiFi—was it 60 up to 7.1 gigs. I can't talk about our future product plans. But yeah, we've got—we're thinking about how to address that.

ZAUDERER: Great, thank you. Another question that just came in, it's really interesting is, is there a plan or effort to measure the noise floor, again, it was noted in this question last time was in the '70s. And I will say from the radio astronomy perspective, with receivers that are a million times more sensitive than standard telecommunication devices, a lot of the rules were written for, you know, thresholds from a single device and so the aggregate impact of a lot of devices really does matter. You want to know what the noise floor is, and how that may affect things in addition. So it's—are they, if panelists aware of plans or efforts to measure the noise for more broadly, specifically, as it relates to 5G in your applications, Michael?

SCHWAB: I think if I'm remembering correctly, there was a kind of memo a few years ago by the FCC to receive information about how to realize such an effort, but haven't heard anything since.

ZAUDERER: Great, thanks. I think that's a very good question. So, we'll note and I think continue to evaluate. So let me see, we have about seven minutes, there have been a couple folks who would liked a question that I think is really interesting. I'm going to direct this first towards Michael, but if there's other comments, please feel free to wait. And—Is there an effort across the carriers to share interference reports to help with the resolution and document known signals? And also related to this, it might be interesting, if you address the issue of the unintended transmitters? And if there's any documentation of, you know, like you mentioned, you know, devices like the wireless microphones, and this idea of trying to understand a system's lifetime and when you might be getting interference from an old wireless device and do carrier share that information as well.

SCHWAB: Yeah. I think Mark and I have responded to this a little bit already via text. The answers were slightly different. I'm not aware of that the carriers exchange this on a regular basis, or if there's any communication channel, that in the carriers. So there's certainly exchange because people move around. And that this kind of spectral pattern was certainly reported to the FCC, if there are escalations. Or if there are new devices, which occasionally happens, that are suddenly showing up in the market and causing interference. The FCC is able to collect this information.

ZAUDERER: Great.

GIBSON: Ashley—Yeah, to add to it that the carriers do is what I put in the chat. The carriers do collaborate on, you know, adjacent market issues when there's interference before and after the fact. You know, they work together to ensure that they keep the signal strength, you know, at limits, where they where they need to be and the SEC rules generally require the carriers to collaborate on resolving matters of interference, and they leave it at that. So, you know, there's been several programs, they've developed over the years to work on that. In fact, there are people that are responsible, they call it compliance within the various carriers to ensure things

like that happen, other electromagnetic compatibility issues and RF exposure issues are dealt with. So there's a process to do that. We are familiar with a situation that occurred in the 2.3 gig band where there was a lot of work done between carriers when that first band was made available to collaborate on code resistance issues, I'll just leave it at that. So, there's a lot of work that gets done. It's mostly the grassroots level between the carriers and, you know, they get it worked out for the most part, and you never hear about it. So—But it's, I would say it's institutionalized, other than them and, you know, responding to the requirement that they have to collaborate and cooperate on issues related to interference.

ZAUDERER: Great, thank you. Five minutes left, I want to give each panelist a few moments to just reflect on what you think the biggest challenges in data monitoring and biggest opportunity that we have, you know, in the coming—in the near future. So if you can think about kind of biggest challenge that you see in a data monitoring, whether it be technical or, you know, a policy level challenge, that would be great. And then as you're kind of starting to think about that, I just want to remind the folks listening that there'll be a chance to join breakout rooms. If you have a question that was not addressed, feel free to join the breakout room of that particular panelist, and you can address those questions there. So with that, I will start with Mark.

GIBSON: OK. You know, I think one of the big problems and the challenges is how to manage that metadata? You know, we've gone now from having to actually be data scientists to manage that data. And so, you know, it's interesting, I mentioned Sizmek, one of the recent Sizmek questions we've dealt with is how can NTIA get better data on commercial operations? And so we're realizing that, you know, the data comes from disparate sources, not just monitoring, but monitoring, and then you correlate that with other data sources. So I, you know, I think applying big data and data science applications to spectrum monitoring is probably something new that we need to deal with. We're aware of several companies that do monitoring. One of them actually does airborne monitoring, actually. And they are—they collect, you know, when you collect IQ data from spectrum monitoring, it—you're getting a whole lot of data. So not only is it trying to do data mining, it's dealing with just the huge, huge amounts of data. So, I'd say that's one thing, and then there's, you know, I think you've seen it in the chat, probably some policy issues around, you know, who owns the data? But, you know, for now, I think mostly what we're collecting is spectrum usage data. And, you know, I think the data is owned by whomever collects it, so.

ZAUDERER: Right. Michael, what do you think the biggest challenge is, and I'll just serve out somebody commented incentive to collect data in aggregate, one of the challenges or problems, Michael.

SCHWAB: Good question. I mean, the amount of data is just increasing the amount of frequency bands, so there's much more work to do. The network carriers are not necessarily increasing head count in the engineering domain. There needs to be a lot more automation and possibilities to deal with spectrum issues, other than the old fashioned manual way that someone's looking wide a certain sectors performing well, and then he's busy for two hours to

find out its interference and then dispatches of company or going out in specific or days to find the source.

ZAUDERER: Right, Bob.

BAXLEY: So I think more of an opportunity. I mean, there are so many RF devices out there that are implicit sensors if there was a connectivity layer, where these sensors could already be exploited. So best deal when pretty sophisticated sensors, but even your theoretically your phone or a low level consumer devices that are already internet connected, see some of this data, maybe you can see harmonics that you could do some inferences on. So that spectrum collaboration challenge was an interesting proof of concept where you could have a collaboration layer, where the devices could communicate, sensing information, and then you could use these distributed devices that are already out there. And it's very expensive to do monitoring campaigns. So, if you could distribute that and use and come with devices, that would be fantastic.

ZAUDERER: That's great. And we're right at time, so kind of intended 20 seconds to Jim. What do you think the biggest challenge or opportunity is?

ARNOLD: So I think I'll go along with some other folks who says the data, but how do you visualize that data? I feel that's the big thing. We need to get away to look at it very quickly assess what opportunities are there.

ZAUDERER: Great, thank you. And finally, Kaushik?

CHOWDHURY: Well, I think there's a great opportunity and be able to combine institutional data, emulated data, experimental data and crowdsourced data. We need an entity that sort of aggregates, absorbs this and makes it available to the community. The opportunity is really because remember to do this, to be successful, to continue to lead this movement in the US, we need to train the next generation of wireless data scientists. And they can only do that in education institutions as they grow up as it's sad to see these data sets from the ground up. So we need to make this available to them.

ZAUDERER: Wonderful. Well, thanks so much to all of our panelists, and I'll pass it back to our moderator. I think to give any other instructions for the breakout room. Thank you.

THIESSEN: Yes, thank you very much, Dr. Zauderer and thank you, everybody for participating in the panel. So, now as you know, we're going to go another breakout rooms for the one-on-one interaction. So, for our panelists, please make sure to remember that you close the app and click on the link for the breakout room, so we don't have any crosstalk. For those that are participants, so you can access the breakout rooms in the iStartup, or you can use the links in the confirmation email that you receive. So, I look forward to seeing you in the breakout rooms and thank you very much.

# 4. DAY 4: AUGUST 13, 2020

## 4.1 Keith Gremban: Introduction of Technical Presentation

GREMBAN: Good morning, everyone, and welcome to day 4 of ISART. I'm Keith Gremban, I'm going to be the moderator overall for the day. I'm a professor with the University of Colorado Boulder, formerly with ITS. And so, ISART has been a big part of my life for a number of years. I certainly, hope that everybody's been enjoying the conference so far. I certainly have.

A quick note that all the presentations from earlier this week are up on the ISART website. Today is going to be a big day. I'm going to be wrapping things up with a bang. So, a quick overview and we're going to kick the day off with a technical presentation from Dr. John Shea, one of the members of the GatorWings team that won the DARPA Spectrum Collaboration Challenge. The challenge was interesting in that demonstrated the potential of collaborative AI to efficiently and effectively manage, and dynamically manage spectrum. Beyond the technical presentation, we have two very interesting panels today. The morning panel is going to cover implementing resiliency in pro-trust network operations. And the afternoon panel will be bringing it all together with some new insights and novel connections. I would look to this panel for some real out of the box thinking.

A few notes on logistics before we start. First, please feel free to ask questions online during the presentations and panels. To both the questioners and the panelists, remember to spell out acronyms. Moderators, please remember to look at the questions that are in the QA section on the right side of your screen. Attendees if you would vote on those, then it'll be ordered and the most popular questions will be asked first. We'll also try to take unanswered questions into the breakout room. And please remember to take advantage of the breakout room. We are—these occur right after the panels and we're trying to the greatest extent to replicate in a virtual environment these critical one-on-one interactions that happen in the hallway. So there will be breakout rooms after every panel. Just a reminder to everybody after the—each panel concludes the speakers and the panelists. The moderators and panelists will move to the breakout rooms. Please be sure that you exit the events screen you—BlueJeans Events before you enter the breakout room or there will be crosstalk which will disrupt the event.

For those of you who can download the brand new ISART app all the information and links you need for breakout rooms are in the app. For non-app users, the ISART confirmation mail that was sent to you last Friday has quick links that will contain a link and phone number for all the breakout rooms. And for each breakout room there will be room hosts that will be there to help if needed. If you run into technical difficulties, you can reach out to conference service staff, that's also listed in your confirmation email. Quick technical note, that the code to access the main sessions on the BlueJeans Events is the same each day. So if you have issues with link, please just try the next comparable link in the ISART app to help you with this. By default, the only information anyone will see on the app is your name and affiliation. So, if you're interested in chatting with others networking, exchanging business cards, remember you go into the app and add whatever information you're comfortable sharing. So I'd like to encourage everyone to

use those tools to ask questions and converse with panelists and presenters in the breakout rooms. I've been in a breakout room at every session and it's been getting better and better and more seamless over the week. So, I think you'll enjoy the experience.

So with the administrative notes out of the way, I'd like to introduce Dr. John Shea from the University of Florida. John is a professor in the Department of Electrical and Computer Engineering. His research is in the areas of wireless communications and networking with an emphasis on military communications, software-defined radio, network autonomous systems, and security and privacy computer in communications. He was co-leader of the team GatorWings, which was the overall winner of the DARPA Spectrum Collaboration Challenge, which was DARPA's 5th Grand Challenge, which the teams use software to find radios to implement intelligent radio networks for collaborative spectrum sharing. So, professor Shea is going to give us a high level overview of the Spectrum Collaboration Challenge. So, I'll turn this over to our first speaker, Dr. Shea.

## 4.2 John Shea: Lessons Learned from the DARPA Spectrum Coliseum Challenge

SHEA: Hi, Keith, thank you for the introduction. So, we can go ahead and I'll try to just give you a very quick some lessons that we learned from the DARPA Spectrum Collaboration Challenge or SC2. And I'll just try and give you an overview of the challenge as well the beginning here, so if we could go the next slide.

So, as Keith mentioned, the SC2 is DARPA's one of DARPA's Grand Challenges. It was a three-year competition to develop and demonstrate the potential for intelligent agents from diverse teams to perform dynamic spectrum sharing. Next slide.

Now, unlike systems like CBRS in the SC2, teams must optimize spectrum utilization at timescales of seconds. And in the presence of diverse users, time varying traffic flows and incumbents. DARPA did not require any specific frequency channelization or didn't even require that teams use a frequency division approach. So, it requires a much greater level of intelligence, to achieve that, then traditional resource optimization. Next slide.

The spectrum decisions are fully distributed. There's no central infrastructure involved, such as the spectrum access system and CBRS. DARPA also challenge teams with a variety of incumbents, Active Passive incumbents, and then different types of interferes, and they're required teams to perform distributed sensing and reporting. Next slide.

The main conclusion that we took from the SC2 is that real time distributed spectrum sharing is feasible today with existing technologies. I think that was well-demonstrated, if you watch that SC2 championship event. At the same time, we could see there's still a lot of work that can be done to improve the efficiency, ensure privacy and security, and develop schemes that will incentivize what we good spectrum usage behaviors and enforce violations of spectrum usage policies. Next slide.

So, a typical spectrum sharing scenario in SC2 looks something like this, there are up to five teams or networks of radios communicating in a frequency band. In the championship event, each of these teams would have 10 radios, so 50 different radios trying to access the same spectrum. In addition, many of the scenarios also contain other non-collaborative radios, such as different types of incumbents and jammers. And then there is a lightweight collaboration protocol called the CIL that allows the teams to exchange some limited amount of information such as spectrum location, and geolocate—spectrum usage and geolocations. Next slide.

So, we're scored, and yes, set, yeah. Oops, right there, that's perfect, and each team's score dependent on their success in delivering a vast variety of IP traffic. But the score is also dependent on the performance of the other teams in the match through this equation that you see here. And basically, what this equation does is create a mixed cooperative and competitive game, there's a threshold for each stage of a match. And if any team falls below the threshold, then every team just gets the minimum score among all the teams. So, you want to encourage everybody to get up to the threshold. That's the cooperative part. And then if every team gets up to the threshold, then each team score is their overall number of points score. So it's a mixed competitive cooperative game. Next slide.

And if you could go and fill this out, up through the bottom line, step through it, there you go. Yeah. So, spectrum sharing in SC2 is based on this very rich, that but – of information, but the information is also very incomplete. In particular, DARPA prohibited teams from disclosing any information about what they were doing in terms of signaling protocols, strategies, anything like that. There was a complete ban on talking to other teams about that. We don't have any online information about how we or other teams are doing other than estimates the teams generate about that. And so, the teams use the still – the CIL to exchange some information about frequency usage, radio locations, et cetera. And also, some incumbents report usage information. And you can sense the spectrum to determine what is in there and how people, you know, how people are apparently using the spectrum. And so, there's a lot of different sources of information, but information is not necessarily accurate or truthful in some cases. Next slide.

I just want to walk you through a couple of few scenarios real quick. So the first is the Alleys of Austin scenario. One of the simplest scenarios that we had, which is three to five squads of soldiers are moving through Austin, Texas, they are sharing 20 MHz of spectrum and there are three stages. And as the stages progressed, the amount of traffic that is being given to the teams to deliver is increasing. And the teams have different amounts of overlap in terms of their spatial reuse because they are sort of moving through this urban environment. In stage 1, you just have some voice over IP flows and command and control screens. By stage 3, you have very all of that plus many file bursts that come in that are quite large, as well as many video streams. Next slide.

And just to show you an idea of what sort of information we would get out of our own tools at the end of a match. So, on the left, we have a graph that shows the score per measurement period across each of the threes across time and the three stages are mark, these are the three the best teams in the championship event. And so, the scores evolve as more and more traffic is added in to the different stages. On the right-hand side, we see a snapshot of the spectrogram

in stage 1 and stage 3. As you can see, in stage 1, the traffic load is relatively low across the teams. Teams can use find a distributed allocation that's completely disjoint. And everybody can handle their traffic. By stage 3, everybody's transmitting on other teams' channels, and you hope to find the channels that allow some spectral reuse—spatial reuse. Next slide.

A—Slice of Life scenario. Each team sort of represents an internet hotspot with a pool of users around it in a congested urban environment. And the teams have different levels of traffic at different stages. So, in each stage, there's one team that sort of has search traffic. And so, those teams need to use more spectrum to score more points, however, the other teams have some incentive not to let them necessarily score as many points during those times. And, again, when you have this search, you want to find those places where you can do spatial reuse. And so, you can see if you look at a little pie chart, here on the screen, it shows percentage of—OK, so reuse. This time, there's 200% of total, so everybody's overlapping with somebody pretty much. Next slide. So, in the Passive Incumbent Protection scenario, this—the teams must control the total amount of power interference power that's being received at a passive incumbent, such as a radio astronomy antenna, the incumbent is not transmitting on the band, but he's listening to something, let's say from outer space. And he will report to the teams his amount of interference received and his tolerance, which is an ever-decreasing threshold for interference power as the stages go on. And if the teams as an aggregate ever exceed the amount of power that he allows, then the team score zero points. And that's what you see in the graph on the lower right corner. And the third stage is the teams as an aggregate transmit too much power. And there's no point scored, some teams don't realize they have to turn off everything for a while, because the threshold drops so low, and so it gets violated. Next slide, please.

So, in the Active Incumbent scenario, you have an active incumbent here. It's like a vehicular radar that is swooping around, sweeping around, and you have to detect it in the RF spectrum is probably hard to see on your screen. But if you check the slides, you can kind of see it in the detail. And again, all the teams have to avoid transmitting on that channel during the times that the radar signal is present. Next slide.

And then finally, here's the jammer scenario that in spectrograms are the top showing jammer on, here's a constant jammer, the jammer had different behaviors, constant sweeping, hopping, on the right the jammer is off. And then there are many stages with the jammer going through different types of behavior. The next slide.

So, our strategy for the SC2 was basically to build everything as flexible, agile, and robust as possible. We wanted to be able to try to find those opportunities in time, frequency, and space to fit in with the other teams. So, we designed our granularity to be quite small to achieve that. And we tried to have a very robust physical layer to tolerate interference in terms of our coding modulation, adaptive, everything's adaptive. And then definitely adapting as many different things from the physical layer, link layer, network layer, and then we also even have the ability to do jamming to other teams. So there were many, many different knobs we had to turn to control our radio system. And that was one of the things we tried to achieve. Next slide, please.

And if you can step ahead, so yeah, down through yeah, yes. So our spectrum—sharing decision engine basically tries to maximize our team's match score. And that is based on determining which flows we're going to transmit because sometimes DARPA gives us hundreds of flows. We can't accommodate them all. Depends on the interference, environment, lots of different things, which channels are used, which should you use, and which radios should use it. Which flows you send in which little time frequency resource units, which we call it packets. And action space you can see is huge. We had a recurring time slot scheduler that was 10 time slots for epics. We had 400 packets, if we use 40 channels, which was our maximum. We had over 100 flows sometimes. So you can see the number of possible packet schedules we could create was an immense number. Next slide.

And the state space was also huge. The inputs to our decision engine included our team's quality of service information, all of the different flows we had to support and how we were doing and supporting them. You know, how many points they were worth, the channel information link quality, which we got from our spectrum sensor. Information from the other teams, which we use to build a interference map, and what was our achieved throughput per pocket. Our peer information, who they were we tried to identify them and how they were doing for each of their flows. And this also produces a huge amount of information. Next slide. Perfect.

One of the first things, one more. One of the first things we realized is that the decision engine couldn't be solved by just some BlackBox solution. Just the state space and action space are just too large to ever train. So we apply the typical engineering approach of decomposing the problem into smaller pieces. Our pieces were basically channel selection, which channels are we going to use in missing control, which flows are we going to support? And then packet schedule assignment? How are we going to put those individual flows into an achievable schedule based on our constraints on the number of simultaneous transmit and receive streams at each radio? Next slide, please.

And so, we did develop a couple of different approaches to doing some of these things. So in terms of channel selection, we had basically a heuristic approach designed by me. We had a machine learning approach that one of our PhD students worked on. And we—one of the dots, that's a dot that is missing here. So, I can't show you the performance. I won't say too much about this. But basically, we found that the ML system was pretty competitive with the expert system, but not quite as good in general. And we just couldn't count on, you know, the expert system overall had the better performance. And we were more confident in it, because we understood what it was doing as it went into different new scenarios. So next slide, please.

So basically, the SC2 demonstrated the—that distributed spectrum sharing among a very heterogeneous set of intelligent agents can be achieved, with spectrum access occurring in timescales of seconds instead of hours. The team's demonstrated an acceptable level of performance in the presence of all these diverse challenges I mentioned, so mobility, traffic surges, incumbents jammers.

And one of the important things that we definitely observed and we heard a lot of feedback about is that, you know, we spent a lot of time optimizing our particular behavior to the rules of

the championship event in the end. And that made our agents much more competitive than cooperative based on the scoring rules that were announced. So it's always important that reward structure will drive the spectrum sharing behaviors. Next slide, please. And go ahead, there we go.

So there were a lot of problems that limit the ability of teams to apply machine learning, or this championship this—competition. So I don't think many teams even tried it. We tried some parts of our system. As I mentioned, the overall state and action spaces are really huge compared to many problems. And that's especially true in comparison to the amount of training data that you can collect. And I'll say a little bit more about that later. But we also found as we went to the last few weeks of the leading up to the championship, when we had to submit our radio algorithms to DARPA. That teams were changing things very rapidly, their strategies, but also their radio algorithms, even the fundamental radio algorithms. And the ML training just couldn't keep up with that. So, we felt much more confident in the expert system approach based on that. Next slide, please.

So, applying dynamic spectrum sharing techniques like those in SC2 to real systems will require the development of what we call a technical ecosystem for DSS. In particular, some of the important aspects of the SC2 that may need to be considered are the design of standard frameworks to drive the desired behaviors. And the development of an information sharing protocol. One of the nice things in SC2 was the development of the CIL which allowed us to exchange some information with other teams. And there's a lot of work still to do on how to make these algorithms more efficient, how to preserve privacy, how to achieve security, how to have compliance and enforce that, though, there's many things still to be done here. Next slide, please.

So, I think a lot of people are interested in how ML and AI can be applied to this. And we do see a lot of potential for those in dynamic spectrum sharing. But new approaches to training agents for that will need to be developed and ML agents will need to be developed that we can be confident or robust to new situations because always we can't provide the training algorithms with every possible situation that may need to operate in. And we also see off potential for machine learning approaches to compliance to privacy, and also to adapt the overall incentive structure over time to enhance the network performance. Next slide.

So, I'd be remiss if I didn't acknowledge all of my teammates, especially Tan Wong, who was a team leader who did most of our physical later—layer, our Mac, and fencing, and spectrum mapping portion of our radio. David Greene who did our FPGA some network layer, a lot of ID and tools. Tyler Ward, another PhD student who did some physical layer work on acquisition link layer, and most of our control plane. Marco Menendez, an undergraduate who did a lot of work on our workflow and some CIL development work. Next slide. And then Caleb Bowyer who did machine learning. Shiming Deng, who did visualization. Quan Pham who did channel emulation tool we were developing, and Josh Agarth also worked on CIL. And especially DARPA, the SC2 team for running the competition and developing the Colosseum, which we're still using now. And the DARPA SCII prize and an NSF year grant that helps support our team's efforts. So, thank

you, for having me here. I see there's some questions. So, I guess I'll just answer the questions if that's OK.

### 4.2.1 Technical Presentation: Q&A

GREMBAN: Right ahead. Thank you.

SHEA: All right. So the first question was hidden terminal prompt an issue and interference management. Well, hidden terminal is a little bit hard to exactly specify in this but yes, absolutely. So we would collect information from all of the other teams about where they would say their radios were. Not all teams were good about reporting that if we knew that, then we could kind of prevent hidden terminal because we knew where their interference would be causing interference to our receivers. But if they weren't reporting it, then yes, we would be transmitting based on what we could sense from one location. But we didn't fuse all of the sensing information from all of the locations into one place, because just the overhead of exchanging that much information.

And I missed—another question was, is jamming avoided by switching to a band channel time, which is not jam? And yes, we could. There was always unjam space. But that's not necessarily what you wanted to do for all of your flows, because those were the areas that all the teams wanted to use, but we preferred not to use that all the time. We sometimes we put our easier to transmit flows within the jams region, because we could still get them through with robust physical layer and put some more, the high data rate flows outside of the jam region.

GREMBAN: OK. Thank you, John. We're out of time here and need to move on to the panel. But thank you very much for a great presentation.

SHEA: All right. Thank you.

## 4.3 Panel 4: 5G Operations – Implementing Resilient Zero Trust Networks

GREMBAN: And people who had questions for John, remember, he will be in a breakout room at the end of the panels. So now let me shift over to our first panel. Our next panel is a great collection of experts from different industries and different backgrounds. And he's going to dive into the complex issues operating with resiliency. Our panel moderator is Dr. Paul Zablocky. I first met Paul when he was the director of the army communications research—I'm sorry, Communications Electronics Research Development Engineering Center. That's a mouthful, so we all call it CERDEC, and he was the Director of the Intelligence and Information Warfare Directorate. He moved from there the Office of Naval Research and is now a program manager in the strategic Technologies Office of the Defense Advanced Research Projects Agency or DARPA. At DARPA, his programs focus on enabling joint operations and robust communications among other areas. Now, I'll turn this over to our moderator for the first panel of the day, Dr. Zablocky who will introduce the other panelists.

### 4.3.1 Paul Zablocky: Panel Introduction

ZABLOCKY: Thanks, Keith. I appreciate that. So good morning and welcome to panel 4. My name as Keith said is Paul Zablocky. I'm a DARPA program manager in the strategic technologies office. My research interests range from robust communications and tactical environments to electronic warfare. And I've worked all of those areas. On behalf of the panel 4 members and myself, I'd like to thank that National Institute of Standards and Technology that National Telecommunications and Information Administration and the University of Colorado for hosting this event under such challenging circumstances.

Panel 4 as Keith mentioned, examines both implementing and maintaining resiliency and zero trust networks. So, I've worked in this area of electronic warfare for a long time, but decided I really ought to look up what resiliency means. And so, according to Wikipedia resiliency is the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operations. That range from simple misconfigurations to large scale natural disasters and targeted attacks like I would cause. We've assembled a panel of four experts from a diverse set of industries and academia to help explain how they address network resiliency in their respective areas. You'll find full bios on each of the panelists on the ISART 2020 website. But I will provide brief introductions to each of them.

So, I'll go through the four—the bios of the four participants or panel members. We have Tim Godfrey. He's a technical executive from the Electric Power Research Institute. And he'll address some of the challenges that utilities face as they enhance their telecommunications infrastructure to enable grid modernization. Next, we have Milo Medin. He's vice president of wireless services at Google, and will help us understand resiliency challenges from an internet related services and product perspective. We have Dr. Wayne Phoel and he's currently a visiting research engineer at the University of Maryland Institute for Systems Research, and the owner of a small eponymous research and development company. Now, you'll find that in his bio, and I actually had to look up what eponymous means, and it is in fact, a company named after himself. He'll provide us insight into some of the unique defense related challenges that we face. Our final panelist is Dr. Sanyogita Shamsunder and Sanyogita is going to talk to us. She's vice president of technology development and 5G Labs at Verizon. That she'll help us understand zero trust network resiliency from a major service provider perspective. And so, with that, I'm going to turn it over to Tim for our first discussion today. And we'll go through the four panelists' overviews of the topic and then we'll hit questions afterwards. So Tim, take it away.

### 4.3.2 Tim Godfrey

GODFREY: Thank you, Paul. Good morning, everyone. Next slide, please. I'm going to give a brief overview of four projects and research areas that we have that are related to resiliency, and network operation and also have to do with spectrum. Next slide, please.

EPRI is a collaborative research organization, a nonprofit that works with multiple facilities dealing with common problems that are faced globally. Next slide, please. One of the big areas

that are driving our work in telecommunications is the call the transition to integrated grid, which is based on the need to modernize the grid to support renewables and widespread adoption of distributed energy resources, which have significant impacts on the power flow and the operation and management of the grid. Next slide, please.

One way that the need for this telecommunication in the field is playing out in the industry globally is the adoption of LTE and the movement toward 5G. And in particular, there's a strong momentum toward the adoption of private LTE, which is not highly exclusive of commercial but that is being used as the core network for operational purposes. That is due to reliability, availability, concerns with commercial networks, utilities able to build and operate the network to their own standards.

Cyber security is a big issue to be able to control all aspects of the network security and also have full visibility in the operation of the network through your own knock. Cost is another interesting factor. When you first think about it, you think that building your own private network could be prohibitively expensive. But for utilities, especially investor owned utilities, capital ventures are preferred over ongoing operational expenses due to the way that they're handled their finances.

Finally, a big issue for many utilities is the life cycle. Personal networks are often out of synchronous, out of sync with the expected field asset lifetime. And they've been forced to retire equipment in the field early because the generation that they were built to was no longer being supported by commercial networks, but the assets were still fully functional. Next slide, please.

Of course the cost of the spectrum is a large issue. And that's something that we think a lot about is how to get spectrum or how to make different spectrum choices, including shared spectrum work for a private LTE network. The cost of the required infrastructure for full coverage is also challenging, the networks for private utility tend to be more coverage limited rather than capacity limited, which is the problem for our commercial networks.

And finally, operating, building and deploying a network is a new skill set for many utilities. What does 5G fit in? This, it's certainly an inevitable endpoint as the whole industry will be moving toward 5G over time. It doesn't immediately solve the spectrum issues for private networks. In fact, it makes it a little more complicated. Currently, the new radio is limited to 5 by 5 is the smallest channel size, most of the utility networks that are operating in the United States are using 3 by 3. So that's a little bit of a challenge. New radio light is moving in the right direction toward giving a little more flexibility. Another bit of good news for the migration to 5G is the advent of dynamic spectrum sharing which allows the spectrum allocation to transitionally move from LTE to 5G incorporating both. Next slide.

One other area that we're starting to investigate is how to find the appropriate spectrum. I've mapped out the spectrum options on two axes from left to right is the frequency band which is very important because the coverage is desirable. From the bottom to the top, it's a, what I call the difference between prime or non-prime spectrum where at the top of the commercial spectrum, it's widely used by operators is available in some areas, less populated areas, but it

tends to be expensive. Bottom, the narrow and cover shared spectrum that are less attractive to commercial, although some commercial adoption is taking place, especially in the CBRS. Next slide, please.

Within those bands, we can look more closely at those that are shared. These three areas demonstrate the three ways that the spectrum can be shared. And the unlicensed bands, it's shared, very granular basis, almost packet by packet. CBRS is controlled by something like SAS, which is enrolled maybe on a day ahead or shorter based on some circumstances. And then we're starting to look at the opportunity to share federal spectrum in the 406-MHz band, which has the potential for harmonization with that 87, 88 in Europe, which would be on more of a long-term sharing basis with incumbents. That's something that we're investigating with the DOE and I know national labs. Next slide please.

Finally, we're starting up a new project on LTE and 5G security, which is more about the underlying standards, and validating, replicating, and mitigating some of the exploits and issues that have been published in the research community. We're just getting started on this and hope to have it underway next year. Next slide please.

Another area that has come up this year has been the changes to the use of the 6 GHz band. This spectrum has been exclusively used for licensed operation over many years. This year the FCC opened it up to unlicensed devices. Next slide. The net effect is the band has become a effectively shared. And our testing that we've conducted as demonstrated that the automatic frequency coordination system is going to be responsible for preventing interference with these fixed services. And there will need to be careful attention given to the existing equipment including side labs. Next slide, please.

Finally, we have a black sky communications project that we did last year that looks at communications in the case of our restoration, or a widespread outage. Next slide. This project investigated non terrestrial systems, including satellite and HF radio over a wide area. I don't know if the slides you're keeping up there stuck on my screen, but I'll go with it. I'm not speaking to the final slide on the resilient communications micro grid communication, which is fourth area that we're looking at, which is taking advantage of peer to peer communications on LTE such as ProSe and PC5 sidelink, do allow communications supporting a micro grid, which provides power locally. In case of a broader outage, you'll be able to also transition to a localized autonomous area.

So, hopefully, these ideas will stimulate your questions and thoughts, so we can have more of a discussion in the breakout room for questions. That's all. Thank you.

### 4.3.3 Milo Medin

ZABLOCKY: Hey, thanks very much, Tim. I think next Milo Medin. If you're ready to go, take it away, Milo. Are you there, Milo? All right. We appear to have lost Milo. Maybe we will move on to …

MEDIN: Do you hear me now?

ZABLOCKY: Oh, yup, we can hear you now. Great. Excellent.

MEDIN: The app keeps switching audio devices on me. First off, thank you for inviting me. And since I serve on the Defense Innovation Board, I wanted to say that up front, these are my personal comments, and do not necessarily represent the views of the defense board, its chair or the Department of Defense. I just have to give that boilerplate away.

Google was one of the first firms to adopt zero trust architecture for internal systems. This was the result of looking at how PLA hackers penetrated our systems back in 2009. And those lessons learned drove a change in our architecture that resulted in a system called BeyondCorp, which is sort of our implementation to the zero trust internal network. Key to this model was not ascribing any rights to access information by being on a particular network segment.

We assume the entire internal network is open and unprotected. That isn't actually true. Of course, we use a one-to-one x authentication on switch ports and enterprise WiFi network segmentation. But the key is to not use any protocols or access control methods that grant rights or to devices by what network segment they rely on—they reside on. That means we rely on internet protocols that require cryptographic authentication for access to information. These are the protocols used for Internet services, not things like NetBIOS or Windows file sharing. Devices that wanting to access a given network resource must be certified and have been loaded with cryptographic certificates that validate it's a device that is authorized. That could be a desktop computer, or laptop, phone, tablet. Users that want to access information must use multifactor authentication to validate their identity. And then access is granted to information based on the roles and the identity of the user and device.

For example, someone in our finance world would not have access to the source code that software engineer would. And a data center hardware engineer will not have access to a personal data, when people change roles, their access rights change without explicit updates being made to code repositories, et cetera.

That's not to say that network location is invaluable. We treat it as a signal, not a key. For example, if my laptop shows up on a network segment in our DC office, but my ID badge was just red accessing a door in my building in Mountain View, that will trigger a security alert and could remove my access to information until that discrepancy is resolved. Patterns of data flows are used to train machine learning models to flag unusual activity and help automate threat detection and defense. Because of this model, it allows as to be flexible about what network resources are used. And we can use a mixture of private and public network access.

Zero trust was critical to enable us to move more than 150,000 people to work from home mode in about two weeks. Because we didn't trust the network in our offices, we could actually move the same equipment to operate from people's homes on public networks without wholesale changes to software and systems. When you use G Suite and other Google products, you're

using the same technology that we ourselves use to protect information across untrusted networks.

When I think about how this could apply to DOD in federal missions, there are several implications. One of the major issues I see in the military that holds back innovation and integration of new types of networks, particularly wireless ones, is this mistaken focus on communication, security, and not information security. Putting a pair of KG on a point to point circuit may protect information flowing or that link from interception, but it does nothing to protect that information from an insider attack on the—at the local networks on each side of the KG.

It also means that newer, faster, and more compact encryptors have to be built to deal with each different type of network needing to be integrated. That's a real issue, especially when it comes to highly integrated devices like mobile handsets. Instead of a zero trust model is use much lighter weight encryption can be used on the communication links, and the data is protected as it flows over the complete network path. This allows the use of commercial networks as well as streamlining integration of new technologies, and dynamic reconfiguration of networks that will be critical in wartime.

It also allows the mixing of flows of data with different security levels and different access rights on common network infrastructure. Depending on the encryption for segmentation and protection, not hard separation of flows, they're increasingly devoid of meaning on higher performance, wireless and optical network infrastructure. That end to end encryption, we're not just the server is authenticated to the client, but the client is authenticated to the server. And that identity and role are used to grant access on a fine-grained basis is the key to modern security that scales and scales to literally billions of users, and to securely accessing resources on cloud infrastructure. Just as DOD decided long ago not to build its separate computers, operating systems and programming language, but follow the commercial sector in IT systems. It means we'll also need to adopt it—adopt zero trust architecture because that's where the commercial sector is going, particularly in a COVID infected cloud native world.

One thing I want to flag here, this notion of relying on end to end encryption and management of identity at the endpoints has fundamental problems for organizational models where some firewall is meant to inspect traffic in the middle of that encrypted communications. IT models where security teams insert themselves between clients and services are very much challenged by this model. Because to do so it means creating holes in the encryption security to do man in the middle attacks on those data flows. Instead, imagine device and application security of both ends. That used to be the model. But industry is rapidly moving away from that because it's not the way the internet and cloud native systems function anymore.

One other point that we—too, is that we believe encryption needs to be adapted and upgraded rapidly. Not just to deal with vulnerabilities that are discovered in algorithms, but also new kinds of attacks from quantum and other kinds of specialized computing systems. After the Snowden disclosures in 2013, Google moved to a zero trust model in our core data center networks in the span of only a few months. Today, our systems do not trust the very data center switching fabric

that interconnects our processors inside a rack. Not only is traffic between data centers encrypted, but traffic between compute nodes in the same rack is encrypted as well. That kind of adaptation is not possible with hardware link encryption being retrofitted on a wide area network, but will be needed to stay secure in the face of new kinds of attacks. As VOD and the US government moved to more commercial models for computing and networking, policies and maybe even organizational models are going to have to adapt, if they don't want to let be left behind in the slower and less secure infrastructure. As my pilot friends in the Air Force say, speed is life. That's true in IT as well. Being static and adapting and not adapting quickly doesn't make you more secure. It makes you a target. Thank you.

### 4.3.4 Wayne Phoel

ZABLOCKY: Thanks, Milo. That was great. Wayne, I think you're up next.

PHOEL: All right, great. Thanks, Paul. I'm sorry for throwing that SAT word at you in the bio, but you know, nobody learns anything from my talk today, at least hopefully, they've learned what eponymous means.

So I want to thank also the ISART organizers. I tuned into a bunch of the panels earlier this week, and it actually caused me to rethink what I wanted to talk about and how I wanted to talk about things today. So thanks, guys for putting together a really interesting and diverse set of speakers. And the thought-provoking program to.

I wanted to get such a little bit more on my background. So currently, I'm a visiting researcher at the University of Maryland. Prior to that, most of my work was defense R&D at MIT Lincoln Laboratory and a few years at DARPA as a program manager at what—as well. So I'm kind of spanning that face of seeing what's going on in academia. With a background from what defense needs are. I also want to acknowledge a new university affiliated Research Center at the University of Maryland called the Applied Research Laboratory for Intelligence and Security or ARLIS. A large amount of the work on 5G and communications networks, that's done at the University of Maryland comes through ARLIS. I just want to acknowledge them.

So, if you go to the next slide, but I thought I would do so my title slide talks about zero trust, resilience and 5G's. So, I wanted to talk a little bit about how I think about that. And when we talk about zero trust, what do we—or trust? What do we mean? And to whom does that matter? Milo did a great job of describing what zero trust is, so I'm not going to go into that. But when I think about how we're thinking about applying in a bunch of different ways. I can't believe there's two views that we can think of. One is how I think it's been talked about most over the course of this conference, which is from if I'm a network operator, and putting together a network and operating that, what is it that I should trust, or shouldn't I trust? So, there's the components that go into my network. The employees that are configuring and then managing that network, as well as the users that I allow onto the network. And these are all the entities that I have to worry about? Who could potentially do so? What could do something wrong to my network operations? From a user, from someone like the US government who is operating

over, working over somebody else's network, or the Defense Department, or, you know, Tim, reminded me earlier today. If I'm a utility, I also can't trust or don't know where I can trust all those components. But I also don't know necessarily, actually how much I should be able to trust the network operators that are running that network, so, setting it just different perspective for people to think about.

If you go to slide 3, I want to talk about a little bit about access control, and the different functions that go and Milo talked a lot about these things in the lower left-hand corner that are some of the topics you would hear about with zero trust. Making sure that you really know who somebody is really limiting, breaking down the pieces of your network into smaller chunks. So you have to contain any kind of bad activity. And then it's really important role-based access, which also gives as Tim pointed out, much more dynamic control as my role changes, it's a lot easier to contain a change, I access. But I also don't think about this concept of trust as being a really a binary thing that either you're trusted or you're not trusted.

But I think you can think of it as having much finer grain scale of trustability. And in order to do that, I think we can think about behavioral monitoring. So, the first program that I started at DARPA was called wireless network defense. And it was really focused on ad hoc networks. But it was looking at attacks against the control plane of those ad hoc networks where there is nodes are already approved parts of the network. But they could be doing bad things to the network, whether be intentional or unintentional. We want to be able to understand from how a node behave even though it's checked the boxes as to whether it's supposed to be there. Should I be allowing it to be part of my control system? So we broke down that one of the approaches we took was to break down the protocols into basic components, and then also assign nodes, soft metric of how much we trusted those based on how we saw them behaving over time in the network. And I think there's what's developed in the 5G architecture has some similarities to that model we were looking at. So then maybe some things we could learn from this trust network overlay that we looked at in this wireless network defense program.

Now we go to the last slide, talk about resilience. And that DARPA program I had two terms I talked about. One was robustness. And the other was resilience. And I defined robustness is really the ability to take a hit and keep operating. And the resilience was the ability once I've taken that hit to reconstitute my network and get back close to my original performance. And in order to do that second part, you need to understand when you've been hit, where it's happened, and characterize what the attacker or the event was. And for that, you need some internal awareness of what's going on in your network. So, I think we could use this concept of multi-level trust metric, eight in that adaptive control of our networks. And I'm really intrigued as we look at what's coming in 5G, and the ability to customize virtual network functions. I'm really curious to know if there's some way to take those and enable those to help with monitoring, evaluating trust, and then reconstituting the network. So there's my thoughts. I hope they spur some thoughts for you guys, and I look forward to the rest of the conversation in the panel. Thank you very much.

### 4.3.5 Sanyogita Shamsunder

ZABLOCKY: Thanks, Wayne. That was terrific. Sanyogita, I think you're up next.

SHAMSUNDER: Thanks, Paul. Can you hear me? OK. First of all, thank you for inviting me. I'm honored to be here with the panel and happy to talk about what 5G and zero trust architecture mean to a service provider like Verizon. So first and foremost, I'm—I've been the president for a few years now. I spent a lot of time on the network side and I'm more focused now. I've led some of the early 5G work in terms of mobilizing the industry and working with the industry as well as that CC and CSMAC and others in terms of the spectrum to the industry. So this topic is near and dear to me, and I'm happy to talk about, you know, some of the other aspects of 5G in terms of security, and the flexibility of 5G provides, and the opportunities, as well as look at where there can be differentiation.

So the introduction of 5G into the communication ecosystem is probably the first tangible example of the fourth industrial revolution, right. We've had several new features of 5G that enable many more things, that can, they were previously possible, essentially bringing the cloud into the hands of the device, so the capabilities of the cloud in the device. What that means that our generation will have access to more data and more machine intelligence and never before and be able to process that and in near real time, so that we can make decisions. Understanding 5G's capabilities is the first step in leveraging the full capabilities of this way. We know—also know that the 5G architecture and standard brings a lot of flexibility in design and deployment of the network in terms of virtualization and service-based architecture. Which allows us to be agile, and like my previous panelists have talked about it quite a bit in terms of, you know, if you're not fast enough. You know, you're going to be left behind. So I think those are some good things.

However, the design and deployment of the network with a 5G network are important and play a big role and how you can—you offer continued security. And so, I believe that not all 5G networks are equal in that sense. And that's also especially important because PGPT as the standards offers a lot of optional capabilities that not everybody may choose to deploy, and that might impact how secure the network may be.

So Verizon has structured our approach for securing our 5G network around four pillars, right. So, one is the global security capabilities. The first pillar of our approach is securing our 5G network is leveraging the existing global security capabilities that we have in place that also supports all our communications today, which is 4G as well as provide networks, and so on. So, the first one is enterprise protection such as physical security of facilities, penetration testing of key systems, and enterprise vulnerability management program. Sometimes it can be a lot of process, but it also ensures that we are able to manage and secure our networks. We have global security operation centers, supply chain security practices, and security governance programs, and so on and so forth. We have partnerships in place to continuously exchange ideas within this industry groups. I don't have to talk about that in a lot of detail, and as well as global backbone network that provides visibility into worldwide threat active behavior that Verizon uses to inform the defense of its network.

The second pillar is the features in the 5G standard. Like I said before, there are a lot of new security features that are part of PGPT's 5G standards Verizon. We will implement numerous optional features to enhance security and that has influenced our implementation decisions. For example, device security features that include for protecting information that could be used to identify and track the subscriber prevent attack—attacks from modifying user traffic, as well as ensuring subscribers only to connect to trusted cell sites. Radio access network security features which provides secure communications on all run interfaces and radio access network, as well as include extra protections that place that are vulnerable to physical attacks. Or the third is the core network security features which include specialized network functions, and enhance protection for service-based architecture that the network functions will use to communicate.

The third pillar is our own unique capabilities. Our design decisions, building upon the robust 4G LTE security principles, as well as tailoring redundancy models and security protection for each network function-based functionality. Implementation of robust device certification processes. Again, it may seem cumbersome, but it really helps us ensure that we are net, you know, hardening every network interface and every device to network interface, securely provisioning and booting network functions and so on. The third is a deployment capabilities involving core services such as PKI's access, management, analytics, and one of that is face scanning.

Finally, the fourth pillar is enabling customer facing services. So, we embrace the concept of zero trust architecture early and we provide solutions such as software defined perimeter today that's unique to the network.

And it will continue to offer that in addition to the security notions that 5G provides, and the capabilities that 5G provides. Such as network slicing, and edge computing. You can think about those as limiting the levels of isolation, slicing, especially if you think about it as providing a level of isolation and resources guarantees to a certain part of customer, so you can separate different types of users into different places. Edge computing, not only will it host latency sensitive applications, but you can also host network-based security services. Maybe even STP in the—in that framework to continue to strengthen the endpoints that may not be secured.

So, 5G can seamlessly support an application. In addition, so having said that, we can put, you know, seamlessly support any other application that uses zero trust architecture, to communicate and to act. And of course, not to forget, as we look at new capabilities, that technology that evolves, we continue to look for ways. We can continue to strengthen the network such as, you know, providing—using the capabilities of quantum. Quantum key disk encryption and so on to continue to strengthen the network as these technologies evolve and make these added—provide added security to the network. Next slide please.

So, some of the key examples for 5G security, that we have implemented I've given you a high level before going to a little bit more detail here. So, devices on Verizon's network will automatically use an encrypted identifier called Subscription Concealed Identifier when identifying the access to the network. So this identifier is generated using cryptographically strong encryption keys that come pre-configured in a tamper resistant hardware element on the

device. And it also includes metadata that could otherwise be used to track user and compromise their privacy.

Secondly, 5G networks break down large multi-purpose network functions from 4G LTE into smaller single purpose network functions that are deployed in a distributed manner. So this is the new architecture that we're talking about. So, Verizon's 5G will leverage disaggregation to deploy and function in a way that eliminates single points of failure. So, you can think about it as a—as an offering the flexibility that you've taken this flexibility and to ensure that we have—we eliminated the single points of failure and minimize the blast radius of a network function major security issue. In other words of malfunctioning network function will impact a small number of customers and a similar failure wherein a 4G LTE network.

The distributed 5G Ram, right. Again, we'll have network functions at the edge of the network, potentially at an unmanned locations or sites with minimal physical security. Our network will ensure that this distributed network functions cannot access reprographic keys protecting subscriber traffic, thereby protecting the network from an attacker physically compromising the site. And the next is this service-based architecture in the core will cryptographically authenticate the identities of any network functions trying to communicate with each other. So while there are several more interfaces available today, they are going to be cryptic—they are cryptographically connected to ensure that you can get access to these interfaces that easily. So, encrypt all network function communications, as well as cryptographically authorized communications between network functions using modern security standard.

The 5G devices go through a rigorous certification process. I mentioned that before. And including penetration testing by specialized team that has deep understanding of how the network works. So, we have several security in-house security personnel in place. And any application service that we test and launch has to go through that security, posture testing and threat modeling and risk modeling, and so on. The 5G network functions that I mentioned earlier, and the containerized network functions that run—they run on the cloud platform. So, this is a little bit of a departure from the 4G network that offers the flexibility. But these four functions don't just run on any cloud, they were—they run on Verizon internal cloud, and we are hardening the Verizon internal cloud to ensure that we have all the monitoring to physical security and so on, and firewalling and so on and so forth. And they also leverage common PKI for identity and many other features that ensure security of the Verizon internal cloud. So, since 5G and evolution of 4G LTE, these four pillars and their associated features built upon 5G security but also improve upon it in the key areas, that the flexibility that 5G offers. And the 5G implementation that we have goes further by in—by the additional capabilities that we have in place already, right. Combine these things, we make sure that we are more secure, and ultimately enable the fourth industrial revolution. So if you want more information on some of these concepts, you can download the white paper that I've put provided a link to, as well as, our annual mobile security index that does a whole lot of testing on various networks today and provides data on how things are—what are the root causes of security breaches? That's all I have. Thank you.

### 4.3.6 Panel 4: Q&A

ZABLOCKY: So thanks, Sanyogita. That was terrific. So we have plenty of time for questions, and we're actually getting some questions. And so, I'm going to jump in and take a look at some of the questions and read them out to the panel. First question we have, which I think I'm going to generalize, but we'll start with Milo answering it. Was there any trade-off with overhead based on Google zero trust? And Milo if you can take that, and then I'd like to ask the other panel members too, to take a shot at that from their perspective?

MEDIN: Sure. So, I'll answer that in two ways. Originally, when we turn it on, on our data center network, right. I think the—it was something on the order of 10 to 15% of CPU overhead, to do that level of encryption across everything, right. Not trusting the data center fabric, et cetera. That changed as new CPUs had more and more graphics support in their instruction sets. And so, that's been optimized significantly. And so, I think it's probably under 5% now, but obviously varies on particular platform and function. I would say also, if you think about zero trust from an encryption perspective on the—on sort of user traffic going into end, right. SSL and the rest had a fair amount of overhead, QUIC, and HTTP3 are actually reducing that kind of overhead for significantly. And so, I think that you're going to find that particularly on slower networks, that the amount of overhead to do zero trust is actually quite modest.

ZABLOCKY: Thanks, Milo. Tim, I would think that overheads a big issue for utilities. Have you done analysis on the overhead implications of zero trust?

GODFREY: We have not. Definitely, it's true that overhead is a big issue. I thought I saw a question on 3 by 3 and 5 by 5. And as I was pointing out that many of the private utility networks are based on relatively small spectrum allocations, which means there is a limit on throughput. So today, most utilities are implementing traditional IPsec tunnels and other types of encryption. But this whole area of zero trust is something you're interested in evaluating and getting adopted. So, I think Milo was absolutely right. There's opportunities for zero trust to reduce overhead and make more efficient use of the limited bandwidth that we have on these networks.

ZABLOCKY: Thanks, Tim. Sanyogita, I'm sure the overhead is a critical issue for Verizon, if you'd like to get your thoughts on that.

SHAMSUNDER: Yeah. I think I mean, to add to what somebody said before, I think Milo said. I think we—the cloud architecture in the beginnings, you know, did receive some initial criticism, but as you can see, it's probably the most robust in terms of security features. And really, there are a lot of the risk comes from connecting to the cloud from unsecured networks. So, to talk about, I mean, to—there are more details in that. But for example, devices today connect from unsecured WiFi, two to—three to four times a day. And typically, those are, you know, networks that you connect from, like in a restaurant or a, you know, retail store, and so on and so forth. So, there is that—of course, I'm going to talk about—I mean, I guess I'm thinking about the overhead in a way that it is, you can—it can be even if the overhead is there, even if it is large. I think it's—you have to kind of work with that, because you can't talk about—you can't—I guess

minimize the importance of security for the customer. So, that's why we believe that nothing, you know, no network is—especially from a customer viewpoint, and a software defined perimeter is an important aspect of security. And we offer that to all networks today.

ZABLOCKY: Thank you, Sanyogita. Wayne, any thoughts on …

PHOEL: Yeah. I wonder—I think, you know, to echo what Sanyogita just pointed out, right. Is that—it's, we shouldn't be thinking about it, as you know, the communication service, and then security as being separate to it, right. It's all part of one big optimization function. And so, you need to—it's harder to do, but you got to figure out how to balance that overhead with what the consequences are of something bad happening if you're not implementing some sort of system like this. And so, I think that's one of the other ways you just need to really think about it. It's just, you know, what's the—what is the right metric that you're using to judge network performance? And it's not just throughput?

ZABLOCKY: Thanks, Wayne. So we'll move on to the next question. And, Tim, you kind of alluded to it, but can you please elaborate more on 5 by 5 versus 3 by 3 issue?

GODFREY: Sure, thanks. The issue is that, as I tried to point out that most utilities are implementing private LTE networks, but we'll have to use smaller spectrum allocations. And most of those that are being currently deployed or are being considered are built on 3 by 3 spectrum. And that is, of course, much smaller than commercial networks that are using 10 by 10 and 20 by 20, or even much larger than that in with 5G and frequency range 2. So the 5 by 5 issue is that with the current specifications for the new radio, the minimum channel size is 5 by 5. So those utilities that were operating in their 3 by 3 allocation, they don't really have room to grow, though without having to go back and find more spectrum which would be economically unfeasible. There's a limited path for adoption to 5G immediately. But the good news is that the NR-Light will bring back those smaller allocations, or the applications that are less bandwidth intensive, because new radio is really this first rollout was for enhanced mobile broadband, which is high bandwidth. So I'm sure the thinking was, nobody would be really seriously offering eMBB in 1.43 MHz of spectrum. Make sense? I hope I answer the question there.

ZABLOCKY: Thanks Tim. We have a few more questions. And this is—this would be another one for the entire group. To implement zero trust in 5G network, what changes in 3GPP specifications are needed, i.e. certification management, relocation, g-nodeB authentication. And maybe I'll ask Wayne to start that one out.

PHOEL: Something's wrong with my mic here Paul. I was hoping you weren't going to call on me first. I say I'm not super person with the detailed 3GP specifications. But I think, you know, certainly adding some of the—one of the big things would be adding something about that role-based access control would be something that you would need to change. I suspect a lot of the other features you need are probably in there. It's just a matter of how you actually configure things. But I'm going to defer to the people who know a lot more about detailed IpSpecs for those who have answers.

ZABLOCKY: Thanks, Wayne. Sanyogita?

SHAMSUNDER: I don't know that changes are needed. I think there is a lot of flexibility. And, you know, 5G does support a cloud-based architecture. And like I said, there are several optional features that are available. So, I'm not 100% sure that maybe change is needed. I think I'll have to get back on that.

ZABLOCKY: Thank you. Milo, any thoughts? Comments?

MEDIN: Sure, absolutely. First off, no changes at all are going to be required. And the reason for that is that the whole point of zero rust networks is not to trust a network, 5G network, LTE network, Ethernet network. So the question about where is identity managed, right? You can't use a carrier, or any individual network element to manage enterprise identity. That just doesn't work. And so, all of the cryptographic work go—that goes on in your, you know, in 5G with regards to managing keys, et cetera. That's all not useful if somebody in a carrier store is going to swap out a SIM and enable the takeover of someone's identity on their mobile device, which has happened multiple times. I think that happened to Jack Dorsey on Twitter. That's how his twitter feed was compromised. So the whole point is you—cellular networks, enterprise networks, Ethernet, you don't trust any of that. The identities got to be managed at the IT system. And you can't outsource that. It's got to be owned by the enterprise. Who owns identity is absolutely vital. And I would also say, in general, right, we have to be thinking about cellular networks, 5G and the rest are only part of the enterprise network. If you're using features or identity for any one network component, as your key, how does that map into an Ethernet? How does it map into the land in your business? How does that work for your laptop that's plug or your desktop that's plugged in? So again, if we—it's just we want networks that are secure. We want them not to be able to be taken over for downtime, but you can't entrust your security to anyone except where the information is stored and managed. And that's not going to be a carrier. It's not going to be some provider. It's got to be the enterprise itself.

ZABLOCKY: Thanks very much, Milo. Tim, any thoughts on that?

GODFREY: I'd agree with Milo that standards are—don't need to really be changed. And just to build on that I think that the move towards zero trust architecture would also be concurrent with broader adoption of the open ran. We've heard some of the analysts earlier in the week talk about which will provide more options and flexibility for private and commercial deployments and hybrid models above. Thanks.

ZABLOCKY: Thanks very much, Tim. So we have another question. And this one is if the same Verizon Security and Policy practices also apply to Internet of things devices hosted on Verizon's network. Sanyo—Sanyogita, it's obviously a question for you.

SHAMSUNDER: They should.

ZABLOCKY: All right. Thank you. So, we have another question. First of all, the attendee is thanking us all for the great presentation. So thank all of the panelists for the great presentation.

Any ideas on using blockchain technology to enhance zero trust? Good question. Tim, any thoughts on blockchain?

GODFREY: That is an area that every cybersecurity team have looked into. We've done some white papers and thought leadership reports on it. We have not found a application or integration into telecom yet, not saying that that's not possible. It could be a—an enabler for some zero trust or other mechanisms that are still emerging.

ZABLOCKY: Thanks, Tim. Wayne?

PHOEL: Yeah. So I guess in general, I'm not a huge fan of blockchain. I don't feel like it's a solution looking for a problem. I—The one, I guess the one place where I've seen it or I feel that it probably is best usefulism, this concept of smart contracts. And it's being used for. I have seen blockchain being talked about when you go do much more like distributed software-defined networking approach where you don't have all the control in one place, and you wanted to kind of distribute that out to the network. So there may be something there. I haven't looked at in detail. I actually, don't know how that really meshes with what we're calling zero trust here. But there may be something there with when you're going to not purely centralized and you're trying to distribute things and control throughout the network, that might be a place for you to do something like that.

ZABLOCKY: Thanks, Wayne. Milo?

MEDIN: Sure. Blockchain is a distributed ledger. And so, if I tend not to use the term blockchain because I like more boring things and make it not appear to be magic. And so, any place of distributed ledger could be substituted by database, you know, that can work too. Blockchain has some advantages in terms of trying to decentralize administration? It's not clear that that is useful in all cases, particularly and the question is really about how does that help you manage identity? So, transaction logs and identity management seem to be different animals. You might use blockchain technology as part of a scheme to sort of distribute these credentials, et cetera. But I think there are better solutions in general.

ZABLOCKY: Thanks Milo. Sanyogita?

SHAMSUNDER: I don't have anything to add. I think I kind of echo Wayne and Milo's points there. The—It is being explored for smart contracts, right and so on. But it's more transactions than anything else. So, maybe there are points in different parts of a network that may be useful, but I'm not 100% sure. Across the board that there is—there's an opportunity there.

ZABLOCKY: Thank you. So I have a question for Wayne, your points on cybersecurity aware adaptive in it, the like—likely as many organic implementations. Question. How would you envision an industry standard to support this functionality given the nature of security by obscurity?

PHOEL: So, I guess I would work really hard to do away with security by obscurity because they're really bad policy. And I used to joke, when we were looking at tactical networks, the best thing we could do is just give our adversaries the specs to the networks because they're incomprehensible. And, you know, they have a much better job trying to reverse engineer things and trying to figure it out from the specs. So, but I actually think from what I've seen and in particularly the 3D paper that Sanyogita puts a link to in her slides, I think is a really great way. It does a nice thorough job of describing the security architecture of 5G. And it certainly removes, I think, a lot of this secure—obscurity there. And so, I think, you know, you just got to be clear about what these protocols are. And I think there's probably a pretty straightforward way to define standards for how different virtualized network functions, and communicate if they're going to try and have developed this network situational awareness inside the network.

ZABLOCKY: All right. Thanks, Wayne. So, you know, I do have a follow up to that, and something I've kind of been wondering about. So, we've put out all of these standards, that also makes it easier to figure out how to attack these networks as well. So, you know, while I understand what you're saying, with removing the obscurity in this, do we incur risk by doing that, do you think?

PHOEL: I mean, so there's a—there's like another Kirkoff's law or something like that with cybersecurity, that, you know, you want to make the really important parts of the security, something that you can change, right? Like a key. You don't want to have your jewels be something that's hard coded into your system. And so, I think a lot—and a lot particular things like Milo has been talking about with zero trust, is that you need to build the system, assuming that there's something bad in there. And somebody can get ahold of the specs, even if you're trying to keep it secret. So you probably do. I mean, you—if indeed, you could really keep all these secrets secret, then you are losing something by exposing them in standards. But given the least, the determined adversaries are going to be able to get ahold of your specs, even though you're trying to keep them secret. I don't think you lose quite as much.

ZABLOCKY: Thanks, Wayne. Let's move on to the next question. And I'm not sure. I guess we'll open this up to anybody who'd like to answer it. But can DSS enable CBRS to work without a centralized SAS system? If it can, how would the incentive and policy or what would the incentive policy look like? And I'll ask, does anybody want to tackle that one? Milo?

SHAMSUNDER: OK.

ZABLOCKY: Yeah, we're not hearing you, Milo.

MEDIN: How's that?

ZABLOCKY: That's much better.

MEDIN: I assume by DSS. The person is talking about sensing. The issue with SAS is you have to have an ESC network to sense the SPN-43 radars and other users. That ESC network is critical for understanding when a primary user has to, is active, and you have to move users around to not interfere with that radar. You could imagine a world where that's being done not in a centralized

way. But it's pretty difficult because I don't think you can get the equivalent performance from a user terminal sensing the radar, as you do from these ESCs that are out there. And more generally, there are certainly cases for satellite and other kinds of systems, where a user may not be able to sense the signal that they're going to interfere with. And so, there needs to be some form of intermediary. That could be done in a distributed way or a centralized way, but it's not going to be done by the end node at all.

ZABLOCKY: Thanks, Milo. I appreciate that. Next question. And again, I'll kind of leave it to the group for who'd like to tackle it? How many different types of policies are there for user equipment access? Any volunteers up, Tim?

GODFREY: No immediate thoughts on that. I don't know if I …

ZABLOCKY: OK.

GODFREY:—but …

MEDIN: Yeah, I could try and take a shot at it.

ZABLOCKY: All right. Cool.

MEDIN: So, if you think about what does that mean user access policy, it means sort of what device? What's—Who's the user identity and what their role is? And so, you don't want to think about this in a mode of thinking. Guest Access, everybody can access read only, or only a certain user group can actually write. What you want is to actually think about your information, not in terms of what your Active Directory login is, or what your OAuth credentials are? What you want to think about it is what—who in the org needs what rights? And if you think about that, and then you can see that it's really huge, right. There shouldn't—It's not about just a few policies, it's really thinking about who has act—who do you want to have access to that piece of information. And so, it's not about, again, a particular user group or domain admins or et cetera. It's really thinking about your enterprise. What's the structure of it? Who—what the workflow is like? This issue about thinking about role is very critical in getting real value out of zero trust networking. And that's the area where it's difficult for a lot of organizations to deal with who's just been thinking about Active Directory, and this user has access or this group has access. Role is much more sophisticated than that.

ZABLOCKY: Thanks, Milo. And we have another question for you that just came in. So you stated who owns identity is vital. And we need to focus on where the info is stored and managed. Could you speak more to that and how this works with edge computing?

MEDIN: Sure. So, if you think about a cloud centric world, you know, your—if your org is accessing data in the cloud, you're going to use AWS's, or Google's, or Microsoft's credentials, right, to getting access to that. Edge compute is simply a piece of a cloud instance that's forward deployed closer to the user. Its identity and access control, ideally, should be stopped off of whatever you're doing, whether that's local to the organization, and in and sort of

arbitrated by some cloud entity or your cloud native and all your identity and management is sitting in whatever cloud resources you are using to enumerate your users. What roles and what permissions they have? A good way to think about it is, who do you trust to control your badge access, right? So who's authorizing employees to be able to get into buildings, right? That's the kind of I—when you think about identity and access control, it's really got that physical analog. Like who's determining who gets in and out of your facilities, who gets in and out of your information? And so, wherever that information is stored, that's going to be where the identity management is going to have to be out. And that's why I say I think enterprises have to own that themselves. You can't—because who knows what role it is? Who knows what, you know, Tim's role is at Emory that says what information he has access to? You know, at Google, I can't get at our finance systems information. I'm not authorized. I'm not in the finance org. Who knows about what your role is? It's very hard to do that if it's some external party. That can be instantiated in a cloud framework, but the enterprise has to own.

ZABLOCKY: Thanks, Milo. Sanyogita, do you have any thoughts on that?

SHAMSUNDER: No. I'm good.

ZABLOCKY: OK. Thank you. So we have a really interesting question here that I think everybody should take us down to that. Where should the industry focus on when trying to isolate information and compute authorized activities? How can information leakage, e.g., through multi-tenancy in hardware and especially through psi channels be tackled? So if we want to just take that one at a time, maybe Tim?

GODFREY: Yeah. That's obviously a very broad and complex problem in terms of the in the utility world. We're dealing with the need for centralized information, and cloud-based systems as well as edge computing, and bringing all those things together, and ensuring that they can work with a comprehensive security. It's great application for zero trust type architecture, the other side channels. It's another whole area of research that we're looking into it in cybersecurity. So, good question. I think the whole scope of it is relevant for the industry to focus on.

ZABLOCKY: Well, thanks, Tim. Wayne, any thoughts on where industry should focus in this area?

PHOEL: Yeah. So, I guess I'm interpreting this, maybe a little narrowly. But talking about slices and interest slice security, right? And can I figure out, you know, what's going on inside one slice even if you know, I'm not inside that set of resources have been set aside for that slice those logical resources, but if I'm like riding on the same hardware. Or can I do something that can influences what goes on in a slice place, dealing resources or something like that? And the only idea I have for this is sort of that I do I was talking about earlier about running something on that hardware that's trying to figure out to understand this information leaking. And doing that kind of real time as you're running the network have like a monitor sitting there to understand. Can I figure out what's going on in the slicer? Or is am I gaining performance I want? Is somebody else doing something that's stealing resources away from a different slice in there? That's just where my mind goes in that particular problem.

ZABLOCKY: Thanks, Wayne. Milo?

MEDIN: Sure. I think this is one of the most vexing challenges that every cloud provider has to deal with. That is to say, think about what is Intel's latest vulnerability that's been seen, or some breach in trust zone and an AMD processor, and an ARM processor, et cetera. And that's not just for cloud, but it's also for mobile devices. If you just think about what information is present on the edge device. I think this is an area where organizations that—this is one of the reasons why I think people have really been moving to cloud compute, because you've got the sort of the best people in the field working on trying to isolate the compute stack from vulnerabilities in the hardware below it. And that's an area where Google has put enormous amounts of resources. And, you know, our team that finds holes, spectrum attacks, and others is focused on that. I think that's—it's one of these things that you have to be updating constantly thinking about how to segment information and how to use cryptography. I think if data is encrypted at rest, and encrypted in flight. Not just in flight, but also at rest. That can be helpful in dealing with these kinds of challenges as well. And certainly, if you're going to run your own compute, you need to be thinking about how data is encrypted at rest.

ZABLOCKY: Thanks, Milo. Sanyogita, any thoughts or things to add?

SHAMSUNDER: Yeah, yeah, that's a great question. And I wish there was a simple answer that we can say let's focus on this, right. I think my panelists have identified a few areas that are—that may be meaningful, but I think we can't rest. I think we have to look at all aspects. I mean, there's a constant evaluation and like I enumerated, we have multiple layers. And it's not just physical, right? Yes, you have a mobile edge compute perhaps and you have a cloud compute at the edge and so on. That comes with physical security as well as, you know, cybersecurity. I guess tools and technologies that will need to continuously have and continuously evaluate and it's the hardware and that this is software. So vulnerability in hardware, how do we address that with some of the cloud things that Milo just mentioned, you know. Redundancy and resiliency is important as well. I mean, resiliency comes in various forms, the need for resiliency. Even the weather is every year for us a problem that we need to address, right. So I think there are, we have to look at it as a multi-pronged solution with multi, you know, multiple approaches to tackle different things. So, I don't know that there is a magic bullet that we can focus on and have all the problems resolved.

ZABLOCKY: Thank you. Great answer. So I think we've—I don't see any new questions coming in. But I think we have time for one more, unless, Tim, you had something you want to add to?

GODFREY: Yeah. Just to finish up on that last question. One kind of a contrarian thought is that at least in critical industries, one approach toward mitigating the type of questions of information leakage, multi-tenancy, and such as does, or those extremely critical applications to avoid using those approaches, avoid virtualization, multi-tenancy and all those things. And certainly, that's not a long-term approach, but in some cases that the industry can take a slower adoption to avoid those unknown threats that may exist in those areas.

ZABLOCKY: Thanks, Tim. So, yeah. I do think we could squeeze in one more question here. And I guess this is one that we got it talked about before, but for your particular industries, what's the one—what's the most critical threat you say? And so, Tim, maybe we'll start with you, what's the biggest threat you see for your industry?

GODFREY: Well, yeah. The electrical industry has, certainly cybersecurity overall and preventing attacks and outages, caused by bad actors, individual or national has been a huge area. And this, you know, I'm in telecommunications. We work closely with cybersecurity, but we have a team of cybersecurity experts that are deeply involved with the industry and governments, and have various levels of security clearance. I can't get into what all is going on and the details. But I know there's a lot of activity, a lot of work, a lot of effort to ensure that the grid and its control systems are secure and resilient to those types of attacks.

ZABLOCKY: Thanks, Tim. Sanyogita, do you have any, you know, what's the biggest threat Verizon sees?

SHAMSUNDER: Oh, boy. [Laughs] I don't know. There are. I know that I was answered for that. I think it's may be—I mean, security is definitely an issue that we are, you know, constantly on the top of our mind, security for the customers and security for our people as well. And resiliency, I think is another—other thing. The weather is like I said a constant thing that comes and you might think it's a dropped call. Not important, but clearly when you're battling fires and thunderstorms and hurricanes and so on. So that that becomes an important call that for a first responder, for a service provider and so on. So, threat can mean different things and if you look at it from a different context, but if you look at it narrowly, that these are some things that, you know, we are constantly on top of our mind.

ZABLOCKY: Thank you, Sanyogita. Milo?

MEDIN: That's an interesting question. I was—my sort of first reaction would be to say, you know, nation state actors, because the same sort of adversaries that the US government has, or many are sort of the same that we have in terms of trying to penetrate into our systems and gain access to information for our users. And we take that very seriously. I—It—But I would say maybe the biggest threat is actually complexity management. That is to say, if you think about all of the different layers, all of the different systems, the multitude of access mechanisms, right? How do you keep all those things manage well? And that's really the heart of resiliency. I think, trying to actually think about identity management cryptography, in a place where you can have simplicity, and not have infinite number of choices there is going to be important, particularly as 5G's attack surface is so much bigger than what you see in LTE, and in wireless networks in general. How do we think about those things, and managing the complexity so that the configurations don't lead you into dangerous zones?

ZABLOCKY: Thanks, Milo. Yeah, good answer. Wayne, any last thoughts on this particular question before we move on to our individual meetings?

PHOEL: Yeah, I was going to go with the complexity thing until Milo took it. I was going to add to that it's not even just necessarily, you know, attacks, right? It's just, you know, the more complex these things are, the more corner cases there are that you just can't possibly explore. So, some system could get in some bad state, due to some sort of random event. And when it's so complex, you don't necessarily foresee that or know how to get out of it. But when you started with Milo prompted me to a different idea. And that's just privacy in general, right? I think a lot of these systems, there's going to be a lot more data out there, we're going to be having a lot more wireless systems on us. And it's just going to be an opportunity to create more of a footprint of where we've been, and you know, what our behaviors are, and how that might get actually aggregated and losing privacy without really knowing about it. I think is another thing that I'm concerned about looking at.

ZABLOCKY: Thanks, Wayne. I think if I'm not mistaken, and maybe Keith can jump in, but I think we're about out of time.

GREMBAN: Yep, you're—we're just—we're out of time, just barely the unscheduled. So it's time now to go to the breakout rooms for one-on-one interaction with the panelists and our technical speaker. So information on accessing the breakout rooms is in the ISART app, or you can use the links in the confirmation email you've received. So, don't forget to close out of this window and then go into the breakout room. Thank you.

SHAMSUNDER: Thank you.

ZABLOCKY Thanks very much, everybody.

GREMBAN: We'll you see there—at one thanks to the—following the panelists.

## 4.4 Keith Gremban: Introduction of Panel 5

GREMBAN: Hello, everyone. Welcome back to the afternoon session, our final session of ISART. Thank you everyone for attending. And I hope you enjoyed our first session today and in the interaction with the panelists. And hopefully, you took advantage of the break to grab a little lunch, maybe take a nap, do some networking to prepare yourself for this session. This afternoon, we will be bringing it all together. We have a panel of polymaths and I don't use the term lightly. I think you'll find this panel will expose you to some seriously out of the box thinking and suggest some radical new ideas to you. Our moderator for this panel is Dr. Pierre de Vries. I could go on for quite length on his qualifications. Let me just stop, but he's the co-director with Dale Hatfield of the Spectrum Policy Initiative at the Silicon Flatiron Center at the University of Colorado Boulder. I've had the pleasure of working with Pierre for the past several years and I will tell you, it's hard to keep up. He's passionate about spectrum issues, and just has a very, very broad point of view on things. So at that, I'll turn this over to our speaker Pierre, who will introduce the other distinguished panelists.

## 4.5 Panel 5: Wrap-up – Bringing it All Together

### 4.5.1 Pierre de Vries: Panel Introduction

DE VRIES: Great, thank you very much, Keith. And welcome back, everybody. This is the so what panel. And our goal is to try and take all the—what is so that you've heard and try and make some sense of it, give you some perspective on it. I will just briefly introduce the speakers by name and title. If you want all the detail about them, you can look at the PDF you got on email, or look in the app, look at the website. As you can see on the screen, this is the old white guy panel. Although, actually I should—you know, Doug would say he's not old. Hopefully, we are diverse in other ways.

Let me just go through the list. So, Blair Levin, he's a senior fellow at the Brookings Institution and equity analyst at New Street Research. Paul Kolodzy is an independent telecommunications consultant and a member of CSMAC. Doug Sicker is a professor of computer science and Senior Associate Dean of Computing at the University of Colorado. And David Tennenhouse is Chief Research Officer at VMware, and a member of the FCC Tech.

Just a reminder for everybody, both the panelists and the audience, when you do Q&A, please define your acronyms. And you might think, you know, we're all experts here. We know what all the acronyms meant. But we actually have a case this morning, where the acronym DSS has two distinct meanings, distributed spectrum sensing and dynamic spectrum sharing. And so it will help everybody if you define your acronyms. So that's where we are. What I'd like to do is to just start and have each of the panelists just give us four or five minutes, a sense of what they think is important, what they've taken away from the conference so far. And we'll start with Blair, over to you.

### 4.5.2 Blair Levin

LEVIN: Thank you so much, and then thank you for having me. It's really been fascinating listening to everything. I think I'd like to just start off by first pointing out that I'm like one of the few non-engineering types, American Studies major and law—law school. And so my observations kind of come from that different world, but they're in an effort to translate a lot of the discussion into different worlds. I'll start with a political observation and then ask two questions.

The observation I'd like to make is that zero trust is really a bad name. I understand the point. And I think it is accurate in terms of communicating an engineering point. But I will simply point out that I don't know that the public wants to buy zero trust networks or politicians want to support zero trust networks. And I would just note that when I was working with Doug and many others on the National Broadband Plan, one of the things we did was we got rid of the so called high cost fund because we realized that actually was a pretty horrible name. Nobody wants to contribute to a fund to increase high cost and we changed it to the Connect America Fund, because we thought everyone would like CAFs, you know. But that actually was the point,

to connect all of America. It's now been changed to Rural Digital Opportunity Fund because the current FCC thinks that that's really what its meaning is.

But talking about how zero trust is a problematic name really leads to the two far more important questions which are how does this discussion capital—translate to capital markets, where I spend most of my time these days. And then secondly, how does it translate to policy and political institutions? In terms of capital markets, I think it's really important to understand, as I think everyone does, the best technology doesn't always win. Of course, many of us here, certainly people my age can remember the battle between Betamax and VHS, where the ultimate winner was not the best technology. But it's also true the next generation tech does not always justify consumer change.

And I think one of the problems from a capital markets perspective about 5G and all the incremental CAPEX is what are consumers really buying? What's the compelling use case? Clearly, there's a compelling use case in terms of certain business applications. But as of yet, we haven't seen any with consumer. Now, of course, that might change. But my point is, a lot of the discussion doesn't go to what is a consumer proposition. There, we'll talk about that more.

Security is one of those interesting things. It's really not an issue as far as we can tell for our consumers until it's the only issue. But by then you're in a very different situation. The second point I would make is, how does it translate to policy and political institutions. And I'll just say I'm going to try to avoid making any partisan points though it may sound like I am making partisan point. There is a growing distrust of expertise in Washington, DC and around the country. We see this obviously with COVID. But we've seen it with a lot of other areas as well. And we've seen it a lot in the area of spectrum, where there are these huge battles between the FCC, and other government agencies that we—used to be kind of resolved quietly through expertise and through engineering. And it's not really being done that way. And you saw it. I think, most recently, when a senator, a senator from Oklahoma was holding up the Republican commissioner, Mike O'Reilly. Because O'Reilly voted for something which was not only approved by the Office of Engineering and Technology, but approved by five, all five of the FCC commissioners, a very bipartisan approach, and was totally about an engineering question. And the senator said, unless you change your mind on the engineering, I'm going to hold up your nomination and you will not be reconfirmed. That's kind of, you know, that's only within the senators rights, but it kind of violates the norms.

And the reason I make that point is, as we try to convince the FCC and other agencies about the importance of adopting certain points of view, we have to understand its implications on kind of the current populace politics, forcing people to effectively pay more for certain kinds of things. And that's going to be a problem. And I think as we think about the next administration, whether it would be a second term or a first term, translating good engineering into good policy through that political filter, and I think zero trust is one of those things that's going to have to go through that, that's going to remain a difficult challenge. Pierre, back to you.

DE VRIES: Thanks, Blair. I just want to pick up on something you've said. We'll come back to this whole question of zero trust. But I was fascinated when you said, you know, what's the consumer

value proposition? And Wall Street isn't seeing the value proposition. What does that mean, gut feel for you about the adoption of 5G? Because the carriers will only adopt what they can pay for, and they can only pay for what Wall Street will fund.

LEVIN: Yeah. So what it means to me is that fundamentally, 5Gs can be rolled out in business centers, high density areas. There is a certain cachet, as there was a few years ago with gigabit networks, where there's a certain percentage of people who have a lot of discretionary income and simply want the best available service. And 5G is that thing. But I think that, you know, that ends that order of magnitude, you could say, 15% of the consumer market, 30%, but it ain't higher. And particularly in a post-COVID environment where you have people who really are going to be you know, a lot more about Walmart than Nordstroms, I think 5G uptake is going to be enormously problematic. And I just think that that means that the networks aren't going to be built out as quickly in suburban, exurban, and certainly rural areas. Because again, there's no—yeah, and someone—and what will be corrected, but don't—do not see a compelling single application where people are going to say, oh, we must have that. Some people say that was true with 4G. It actually wasn't 4G, it was always going to be about video. It turned out there were other applications like Uber and some things that proved very valuable. But the market for 4G was always pretty clear.

### 4.5.3 Paul Kolodzy

DE VRIES: Right, thanks. Let's move on to Paul. Paul, I think you may be muted.

KOLODZY: Thanks, Pierre. Thanks for reminding me. You know, first of all, it's great to be at a conference where you pick up a few new things, some new ideas, and some new thoughts and some new work. And so I actually got some of that out of this meeting. So that makes it a win just in its own right.

I think that as we already said, the goal of this meeting was basically look at a spectrum, 5G spectrum and zero trust networks, and trying to figure out exactly how we're going to address zero trust networking challenges, hence. Now I look at it for zero trust networks in a sense in two separate categories, and looking what I called internal and external agents. I think you see a lot of that within the discussions that were going on this week. One of them is really with respect to spectrum and the physical layer, which is the external agents in the sense to—to provide zero trust. For example, you know, do you have enough trust of your information flow through the network? Do you have enough trust that the information is not going to be compromised? Do you have enough trust that it's going to be the typical CIA capabilities that we think about for trust, which is confidentiality, integrity and assurance? You know, and we heard a lot about that about trying to look at different ways of addressing that problem by looking at dynamic spectrum, looking at—I think Milo mentioned earlier about the end and encryption or tunneling issues, and looking at also diversity issues and trying to see if they can help you in the sense of these external agent. OK?

However, you also have to think about that there is internal agents as well. And we did talk a lot about that today, on this week, but we may want to think about that. And that is, when you assume that you have compromised hardware, software, or that there's analytics that is being taken—that's taking place at the boundaries. That we'd hear some things about supply chains trying to say they're going to take care of this and trying to secure those supply chains one shape or the other. We either secure those by requiring a particular supply—supplier. We can actually look at distributed or heterogeneous systems. That was discussed a little bit. And we've talked about open source as being it.

But what it—what I've tried to do is to try to make the sense of methodologies of not having an insider versus dealing with you have an insider, to begin with. And so that is one of the aspects that we—we've had projects when I was working with some of the people at DARPA, talking about insider threat, right? And how do you actually deal with that? I know we don't like to talk about that but if you talk about the military, it goes overseas, it does a lot of things where we don't have control of the network. It's different if you're in the United States versus someplace else. And so, that's one aspect that I kind of got out of this that we were talking about.

One other thing I'd like to talk briefly about is we are talking about operations that people are doing overseas, around the world, you have to start taking a look at the global marketplace and the equipment fires. This is more like the insider threat and the like. And that because of the global marketplace, you're not going to be able to determine all the different providers that are going to be an impact to any one network that you might use. You might be able to control that in United States, but you may not be able to control that elsewhere.

And so the question is, when we talk about some of these issues, we need to not talk about them just for the United States. We need to talk about them globally, because you're going to operate globally. And how are those things? Maybe some things that we actually put in place here may not be available there. And because the United States doesn't drive all of these economies, like they don't drive all the materials, and the components, and the chipsets, and the device, and the subsystems, we're not going to be able to control all of those pieces.

So the question is how do you actually address it when you can't control it? And that you're going to have to be able to understand how you work with a system that is not trusted, and that you have to be given up certain capabilities. And the one way that I think about this, something I brought up at the FCC TAC many years ago, which is I see a lot of what we do today, and a lot of the meetings material was building a better castle, then we would build—we would build higher walls, we would build thicker walls, we would build, you know, a lot of different things. But that actually didn't solve the problem for castles. They had to put archers up there. They couldn't be just defensive. They had to be offensive too.

And so the question is when you start talking about zero trust networks, what's your offensive side of that? And finally, I'd like to leave with one other comment which actually Blair brought up and I just wrote down here, which is your incentives of security. One of the basic problems is the value proposition for securities, especially for capital markets. You have a timescale problem. It's you have to do a lot of work to make sure that you have security. But people are only

interested in it when it's- something bad happens, and then it's actually too late. And so the timescales of developing security challenges are definitely completely opposite of the timescale that we tend to -

DE VRIES: Great, thanks, Paul. Just to pick up on something. We'll definitely get back to incentives. But I was really interested and this goes back to what Blair was saying about zero trust, which is people don't want to hear those kinds of words. But when you said, you know, the insider threat, something that Lisa Porter said on Tuesday was, you know, after Edward Snowden, everybody in government understood the insider threat and it became a lot easier to talk about zero trust. To what extent is that threat something that the general public or just you know, your CTO, CIO in some Main Street company have to think about? Or is it going to be under the hood, under the …

KOLODZY: And you just—you faded out there under the hood, under what?

DE VRIES: Yeah, so is that always going to be a hidden engineering problem that those untrusted experts deal with?

KOLODZY: No, actually, I think it has to be somehow formalistically looked at because it's going to get much, much trickier as time goes on. And what I call the insider threat is two pieces. One is the individual. So it's the flesh and blood insider threat. And it's also the equipment insider threat. Who is going to actually put something there, either person putting it there, or just because of your—how you buy equipment, that it's there. I mean both of those have to be addressed. Thank you.

### 4.5.4 Doug Sicker

DE VRIES: Great. Thanks. Doug, over to you.

SICKER: Thanks, Pierre. So, I agreed a lot with what I've heard so far on this panel. I'm going to try to take it a couple of different directions and hope this is useful. So my first comments aren't really—it shouldn't—I don't mean them to sound like a criticism. But I think this actually indicates how early we are in thinking about zero trust in the application to spectrum management and wireless networks.

What I was hoping to see out of this conference was a bit of a roadmap, how zero trust is going to apply across all the types of spectrum users and what this might mean from a technology perspective, how we could inform public policy. And I don't know that I saw that, I saw bits and pieces. But the reason I mentioned that is that I think the concepts of zero trust will apply very differently, depending on the application to the use of the spectrum. And really understanding that might actually help us think about what policies might help bring some of this into focus. When I think of what traditionally ISART looks at, a lot of these things are a bit outside of scope. I'll come back to that a moment—in a moment.

I also wonder when we talk about zero trust in this domain, whether it causes any complications, or rather complement spectrum management efforts that are underway. And at best, they would be—zero trust would be orthogonal to it. But I'm not clear on that, and that there's some other thing that I could hope to really understand kind of walking through this conference. So again, I—not a criticism, rather, I'd say a challenge, I'd like to see more of that. I'd like to understand how these things actually fit.

And picking up on a topic that was talked about a lot about this—the meaning of zero trust and whether we really are talking about zero trust is an interesting concept, because much of spectrum management is based really on trust. And, well, maybe it's not even trust, maybe it's faith, faith that things will work as they're supposed to, and overtly conservative faith in the design of the protocols and the assignment of spectrum. But what we're talking about obviously is something that's further up the stack necessarily, and it really shifts to crypto constructs that we can have faith that would because we can—they're provable.

So—but I believe that this applies to a more narrow aspect of what we usually do at ISART. When I think of ISART, I really do think of things in the area of vector management and metrology and interference mitigation, a lot of these sorts of things. So understanding what any of these brings to the classic problems of interference with GPS, or interference with radio astronomy, or anything else, or whether any of these have differences in their application, I think would be very, very useful thing to understand better.

I guess I want to also take a step back and touch on some of the things that Blair mentioned. We clearly have a broken model of spectrum management at the federal level. And things have gotten worse. I do wonder what we can do with an ISART. And in any of these conferences that we're doing that that might improve this posture of science and measurement and engineering, as it applies to these national needs. And I do hope that one of the things that we think about as we start thinking more about security, is how that fits in to the economic rationale and to the national needs rationale. As was said, there were often this attribute that comes only in emergency, only when we're worrying about it, rather than where it should be in the planning stages. But if we can't get those incentives, right, and we can't think about how some of the supplies and where it applies, we won't be able to actually have that kind of coordination and management at fair enough level. And that brings me to one other thing, and somewhat more controversial. I do see a strong leader, a higher level of coordination in spectrum management. And that's something that I hope that we could see looking forward.

DE VRIES: Follow up on something you said about you know, you—one of the things you were expecting that you didn't see was a roadmap. And that's probably because we're so early. And that's one of the things that surprised me over the conference. We've done a number of conferences on it, is that security, forget about zero trust, just worrying about jamming, sniffing, spoofing at the radio layer. If you compare it to cyber security and the endless conferences on cyber security, radio networks do seem to be really late. Why?

SICKER: Do seem to be really …

DE VRIES: Late. I mean, we are coming to this late, the thinking about resilience about security seems to be very far behind high layers in the network.

SICKER: Well, I mean, in some way, that's the case. In some way a lot of the aspects of the problems that have been solved in the wireless space as it relates to security are unique. And in that sense, it's not surprising that third—the third that it's later. However, many of the problems that get identified as security problems are really reliability or resilience problems, and have a different application, a different way of being solved and consulted a different layer. When I think of a lot of the stuff that's going on right now that's interesting, I see some really wonderful hardware that's coming out, the software that's coming out, that's not being talked about even here. That could have a profound impact on improving resilience of the networks at the radio level. We are seeing the ability to suppress interference with adjacent links in ways that we couldn't do before, anti-jamming technology and other things that are coming out, really complement this issue of what we think of and how we conflate kind of link in physical layer availability with a lot of the other security things that go up the stack. I, you know, I would love to see, ISART for example, focus almost entirely on that. What can we be doing at the physical layer to really improve those links, and that was resilience and reliability at the link. And that's not to say that we also shouldn't be you know, you heard my complaints a couple weeks ago. Zero trust is inherently a multi-layer issue. It's not a five layer issue. So we need to be thinking about much more, and Milo talked about that earlier. So I think I would say that the challenges in the radio space are unique enough that—and conflated with problems with link reliability that they're unique.

### 4.5.5 David Tennenhouse

DE VRIES: Right. David, over to you.

TENNENHOUSE: OK, thank you, and great to be here at ISART. I'm going to say a few words about virtualization then dive into zero trust, as with others and speaking for myself as a research guy and not for VMware's product team.

Something we haven't been talking about these past few days is the role of virtualization and software defined networking will play in improving the robustness and resilience of 5G. The essence of virtualization is the recasting of physical resources so that they can be safely and dynamically shared. In the 5G core virtualization will not only bring enormous cost savings, it also allows us to isolate the network functions, monitor their internal operations and interpose on the flows of data in and out of them. It also allows us to implement network slicing and micro segmentation, all these are key enablers of zero trust. We're also going to push many of these benefits to the RAN as we take vRAN to the CU and eventually to the DU.

Going out on a limb now, if you asked us to do that, I think of spectrum sharing as a step towards virtualizing the spectrum itself, so that it can be dynamically shared. Eventually, we'll go beyond sharing spectrum between government and commercial use. We're going to extend the concept to facilitate the dynamic sharing and spectrum amongst operators. We're going to have

to find a balance point between providing enough fixed assignment to incent infrastructure build up, and enough to that dynamic assignment to aspect—and to flow to where it has the highest utility.

The getting to zero trust, I want to address the conundrum. Why has this event focused on zero trust than so much of its time talking about network robustness, and resilience? In computer systems, zero trust is focused on protecting users or organizations from having their data fall into the wrong hands. Milo Medin did a great job of describing this in this morning's panel. To recap, users and organizations assume the network is compromised and can't be relied on to ensure data security. The network doesn't inherently trust users, their devices, peer networks, administrators, et cetera.

But, and here's the big but, zero trust networking doesn't address availability. And that's the reason for this week's apparent contradiction. Availability is the reason we've been hearing so much about robustness and resilience. So how should we think about availability?

Let me divide this into two subcases. I think this is part of what one of the speakers was asking for. First off, Dr. Porter's characterization of zero trust means we can't count on perfect availability, bad stuff happens. So all the talk of having the 5G network host real time control, control over vehicles and factory automation, et cetera, things that can lead to loss of life or property if they go wrong, that's such nonsense. If the stakes are really high, engineers don't design systems that depend on real time wide area connectivity. Instead, we deploy systems that work better when there's connectivity, but are backstopped by a fail safe that doesn't rely on that connectivity. This suggests we're suggesting some of the five key requirements that combine extremely low latency with extremely high reliability. Engineers won't rely on them anyway. And as Kumar Balachandran said on Tuesday, every new performance requirement is a potential risk.

OK, so the second subcase is more subtle but more interesting. There are many less urgently critical systems that depend on connectivity to facilitate their efficient operation. They have more relaxed requirements, but our society will not function for long without them. This is the soft underbelly we need to worry about. Even though we can't count on perfect availability, we mean—need to be able to rely on some imperfect form of available. The good news here is instead of trying to have fully trusted networks, we can relax some of the constraints. As Milo described, we use zero trust networking to protect the data itself. That takes a big challenge off the table. It means the network is focused in their key role, which is to move packets from A to B. And they don't need to be perfect to doing that. They just need to do so with a high enough probability to keep applications functioning.

And that's why the 5G work on improving robustness and resilience we've been hearing about this week is so important. As William Webb suggested on Monday, we don't even need any one network to obtain that statistical availability. We just need to be able to count on the ensemble of network operators to provide an acceptable degree of resilience and robustness.

I view the need for probabilistic model of availability as being a special case of Dr. Porter's call for risk analysis. If we can statistically characterize availability, then we can let zero trust networking and end to end application thinking carry the water from there.

So finally, I just want to emphasize another point that was made on Monday, the need to distinguish between small outages and big ones, and to have a separation of concerns with respect to how they're addressed. Operators will deal with the local outages the customers complain about every day. But operators, regulators and government agencies need to work together to guard against widespread and especially against multi-operator outages, whether they're malicious or accidental.

DE VRIES: Thanks, David. Just trying to make sense of what you said and when we're about to just do another round and I'd like all the panelists to just take the opportunity if they want to reflect on what everybody said. But in—one way that I'm trying to make sense of part of what you said, David, was zero trust is perhaps not the right term. There's been a lot contradiction and complication around it. And we should think more about availability. Is it a means versus ends distinction? That actually we should be talking about the ends we're trying to achieve availability, not the means zero trust?

>> Well, I guess I'd go to, you know, I think Lisa's comment that zero trust is more a philosophy, right, and kind of a defensive approach. And I think that's the bucket you want to have it in. Now in the networking world, you know, we talk about zero trust networking, and that's a mechanism, right, to protect data in the presence, you know, of bad actors. But I guess my observation is, you're still going to need some degree of availability, but you don't need perfect availability. So you know, it's that zero trust philosophy leads you to saying, let's not count on perfect availability, but I don't think it can take you all the way to saying, Pierre, I don't need anything at all, right? For certain extreme cases, and I was identifying things like the vehicle or that factory where somebody might die if you don't have connectivity in the short-term, you just shouldn't do that. You need to have a backstop. But for many, many other cases, we can rely on something softer and have this more statistical form of availability. And I think that's something that our community can deliver.

### 4.5.6 Panel 5: Q&A

DE VRIES: Very good. Thanks. So, well, let's just go back. Blair, do you have any thoughts off the cuff prompted by what you've heard in the last three minutes?

LEVIN: No additional thoughts. So I certainly appreciate how everybody moved into a lot of different topics. It's a very robust discussion.

DE VRIES: Paul?

KOLODZY: Actually, I want to comment briefly, I mean, David put together there and discussed. I agree and disagree. And I think it's kind of an interesting area, which is, what are you trying to have at the endpoint? Sometimes we're now moving to more levels of autonomy. And so now

the question becomes there's a trade space going on there for availability and autonomy, and what latency and like that you need. And I think that we don't, we tend to forget, we tend to be so focused on our problem, that we don't ask the question, what's the application and is there things at the edge that are happening that makes the network not as critical anymore?

DE VRIES: Thanks. Doug, any thoughts?

SICKER: Sorry, I was on mute. No, I agree with the other panelists. And I was pleased to hear that I wasn't confused with the narrow scope of zero trust. I had mentioned this to you, Pierre, that you know, we were kind of applying a narrow problem to—a narrow solution to a wider problem. And, again, I think it's interesting, but I'd like to know exactly what problems does this solve for us here. And that would be probably one of the most redeeming aspects of this conference to know, OK, well, what do we get out of that? But I agree completely with David in terms of availability and kind of the robustness of the link is distinct from what this provides.

DE VRIES: Yeah, I think this is one of the questions that I'd like to circle back to everybody right at the end of our session is something like, what should we have called the conference? It wasn't zero trust. You know, is it a naming issue or was it a substance issue? It sounds to me as if what I'm hearing from you guys that it's a substance issue. Let's just get to a few questions and then just remind that for folks, you can click on the Q&A button on the right of your screen and put in questions there. If you see a question you like, click the like button. That will help me sort them if we get lots of questions, which I hope we do.

So the next thing that I want to get to a nice—you know, one of the reasons why we have Blair go first is that there was pretty much a consensus that we all just want to cue up what Blair had to say. So I'm going to cue up something else that Blair was saying, which was this distrust of experts, which we've seen. Personally, I think that there's actually a lot to that. And I guess I can say that because I'm STEM educated. The way I was thinking about it is, you know, one, it's always good to start with an Einstein quote, even if Einstein didn't actually say this. And the thing that came to mind that I stumbled on recently was he said that the intuitive mind is a sacred gift and the rational mind is a faithful servant. With the implication we need both. So we've had a lot of rational analysis so far this week. And, you know, that's where I imagine all of us operate. But my challenge to you is when you think about this field, and when you think about your reactions to the conference, what feelings come up for you? How do you feel about all this? Do you feel excited? Do you feel frustrated? So actually, since nobody's answering- hold on. Go ahead. Go ahead, Blair.

KOLODZY: … is that I feel kind of a malaise.

DE VRIES: Mm-hmm.

KOLODZY: And the reason I feel malaise is because we're thinking about we're still in the 1980s, and we're trying to look at problems the same way we look at them then, which is understand them, evaluate them, try to figure out what the solution and we're being typical engineers, which is great. Engineering is the first step that you do. But then there is not that innovation. I

hate using that word. But looking at this at a different perspective and asking the question, where are we going toward? And sometimes we tend to be looking at where we are versus what is going to happen over the next 5 or 10 years with these technologies, and ask the question where we should be trying to position ourselves. Not necessarily, in fact, we should be talking about 5G, we should actually be talking about what's beyond 5G or what is 5G going to enable us to do to be able to address this problem.

DE VRIES: So I mean, it sounds to me as if you say malaise, which is a lovely word, you're bored. But it also sounds like you're frustrated that we are being myopic. Is that right? Oh …

KOLODZY: Yeah. Go, Doug.

SICKER: Oh, I don't want to—I want—I thought Paul was going to answer that. But I wanted to—I wanted to say I'm concerned. And my concern is really—and if we narrow it back down to 5G is just the cost of doing business, from an op-ex and from a cap-ex perspective, particularly. What we have going on and how he's managed spectrum, I think, is broken. And it would take some interesting leadership to kind of move out of the rough stuff we're in I think in the spectrum management perspectives. And this also goes back to Blair's comments about the discord that's going on within the federal government. All of these things caused some concern that there isn't leadership to kind of move us beyond, but the battles to have a national perspective on what 5G is and what it could bring. But my concern is actually, again, the cost Blair mentioned at the beginning, which is, it's going to be have and have-nots. And that's a very unfortunate thing when we think about it going forward. This is where government should be stepping in.

DE VRIES: And the other bidders—that's, yeah, David first, and then we'll go to Blair. David first and then …

TENNENHOUSE: Yeah. So, you know, when you ask about emotion, I'm going to say I'm excited, alright? That, you know, in the sense that, you know, we're going to have this ability to deliver gigabit, or at least some fraction of the gigabit to people wirelessly, and that means we can deliver basically all forms of content of whatever resolution wirelessly, and that's just a huge change. Now, having said that, I also have concern in terms of the—you know, that the research for me is excited. From a longer term basis it's great. From the short—near term, I think I'd agree with Doug and some of Blair's comments, which is near term, there's concern over the economics of this thing. And I'm particularly concerned about the economics of millimeter wave. And, you know, whether or not it's actually really ready to deliver economically at, you know, at prime time, it's at scale. So, you know, we may need a couple more breakthroughs there is what I'm basically saying. I'm also concerned but, you know, we've got the overall economy, which might be you know, headed towards another drop, so we could end up with a rerun of 3g, which you may recall the adoption cycle. You know, the story ended up great in the end for us enthusiasts, but the adoption cycle was much longer than people expected, created quite a bit of economic hardship for operators, et cetera. So, you know, that's a—that combination of enthusiasm, long-term concern, near term.

DE VRIES: Blair?

LEVIN: Yeah, and just following up on David's comments, I think it's really important that scientific and technical work continue no matter what else is going on in the world. And yet we have to acknowledge that the year 2020 is going to be remembered as the year of COVID. And one of the things that COVID demonstrated really quickly was that in a world of remote everything there are lots of people who will not thrive. And that it's not only about not getting worse, I mean that it—this—it's going to get worse. And what we're going to see in here, just I could point to numerous examples, we're going to have millions of school kids who normally would go through what's called the summer slide, by which they mean, you know, you stop your reading level wherever it was in June and come back to school in September, it's now back to March. Well, they left school in March. And when they come back to a physical school, if they ever get back there, you know, they're going to be way behind in their reading. And we have all this wonderful technology, and yet, we're not utilizing it to solve that problem. And let me put that problem in really concrete perspective. Every year, educators get together and look at what are the fourth grade reading levels, and with just that one data point, they can predict with unerring accuracy the prison population 11 years later. That's going to be a huge problem, because reading levels are going to be way down. And my point is not in any way to criticize this kind of work, I'm just saying we have to keep in mind both the importance of constantly pushing the envelope from a scientific and technical perspective to build greater resiliency and growth in the economy. But we also have to understand that what COVID demonstrated is that we really can't have two different economies. We're all now on the information economy. But for those who aren't on it, we have some bigger—we as a society are going to have much bigger problems than we might have anticipated.

DE VRIES: So Blair, I take your point about the haves and the have-nots, and others have raised it and the problem- the problems that COVID has highlighted that we have for the audience of this conference. What would you say to us, what should we be doing differently given that?

LEVIN: Look, if I had a good answer to that question, I probably would have already given a talk on that or written something on it. I do think that the kind of scientific and creative expertise, you know, there are good reasons. And this goes back to a whole question of incentives. We tend to do those things which capital markets are incentive to produce, and capital markets don't effectively drive toward equity. That's just—that's not their job. But that is, in a way, part of the job of the government. So I don't exactly know the answer to that. But what I would simply say is we have to figure out ways of creating incentives for this community to solve some of the other problems. And if we're—you know, you—if the systems aren't secure, nobody wants to use them. And I love the timescale—the definition of that problem. But we also have to think about if we're going to essentially advantage lots of folks to be able to do certain things, we have to continue to look at what does that mean for society. And what I think kind of—you know, this is—we dealt with this in the—with the disabled community. If you build it in upfront, you lower the cost by enough so that you can include lots more people, and we have to try to figure out are there analogies to that, to make sure that the changes that we're doing reach everybody?

DE VRIES: Great. So I'm going to take a few of the questions in the Q&A. I imagine that we're not going to get through all of them. I apologize to people whose questions don't get asked. I would encourage you to take your questions with you into the breakout rooms. So just follow on this. Describe a concern that a number of you have raised. I want to combine two of the most recent questions. One was it may be important to think about the economic and regulatory imperatives around this, you know, system features and then in one—in the case of the question it was like making it more trustworthy. So, you know, what are the carrots and the sticks? A related question to that was isn't—if we're expecting government to step in, isn't that asking for the impossible? Isn't government part of the problem? How should we be thinking about the role of those institutions? This is a jump ball. Wave your hand and start talking. David. David, you're on mute.

TENNENHOUSE: Thank you, different location of the mute than I'm used to. You know, something that I've kind of come around to over time is transparency can go a long way. So if in other words, if the government, you know, helps ensure the collection, the dissemination, et cetera, of information on the trustworthiness of systems, that then becomes the mechanism, you know, in a basis on which companies compete, the information's out there. You know, company that's doing well can trumpet that, that forces another company to respond. So, I—you know, having seen sort of many ways in which regulation fails, transparency, I think is a really good step.

DE VRIES: Oh, OK. Paul.

KOLODZY: Yeah, it's a good question, because I've been trying to look at analogies and where do you have regulatory effects and where can you actually build market value for these inverted timescales, meaning a very big issue that occurs very rarely and then you have to have a lot of investment. Chemical industry tries to do that. Pharmaceutical industry tries to do that. But the issue is, is that they've made it large enough that—of a community that they can state, they basically flatten the curve, that those spikes don't occur because many of the spikes occur, and they flatten them out over time. I think regulatory comes into play when the spikes are so infrequent, that you try to find some way of leveling them off. That way, it could be maybe liability, maybe or an advantage. So somehow, how do you provide an advantage to somebody who does an investment, right? So that when a problem occurs, like this insider threat, or whatever, or mean, one zero trust, that it actually if they've done the right thing, they get some kind of market advantage. Out—to me that instead of having a stick, I'd rather have that carrot where they can say, hey, they can look at the market, can look—look at the probability of event and then try to actually fit this in as risk benefit ratios.

DE VRIES: Is there anything that's preventing the market from doing that now?

TENNENHOUSE: I think …

KOLODZY: What's in David's point—Sorry.

TENNENHOUSE: Go ahead, Paul. OK, so let the transparency, you know, make it really apparent when somebody screws up.

DE VRIES: OK. So that's one of the things that came up in a number of panelists. Thank you for that cue, this point about transparency. One of the topics of the—one of the four pillars of the conference was data collection, measurement, observation, that's something that IT hasn't—has always done. And one of the things that came up, two related questions. One is if we're going to be collecting all this data, different people are going to be collecting this data, but the value is greater when it is shared. So how do we incentivize sharing? So that any thoughts on that? How do we make data that people need to train engineers or build better systems available to everybody?

SICKER: So this gets back to my earlier comment, which nobody ever wants to hear, which is you know, this is the role of government to be, you know, helping or encouraging or obligating the sharing of this kind of data. But I would argue that I don't even know what data we need to collect or let alone how to collect it. So if there is some fundamental metrology that needs to be going on here, to get to the heart of what's happening. When I look at the—like the National Broadband work that launched the early work in measuring broadband access speeds, there are so many ways of doing that now. And each of these has their strengths and weaknesses, and even just coming to a core set of understanding would be an important set of per step, which is, how we do measure this thing. And in parts of computer science, we have this very, very well agreed upon, there are four areas where we understand what it means to measure. We have test sets for doing it, but we really don't have much of that in this space. And we certainly don't have a way of collecting or sharing it at this point. And if there was a time as Henning and others pointed out earlier, that the federal government did collect this data. And that was gotten rid off. In my early days, when I was chairing the steering committee for NRIC, we were still collecting data and looking at outages. And much of that is gone, or it's been so weakened, and so made not transparent that you can't get your hands around it. And that's a real problem on—you know, data consumers don't have access to data, let alone public interest groups who would actually probably process that data and give signals to consumers based on it.

DE VRIES: Go ahead, Blair.

LEVIN: Yeah. And I think this is a really important point. And I would argue that in an information economy, the government should look at itself as needing to make sure that it is a repository of common, reliable, relevant information that markets have no incentive to collect. And it's not clear to me that the market really does have incentives to do this. One way of doing it is to essentially have the government say to industry, we're not going to tell you how to do it. But there should be an industry driven group that ranks for example, security. Now, part of the problem with that kind of process is that you can, well, if you do security, should you do performance? Should you do price? Should you do—you know, there's a number of different factors. But at the end of the day, I mean, I think that is actually the government decision. What are those kinds of things that should be ranked? Some years ago, there was an effort that really was both a kind of a public and private effort that ranks the energy use of a building. So we have the LEED system, which, you know, tells you whether in a building that's energy efficient.

That did lead to those buildings getting a better rent. And in the same way, if you had networks that were ranked by security, and there were big office buildings, who knows what the future of office buildings is as we all are doing this for our homes. But still to have kind of like a one to five ranking, it would arguably lead to the higher rents and stuff like that. So government doesn't have to do all the details, but government absolutely has to do the job of making sure that certain kinds of information, security be one of them, that that information is collected not only at the time of the emergency, but on an ongoing basis. And one of the problems, frankly, that I think the FCC has, is that as we got into the post 96 act competitive world, the mindset was, well, now we have competition, competition takes care of all problems. And I would argue that, well, it doesn't really take care of the problem of information. Effective markets depend on information. And yet, there's lots of incentives to not give consumers information. And government, it doesn't need to price regularly, it doesn't need to do a lot of other things. But it should give better information.

DE VRIES: Thanks, Blair. David, do you have a point? You're muted. There you go.

TENNENHOUSE: Yeah. Actually, I think just about along the way covered, you know, a lot of those points. One thing I'd say is sometimes the government—I want to actually, I guess, emphasize one of Blair's points. The government may only have to give soft nudges. So for example, when it funds academics to, you know, get started, say an academic does an initial benchmark, that often leads to an industry group, you know, now the interested parties start realizing, oh, we're going to get judged. Next thing, you know, you've got an industry group where different parties are collaborating on that benchmark. So, you know, government, I think, in some cases where, you know, you're absolutely right. In some cases, it should be the source of the authentic data. In other cases, it may be able to just, you know, nudge in various ways, and academia and research can play a big role here, too. I will say, like NIST and you know NTIA and these organizations have played very big roles over the years.

DE VRIES: Thank you. Paul, before I turn to you, I just want to throw in something from the Q&A, which came up which is when sharing data, so this is more of a technical question than the regulatory engineering - regulatory institutional. When sharing data, how can we verify the accuracy of the combined set of data when it comes from different sources? And also, and this is a question that a panel yesterday took a hard pass on. How can we ensure privacy? And I'll add, do we have to worry about the wiretap laws? Paul?

KOLODZY: Wow. That was a great setup. That was exactly where I was going. I'm actually all for transparency and I want to collect lots of data. And usually, if it's just the four of us that are on this panel, and we're collecting the data, I'm sure it will be done correctly and we would keep it private. My biggest issue is that it's usually one generation after us or two generations after us who have all this data, that actually with all the analytic skills that we have been developing in this country that people have made hundreds of billions of dollars on, the question becomes, how do you prevent those kinds of skills being applied to the data? I think there's a great research question there. Meaning can there be homomorphic processing to get information on this, is there technologies that can be developed so that we can collect all this data to get all this

transparency, but to somehow ensure that you're only answering the questions that you're allowed to answer or ask, I should say?

DE VRIES: So David, if you could just make it shorter? Like we've got—we could probably talk for two hours.

TENNENHOUSE: Yeah, I just want to—I just want to point folks at differential privacy. So one of the few places we can do well, we can say something grounded in math about privacy is when you're talking about aggregates of data. So there's some really pretty work there.

DE VRIES: Yeah, wonderful point, took the words. But one of the things I'd like to move on, we've probably only got about five minutes before we start wrapping up, is the question of complexity. And actually, this is also partly a cue for thinking that David has been doing about AI and machine learning. You know, another supposed Einstein quote is everything should be made as simple as possible but not simpler. And since I'm not an engineer, it's not clear to me whether that rubric was observed when the 5G architecture was developed. But clearly, we're introducing a lot of new services. We've already had a quote, you know, Kumar has been quoted, you know, every new performance requirement is a potential risk. Milo and Wayne yesterday talked about the biggest threat that they see is complexity management. So how do the panel think about the problem of complexity management when trying to have a resilient, robust network and what we should be doing going forward about that? Go ahead, David.

TENNENHOUSE: Well, you know, one aspect, you know, reduce the requirements, right, clearly helps. But the other is this the space I'm actually really optimistic about. And, you know, in the kind of cloud side of the world, we've got a lot of new approaches to automation. It's not just about machine learning. In fact, it's about declarative methods where, you know, the operators describe how they want the thing to behave and the system is automatically nudged by continually measuring present state versus desired state, to where it needs to be. And, you know, we've actually gotten pretty good at this. So, you know, complexity is something that engineers, you know, master, that's their job.

DE VRIES: OK, so—but 10 seconds. I think you have something very interesting. DARPA has been trying to do something exactly in this area, which is actually the question, how do you create complexity for your adversaries. You'd be able to deal with the complexity on your own. Given the tools and some of the research, that could be a very interesting process. It's almost like doing the same thing try to with cryptography, is try to understand how do you use that kind of asymmetry to your advantage. You know, one of the things that I want to go back to, and there are a couple of recent questions in the chat is just about this whole question of zero trust. Again, let's just keep worrying away about a little bit. There was one question, which is, does zero trust imply that zero trust is written—is needed to preempt a cyber security warfighting arms race? And is it realistic to expect that to happen? And the more general question, is zero trust a critical technical topic or is it a statement that resonates with general trends in society? Blair, I think I'll start with you since I think you've said right at the top that zero trust does not resonate.

LEVIN: Yeah, it is a term that automatically raises the question of trust, which is one that I think most consumers don't think about. And therefore, why are you kind of—it's almost as if you had a hamburger, because they're trying to sell a hamburger that's like almost safe. You know, it's like, why are you talking about safety in hamburgers or, you know, it's like the—you want to assume that kind of level.

DE VRIES: But that—do we end up as a community misleading or lying to users if we pretend that something is trustworthy that isn't?

LEVIN: No, it's a great question. And I don't know how to answer it, right. Look, I think there's, you know, one of the things that will be—will happen over this decade is that we will continually see market forces drive certain technologies in ways that have short-term financial gains but have long-term issues, such as not building in these levels of trust, but where kind of the liability is. It's kind of like, well, you know, if you lose, you go bankrupt. But if nobody notices, you make a lot of money, fell off to somebody and you have out of—and you get—you get out before you're caught. Government institutions currently are not operating in a way to do that. We are, you know, the most institutions in government are still operating the way they were back in the 1950s. Yes, they all have websites now. The websites aren't always that good. So they don't have—the government doesn't have the technical expertise. And whether it be questions of AI or 5G or many other things we can think about, we need to have institutions to figure out how to create the appropriate incentives to be fair. I raised that question about zero trust, Doug, because it's really counterintuitive. But I don't think I have a solution to it.

DE VRIES: Go ahead, Doug.

SICKER: So I said this before, I mean, I am concerned that we are misapplying a very legitimate security mechanism, zero trust, to a bigger set of problems. It's not the silver bullet for all the security and all. It's a way of approaching these interfaces and these boundaries where there had to be some trust put in before that we now have other mechanisms that we can rely on. And in some sense, it's real trust. It's you're taking something from a—you're taking something up a level where it's verified. But this is a very narrow set of problem that it solves. And that's why I said it's not a panacea for wireless. That was my point at the start of my talk. And so …

DE VRIES: So my question for you would be, Doug, how would you frame the problem we should be looking at?

SICKER: Well, I mean, I think it's the traditional problem of what are all of the threats and risks that we see across this space from if we are focused on security? And how can we, you know, mitigate as many of them are the ones that are of the highest caliber? You know, do I believe that 5G is going to expose more surface and lead to more attacks? Yes, I do. I'm not as optimistic maybe as getting there, but I do believe we'll see some, you know, an increased set of opportunities just because of the surface area, and the complexity. But with that said, that's me looking through it from kind of a penetration testing perspective, something that I do a lot of—that I play around in. That's only one aspect of security as well. There's so many things to be considered in this big bucket of what you could—what you worry about as a secure network—

secure wireless network. And again, we still are conflating it with all of the availability issues at the physical layer. So I think if we don't parse those out, we'll be kind of confused in what we're discussing. And I certainly think that zero trust is a worthy thing for us to be pursuing. But we also have to realize what it applies to and what it doesn't apply to. And that's why I thought it would have been useful at the beginning to say, here's what we're doing as a roadmap for wireless.

DE VRIES: Thank you very much. So we've got 10 minutes left. So I'd like to just do a wrap up. And we'll go in reverse order. David, we'll start with you. And then we'll go to Doug, Paul and Blair. But my question for all of you—And of course, you know, you can talk about whatever you want to talk about. But my question for you is what do you think is the most pressing question that this community should be addressing going forward? The—another way of framing it is we're going to have to make good decisions going forward. We're going to have to pick research areas. We're going to have to pick technologies. What are we lacking in order to make those decisions? David, over to you.

TENNENHOUSE: Well, I'm not sure if this one, you know, hits the mark on most pressing. But it's coming at us really fast. There's wide open questions around the use of ML within the network. You know the—particularly the kind of ML, machine learning, that everybody's really excited about are these deep neural networks. And the catch is we don't understand how they work. And if we'd apply technology, and I should actually say, people are now looking at using these things really deep within the bowels of the network, you know, for congestion control, for dynamic spectrum allocation, for all sorts of things that are really in the real time aspects of the network. And if you embed in the network something where you don't actually understand how it works, and you don't, in some other way, constrain it, then inevitably, it's going to surprise you, it's going to fail when it gets unexpected data, and people are going to—adversaries are going to attack it. Oh, you know, this stuff is coming very fast. It's coming towards the real time aspects of the network. There are ways to constrain and reason about how these works. You know, even if you don't understand it, you put it in a box and you wrap constraints around it, and we need to get there. And we need to establish that it's good engineering practice.

DE VRIES: Thanks very much. Mr. Sicker.

SICKER: So the question was what is the most pressing question?

DE VRIES: By other words … a roadmap.

SICKER: Yeah, exactly. That was one of the things I said earlier but—and the other reason I say a roadmap is because I think it matters what spectrum user you are, and what your concerns are. I agree with David that ML and a lot of AI tools are coming down. The ones that I'm seeing applied in wireless space, I think are pretty well-bounded and I think we understand how they work fairly well. I've been playing around in that space. My concern still is why are we not adopting technology that's out there that could improve some of the situations that we know are happening? And maybe that's an incentive problem. And understanding those incentives of what we could be doing. There are things that we could do in the radio astronomy space to

protect them better and kind of isolate them. And radio astronomy is very different from GPS, I think. I think we can all agree from that, that GPS really needs to be protected in an interesting different way. And so, what can we do to move ahead on some of the wonderful research that's going on? And this is another thing that was brought up before, which is, you know, this kind of idea of what's the horizon of research? And are we going to get stalled? I don't see it at this point. But maybe there'll be a feedback loop in terms of suppressing research dollars. At this point, we have so much pent up research that has been done looking at solving 70 of these problems that have not been really adopted in the—in the wireless space, you know, and that's a curiosity to me. I spent my last five years playing around in the terahertz, that's still way out. So we have a lot of work that's pent up ready to release as the need comes. But again, I still wonder why we haven't gotten more. And I'm not talking dynamic spectrum access. I'm talking fairly straightforward adoption of technology that could better share a spectrum. And I wonder why that is. And that's an open question for me that I think speaks to the need of kind of some roadmap, thinking about future use of spectrum.

DE VRIES: Thanks. Paul?

KOLODZY: I'll take this a little different. I like to try to get the incentives right. And so, I'm going to try to say that maybe there's two real simple questions that we can try to answer. And that is, how do we get the incentives that the consumer or the user is actually the one who wants to drive this? Meaning you had drive—you had your security software, right, for your computer. Why? Because when you ran it, you actually saw all the viruses that took off your machine. So there was a feedback mechanism that gave you that you had a problem, your machine slowed down, you use this virus software, and eventually took care of them and took care of it. So I wanted to ask the question is how do we try to make the application layer drive the diversity of the network, in a sense is how to move the security to the user? How do you actually get the user to have the knobs to actually impact their own capabilities and their own security? The second one which is like, which is really similar, which is how do I drive that by getting the consumer? How do I get the consumer the tools to be able to measure security in their own right? But that way, they can actually ask the question, given this feedback in this transparency that we're talking about, basically, to understand that they have a problem, they are at risk. Now, they may not—yeah, they'll take the—they'll make their decision if they're—if that being at risk is important or not. But at least it will get us as a research community to start thinking about with all those knobs that are now in the network, maybe some of those knobs should be pulled out of the network and not be just the ML operating, but that the user operates on them.

DE VRIES: Great, thank you. Blair, over to you.

LEVIN: Yeah, I would just follow up on that. And I think that that's a really important insight, which is, how do we think about it in terms of the tools that consumers get? And I would just end by saying that, that's unlikely to happen unless there's an intermediate government institution, or some other kind of trusted, nonprofit institution whose motives are to achieve that but who may not have a, you know, financial stake in the game. And I think that that's, you know, that's part of the problem that we see, you know, on different—a variety of different fronts. I'll just close by saying it was, you know, fascinating watching the big tech hearing the

antitrust hearing a couple of weeks ago where, you know, if you were an antitrust lawyer, you might have said, well, wait a minute, why is this guy waiting privacy? That's not really antitrust. Or, you know, suppressing conservative voices, is that really antitrust? But the point is the public, the government, and the kind of folks that most people on this call are working with or for, we have to figure out better ways of giving people tools, so that they do trust it. And what you saw in that hearing was—and really, what is remarkable change, I think, from 10 years ago, again, when Doug and I worked on the National Broadband Plan, there was enormous trust in the companies that no longer exists. And I'm not pointing to specific companies, but there's just a level of distrust that makes it much more difficult to, I think, move forward the way we should.

DE VRIES: All right, thank you very much. We are getting close to wrapping up. And one of the things that I was interested in listening to all your comments, actually, but particularly Paul and Blair at the end was talking about, the user and the consumer. And I think one of the things that we haven't had a chance to look at is what are the primary threats by the user type? So there are end users that are military grade. So right at the beginning of the session early on, there was a question, is it really important at all to think about military grade jammer resilience in military networks? You know, given what we know about 5G systems today, how much is good enough? Does anybody want to speculate about partitioning for the risk tolerance or the threats to different kinds of user groups? No?

SICKER: Well, Pierre, of course, we do that already. I mean, that's just kind of how it's done. And so …

DE VRIES: And what would you say is most vulnerable, Doug?

SCIKER: To what?

DE VRIES: So you—because you—so let's think about risk. You've got, you know, high impact, low frequency risks. You've got high frequency, low impact risk. They will be different for different groups. Who needs most attention to be protected from risks?

SICKER: Well, you know what, you know that risk is this kind of exposure and, you know, what's the probability and what's the impact, right? We tend to organize around that and organization had a lot to lose, are the ones who are going to be most sensitive. You know, some of the stuff with movement towards 5G and how we move up into the core of the network and the potential, you know, broadening of the impact of an attack might make consumers more interested in what it means from a security perspective. But clearly, the military and the government and others are going to have a much higher bar. When I think of classic attacks in the network, what it tends to focus on are high resource, you know, high dollar mark resources. And this could be you know, healthcare, this could be credit cards, this could be any number of things. But, again, you need to, before you can pick any attempt at putting that down, you have to define what that, you know who—what is the actual threat? What's the attack and who's the target? I think the question about, you know, does 5g systems need to have I think you said military grade anti-jam or something, of course not. But the military does need the anti—military grade anti-jam, so.

DE VRIES: Very good. And with that, our time is up. I'd like to thank all our panelists. One of the drawbacks of being virtual is you can't hear all the applause. But just imagine all the applause. My apologies to everybody whose questions—excellent questions did not get answered. Please take them into the breakouts, which we'll reconvene in 15 minutes. And with that, I will hand it back to our day moderator, Keith Gremban.

## 4.6 Closing Remarks by Sheryl Genco

GREMBAN: Well, I want to add my thanks to Pierre and the panel. That was very interesting and gave me, gives us all a lot to think about. So before our breakout session, I'd like to welcome back Sheryl Genco, the Director of the Institute for Telecommunication Sciences, who has some closing remarks to close out this fabulous ISART 2020. And just as a reminder, remember to join that center breakout room. It'll be fun to get your questions directly. Sheryl.

GENCO: OK, thank you, Keith. Audiovisual guys, can you hear me? Great. So the focus of ISART this year was on 5G and zero trust network. Wow, even the title is controversial. That makes for a very good conference. It was the 18th ISART, and I want to thank everyone. We sparked new research and ideas and thought for this last four days. I want to recognize the fact that we had a breadth of participants. We had government, industry and academia. This was not just a scholarly exploration, but a practical exchange of ideas, in how to operate safely in a 5G world and beyond. In the panel we just heard, a lot of conversation about whether or not we need a roadmap or a vision for zero trust. And that'll be some interesting thought to go through over the next years.

We set up the week by setting a baseline with tutorials and the current state of 5G. That was a fantastic set-up workshop. And I want to thank everyone who presented and attended. We opened the next section with setting the stage. We had talks from NTIA, NIST and DU. And in fact, Terri Fiez from CU made me really want to go back to school, some very, very exciting things happening at CU. And I don't think I'll be going back for another PhD, but was very exciting. We heard from Joe Evans in our keynote address, who is the technical director for 5G at the Office of the Secretary of Defense, and he provided significant detail about how the DOD is approaching 5G and zero trust.

The next day, we framed zero trust today. The panel gave a deep dive into what we thought zero trust means within the spectrum world and the known risks that existed today at the intersection of 5G new radio and zero trust. There was a lot of excellent conversation in the breakout rooms during that particular day. And you know, as we just heard in this panel, a lot of conversation about whether or not a zero trust role is a liability. What does it mean? Is it necessary? There are many, many things coming to share that perspective as we go forward.

5G design, resiliency at the radio layer. As you all know, ITS, has a long history of radio engineering and testing. And it was particularly interesting for me with my background. And in that section, we took a deep dive into the current state of open radio access networks, with various technical presentations and a very lively set of conversation. 5G deployment came next,

implementing secure and resilient solutions. Explored how to implement secure and resilient technical solutions in a rip and replace world with the zero trust environment.

So an overview of supply chain verification problems and possible solutions, which I thought was very interesting because it came from the inside channels and included the RF detection of malware. So again, I particularly was vibing with that section because of my engineering experience in that area.

We saw NTIA's own Jaisha Wray outlined all the things that are happening in the government. And that made my head spin. I might have to go back and look at her video and sort of try to learn more about what she was talking about. Thank you, Jaisha.

And 5G is certainly more attention related to security than LTE had. But this attention also has led to some advances in security, overall. So, during that session, one of the takeaways that I actually texted out to my family and friends, was that an attack occurs within three minutes of a new IoT device attaching to a network. That was amazing to me. And, you know, we – that alone was a significant outcome of that deployment action.

Went into 5G monitoring and data collection and the feedback loop there. Modern data is the nexus of feedback loop among design, deployment and operations, and could be the secure – the key to securing the 5G radio layer.

Doug Boulware gave us an excellent presentation, I felt, on the presentation of spectrum monitoring, the importance of understanding that from the RF side, the intersection of the vast array of data. This was sort of something that is also very near and dear to me, because then we saw a whole series of data that was collected from the air from Mark Gibson, and Northeastern University. The data collection and the platforms at Northeastern University also made me want to very much attend school again and dig into that. We discussed AI and machine learning as a double edged sword. Often actors with, you know, malignant intent do bad things, but they can also be deployed as white hats to detect and mitigate threats at far greater speed and resiliency than normal human. Big data is definitely an area of exploration and various places have put data sets online, including ITS and others. And we're looking forward. All of us together here at ISART are looking forward to understanding more about how new big data ML can possibly help us with our future research.

5G operations and implementing resilient zero trust networks came next. As a 5G monitoring and data collection, we saw the intersection of spectrum monitoring and sharing and looking forward to how we can collaborate with the – the many opportunities that give us many challenges. John Shea recognized this in his presentation of the policy and work that they're doing there. Significant value was brought up in the panel and the mixture of different types of information. And our previous panel just before my speaking really touched this. It's sort of the intersection of the network, the physical location, the endpoints, user roles, responsibilities, and many, many other pieces of information allowed, that will provide us a coherent and real time understanding of the use of network that we need to create. Our panel seemed wrapped up. I was very much interested in the idea that not only is it the network that we are trying to secure,

but bad actors, good actors can take many types of analytics on this data. And what do they do with the analytics?

We touched upon the ideas of security of private information, and what is done with the aggregation of data, and really something to be—understood in the years come. Another piece that came up in our just previous panel was this idea. I hadn't thought of it before, but this idea of the timescale security problems versus the timescale to protect. And that is really what made me scared. I mean, they talked about malaise or a difficulty. But that was a little bit interesting, because if we don't get moving on this, we're going to be behind the eight ball as a country. I thought there has to be a challenge that we drove down. I think it was Doug that talked about a roadmap. I think it's more than a roadmap. I think it's a vision, a vision of how we apply across applicants or use of the spectrum and how different users of this spectrum might apply zero trust.

So with that, I want to just recognize that I think this week, we definitely advanced innovation in communications technologies. We informed each other and we investigated some of our nation's most pressing telecom challenges.

I want to recognize the fact that we will be sending out a survey for—to those of you who participated this week and we really want to get—to hear your input. We know this is the first ever video and everybody wants to visit us in Boulder and we love to have you and host you here next year, if it will be possible. Over the next months, we'll begin to think about ISART 2021. So your survey and feedback will be very important, and we will take it seriously.

The slides from all the presentations are being posted and linked to each speaker on the website and on the agenda page. We received a number of inquires about if and when videos from ISART will be available. And, you know, there have been many important discussions this week. And we will be posting the videos on the ISART website soon. But we must comply with federal regulations in posting videos including captioning, and it may take us some time. We hope to make them available within the month.

I want to thank the honored speakers, the moderators, the thought leaders, participants. I want to especially reach out to all of you who had excellent questions not only in the chats but in the breakout sessions and made this very much virtual interaction worthwhile. I want to particularly shout out to Howard McDonald and Pierre de Vries whose questions made me think almost every single session. So, thank you, gentlemen. Again, to Keith Gremban, Pierre de Vries, Dale Hatfield from CU, Terri Fiez. Thank you for co-hosting. Thank you NIST for co-hosting, Melissa Midzor. NTIA, ITS Rebecca Dorch. Let's all give her a virtual applause, amazing, amazing. Andy Thiessen co-chair, and Lilli Segre, who was instrumental behind the scenes and helping us get all these fantastic speakers. My thanks wouldn't be complete without thanking the audiovisual team at Conference Services. Nice work, seamless. I sort of gave up all control of my life to this audiovisual team and it went smoothly. Thank you. Now, please remember, join our last set of panelists in the breakout rooms and chat with the polymaths about all of the things that we've just heard. We'll see you in ISART 2021. Have a safe, inspiring and productive year! So long from Boulder, Colorado.

NTIA FORM 29
(4-80)

U.S. DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

# BIBLIOGRAPHIC DATA SHEET

| 1. PUBLICATION NO. | 2. Government Accession No. | 3. Recipient's Accession No. |
|---|---|---|
| SP-22-558 | | |

| 4. TITLE AND SUBTITLE | 5. Publication Date |
|---|---|
| ISART 2020: Proceedings of the 18th International Symposium on Advanced Radio Technologies — 5G Spectrum and a Zero Trust Network | February 2022 |
| | 6. Performing Organization Code<br>NTIA/ITS.D |
| 7. AUTHOR(S)<br>Institute for Telecommunication Sciences | 9. Project/Task/Work Unit No.<br>3102012-300 |
| 8. PERFORMING ORGANIZATION NAME AND ADDRESS<br>Institute for Telecommunication Sciences<br>National Telecommunications & Information Administration<br>U.S. Department of Commerce<br>325 Broadway<br>Boulder, CO 80305 | 10. Contract/Grant Number. |
| 11. Sponsoring Organization Name and Address<br>National Telecommunications & Information Administration<br>Herbert C. Hoover Building<br>14th & Constitution Ave., NW<br>Washington, DC 20230 | 12. Type of Report and Period Covered |

14. SUPPLEMENTARY NOTES

15. ABSTRACT (A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here.)

The topic of the 2020 International Symposium on Advanced Radio Technologies™ (ISART 2020), which took place fully virtually August 10 13, 2020, was "5G and a Zero Trust Network." The symposium aimed to identify challenges for spectrum to be available, reliable, assured, and secure in a no-trust environment; explore potential technical solutions; and identify research areas that facilitate securing spectrum for rapid adoption of assured 5G networks. Opening tutorials, a framing conversation, and an opening keynote address were followed by four technically substantiative panels were designed to look at the zero trust theme from the design, deployment, monitoring and data collection, and operations perspectives, and the critical importance of feedback among all four components. A wrap-up panel brough together polymaths to help draw new insights and connections, identify potential new research areas, and add to the history of ISART triggering important out-of-the-box thinking, innovative ideas, and novel solutions. The text of these proceedings is taken from a transcription of the video record. A best effort has been made to correct spellings of names and terms of art, but it is in no way an "edited" transcript.

16. Key Words (Alphabetical order, separated by semicolons)
5G, open radio access networks, radio layer, resiliency, security, spectrum, spectrum monitoring, standardization, supply chain verification, Wi-Fi, zero trust

| 17. AVAILABILITY STATEMENT | 18. Security Class. (This report) | 20. Number of pages |
|---|---|---|
| ☒ UNLIMITED. | Unclassified | 227 |
| ☐ FOR OFFICIAL DISTRIBUTION. | 19. Security Class. (This page)<br>Unclassified | 21. Price:<br>N/A |

# NTIA FORMAL PUBLICATION SERIES

## NTIA MONOGRAPH (MG)

A scholarly, professionally oriented publication dealing with state-of-the-art research or an authoritative treatment of a broad area. Expected to have long-lasting value.

## NTIA SPECIAL PUBLICATION (SP)

Conference proceedings, bibliographies, selected speeches, course and instructional materials, directories, and major studies mandated by Congress.

## NTIA REPORT (TR)

Important contributions to existing knowledge of less breadth than a monograph, such as results of completed projects and major activities.

## JOINT NTIA/OTHER-AGENCY REPORT (JR)

This report receives both local NTIA and other agency review. Both agencies' logos and report series numbering appear on the cover.

## NTIA SOFTWARE & DATA PRODUCTS (SD)

Software such as programs, test data, and sound/video files. This series can be used to transfer technology to U.S. industry.

## NTIA HANDBOOK (HB)

Information pertaining to technical procedures, reference and data guides, and formal user's manuals that are expected to be pertinent for a long time.

## NTIA TECHNICAL MEMORANDUM (TM)

Technical information typically of less breadth than an NTIA Report. The series includes data, preliminary project results, and information for a specific, limited audience.

For information about NTIA publications, contact the NTIA/ITS Technical Publications Office at 325 Broadway, Boulder, CO, 80305 Tel. (303) 497-3572 or e-mail ITSinfo@ntia.gov.