Silicon Flatirons Conferences

Saving our Spectrum: Handling Radio Layer Vulnerabilities in Wireless Systems

October 19, 2019

University of Colorado Law School, Boulder, CO

Transcript (unedited)

This is a transcript of the Saving our Spectrum conference held by Silicon Flatirons at the University of Colorado Law School, Boulder, CO on October 19, 2019.

More information about the conference is available at https://siliconflatirons.org/events/saving-our-spectrum-handling-radio-layer-vulnerabilities-in-wireless-systems/

This transcript has not been edited or corrected in any way, and is presented in its raw form as received from the transcription service.

Information added to the transcript is *marked by italics*.

Contents

Program 2

Welcome 3

Opening keynote 5

Panel 1 - Mobile Communications 11

Panel 2 - Health Care 27

Panel 3 - Solutions and Next Steps 44

Closing keynote 63

Program

Welcome

- Pierre de Vries (Spectrum Policy Initiative Co-director and Executive Fellow, Silicon Flatirons)

Opening keynote

- Julius Knapp (Chief, Office of Engineering and Technology, Federal Communications Commission)

Panel 1 - Mobile Communications

- Moderator: Pierre de Vries
- Panelists: Jeff Reed (Professor, Bradley Department of Electrical and Computer Engineering, Virginia Tech),Tom Sawanobori (Senior Vice President and Chief Technology Officer, CTIA), Scott Fox (Chief Executive Officer, Global View Partners), Jay Jacobsmeyer (President, Pericle Communications Company), Yomna N (Research Engineer and Technology Fellow, Electronic Frontier Foundation)

Panel 2 - Health Care

- Moderator: Liz Harding (Shareholder, Polsinelli)
- Panelists: Stephen Berger (President, TEM Consulting, LP), Phil Englert (Global Leader for Healthcare Technology, Deloitte Advisory), Erin Kenneally (Portfolio Manager, Cyber Security Division, Science & Technology Directorate, U.S. Department of Homeland Security), Shreyas Sen (Assistant Professor, School of Electrical and Computer Engineering, Purdue University)

Panel 3 - Solutions and Next Steps

- Moderator: Keith Gremban (Research Professor of Technology, Cybersecurity, and Policy, University of Colorado)
- Panelists: Rebecca Dorch (Senior Spectrum Policy Analyst - Office of the Director, NTIA Institute for Telecommunication Sciences), Monisha Ghosh (Research Professor of Molecular Engineering, University of Chicago), Clete D. Johnson (Partner, Wilkinson Barker Knauer, LLP)

Closing keynote

- Dr Lisa Porter (Deputy Under Secretary of Defense for Research and Engineering, U.S. Department of Defense)

Welcome

Pierre: Welcome, everybody. I'm Pierre de Vries with Dale Hatfield. I'm co-director of the Spectrum Policy Initiative here at Silicon Flatirons. It's wonderful to see you all here today in spite of the first snow of the year. Thank you very much for braving it. You won't be disappointed, we have a wonderful lineup. Before I say a few words about the conference, I just wanted to do something very special — something we've been waiting for a long time — to introduce Amie Stepanovich, our new Executive Director of Silicon Flatirons. She's an expert in domestic surveillance, cybersecurity, privacy law. Comes to us from Access Now, Washington, DC advocacy organization, very experienced in the policy space, very experienced in technology. I'd just like her to introduce herself to you. Please go and say hello to her later on. Amie. [Applause]

Amie: Thank you so much, Pierre, and thanks all of you for coming here today. When the staff told me on Tuesday that it was meant to snow today, I laughed, because I just moved here from DC, and I couldn't imagine 79 degrees outside, that it would snow two days later. And yet, I woke up this morning, and there it was. So, I really appreciate you all coming out today. I want to thank a few people before we get started... In particular, Dale and Pierre, as well as Keith and Scott for the work that they've done, putting the program together today, that you're all about to see. I want to thank our amazing staff for their tireless work. Kelly, Vanessa, Sarah, and Heather have worked really hard. And if you see them around, I hope that you have a chance to say hi. They really try to put their heart and soul in these events. I want to thank our speakers who were able to make it. I want to thank our supporters and our partners, without which we would not be here today, on being able to provide this program to you. And finally, I want to thank all of you for coming, and for bearing with us, and with the weather. I cannot wait for this program. I'm really excited for it, and I hope that you're all there with me. So, have a great day, and I will talk to you all, I'm sure, throughout the day and throughout the breaks. And I'll turn it back to Pierre. Thank you.

Pierre: Thank you very much. [Applause] To talk about this conference, *Saving Our Spectrum: Handling Radio Layer Vulnerabilities in Wireless Systems*... Why this conference, why now? Radio services have always been important for more than 100 years, but they're rapidly becoming essential, something we cannot live without. The question of what it means to secure these wireless systems, to make sure that they're confidential, that the integrity is maintained, that they're always available when we need them is something that researchers, and academics, and industry has been working on for a long time. But we have the sense that it's something that policymakers have not been focusing on with as much attention as perhaps it merits, particularly at the radio layer. So, to address that, we've gathered together the community... This is a follow-on from a round table we had in Washington, DC in March, and there's a link to that if you go on the event webpage if you want to read more on that. We're going to focus on the radio layer of these wireless systems today. A couple of reasons for that... One is that, obviously, cybersecurity is an essential topic. It's an unavoidable topic, but there are lots of people

working on it, and there are lots of conferences about that. What makes radio special, unlike computers that are plugged into the wall through wires, for example, is that in order for them to work, they have to be open to the world, because if your radio can't hear anything, it doesn't operate. In addition to all the cybersecurity challenges that one has with the radio system, they don't have the refuge of hiding behind the wire or a fiber. And as Keith Gremban has said, "How do you secure something that everybody has access to?" That's the goal of this conversation, to help us begin to map out what some of the risks are and understand how we prioritize the scarce resources. I just want to ditto all the thanks that Amie expressed, but just a special thanks from Dale and me to Keith Gremban and Scott Fox — they're our unindicted co-organizers — for helping us trying to put all this stuff together. A couple of announcements, just for background... If we could just have the screen off, please. The first is, this event is being live-streamed, that is open to press. If you have a Twitter habit, the hashtag is #SiliconFlatirons. In order to facilitate as much conversation as possible, we've asked the moderators not to actually provide detailed introductions to their speakers. The speakers deserve detailed introductions, but you can read faster than the moderators can talk, so please, if you want to know more about somebody, just look it up in the program. For those of you who get overwhelmed by lots of conversations — and I'm one of those people — behind that wall, we have something called The Introverts Refuge. So, if you need to take a break, go out the back door and make two lefts. The rule there is no communications, no phone calls, no conversations, and if you can help it, no eye contact. It'll help introverts like me to just decompress. All right. So, let's get going with the program.

Opening keynote

Pierre: As we all know, there are millions of public servants in this country, and if you go to Washington DC, there are tens of thousands of people who work for the federal government. I know a few of them, and the people I know are dedicated, hard-working people. But if I had to hold up somebody who I know, from personal experience, truly serves the public, it would be Julius Knapp. Mr. Knapp is the chief of the Office of Engineering Technology at the FCC. I probably shouldn't say this, but I believe he's been at the FCC longer than I've been out of college. He rose through the ranks, he became chief of the OET in 2006. He served four confirmed FCC chairs of both parties. And every day that Julius remains in government and the siren song of working in the private sector for a lot more money, he's successfully resisted. And every day that he's in DC, working at the FCC, is a good day for all of us. Julius' patience and good humor are amazing. That's probably why he's been in the job for so long. Everybody who's worked with him knows Julius' self-deprecating laugh. It not only diffuses tension, but I've learned that when you hear Julius give that little laugh, that's when you really need to pay attention. But you don't only have to pay attention then, you always need to pay attention to Julius Knapp. So, with no further ado, Mr. Knapp.

Julius: Can I stay behind the curtain? [Laughter]

Pierre: The wizard of OET, ladies and gentlemen. [Applause]

[set-up conversation deleted]

Julius: Yeah, good. When we don't have our cell phones with us, we feel like we're missing an essential piece of equipment. I've mentioned this a few times before, but even wireless in socks... And I was wondering, what the heck do you want wireless in socks for? Although today would probably be a good day to try them. [Laughs] Because there are heated socks that you can actually control by Bluetooth. So, just about everything is going wireless. When you stop and think about our vehicles, and count up all the ways that they are connected. GPS... And then, there's the entertainment, satellite radio, AM and FM, your toll tag readers that we've had for a long time. Ultrasound, actually, you're using radio signals to vibrate the sensors. The connection of vehicle-to-vehicle and vehicle-to-infrastructure. The electronic controls, which maybe don't transmit, but also use radio frequencies. Tire pressure monitors that have been around for a while. Of course, commercial wireless, and Bluetooth, and Wi-Fi. I've said this before, they don't want to advertise how big the engine is any more or the styling, just whether it's got Wi-Fi and Bluetooth or LTE connected to it. I just thought this was a good example that we don't appreciate how much wireless is embedded in the things that we just do day-to-day. Then, 5G. 5G is going to greatly expand the use cases. Even with the list I have up here, it's not everything. Public safety, transportation, healthcare, education, energy, media, smart cities, agriculture, building and home automation, and others. Certainly, you're going to hear about a little bit later today about DoD's interest in the applications

there. So, more coming for connectivity. What are some of the technologies? This is a slide that really originated from our Technological Advisory Council. When you think about all the different ways things can be connected... Let's not forget about wired for a minute because wired plays a role, too. Certainly, cable systems is a great example. All these systems can tend to be hybrids, part wireless, part wired. We have the wireless personal area networks and sets of standards there. The local area networks, our home wireless routers, the wide area networks, all of the Gs, and so forth. There are lots of ways and lots of standards for ways you can connect things. Now, spectrum. I thought I'd throw in spectrum since it's in the title for the conference. [Laughs] On what we think of as the licensed side... Because we've been providing for flexibility in all of the commercial wireless bands for a long time. We're all familiar with the cell phones, but when you go to conferences, maybe you'll see it has been offered for years as M2M, machine-to-machine, before the term IoT really came into vogue. [Laughs] Those things have been around for a while. We've made spectrum available a whole bunch of bands. I won't go through all of the details of them. But more recently, 600 MHz band through a TV incentive auction. NTIA and the Department of Defense have turned on the initial commercial deployments of what I think is probably the most sophisticated dynamic spectrum-sharing system in the world for the citizens' broadband radio service at 3.5 GHz. We've opened up new licensed spectrum at 24, 28, 37, 39, and 47 GHz. I always feel like saying hike at the end of that. [Laughter] In one of those places at 37, we're working with DoD to find ways that we can implement even more advanced sharing. We've got two proceedings that are pending that are getting a lot of attention. One is what people refer to as C band. Because a lot of the world is looking at what's called mid-band spectrum for 5G, and roughly the 3.4 to 3.8 GHz range, give or minus a few gigahertz. [Laughs] Then, at 6 GHz — because unlicensed is also needing room to grow — is interested in sharing spectrum at 6 GHz with point-to-point microwave and a few other services. Then, on the unlicensed side, sometimes folks have the misunderstanding that there are just unlicensed bands. Well, these are bands that actually were provided for industrial scientific and medical equipment that generated large amounts of noise. You've got unlicensed working at 915, 2.4, there are a whole bunch of frequencies at 5 GHz. We've opened up more spectrum at 57 to 64 GHz. We've opened up spectrum roughly in the upper 70s, 76 to 81 GHz for vehicular radars and so forth. And we've actually opened up spectrum above 95 GHz for unlicensed use. The downside is, if you're looking about spectrum vulnerabilities, there are lots of bands to be thinking about. How many of you have read the report [Laughs] from the round table? All right. So, I'm just going to give you a high-level overview because I was very impressed. So, Silicon Flatirons, and partly what sparked why we're here today, [Laughs] had a round table to talk about this very topic. I've only clipped a part of the conclusion out of this because there were a lot of ideas... And we'll talk about them in a minute. So, I'm going to read this to you. The conclusion was, the round table discussion was only the starting point, more challenges were raised than solutions proposed. I think the solutions all come in the third panel today. Is that when...

Pierre: Yeah.

Julius: Yeah. [Laughs] The participants agreed that further discussions must take place to assess challenges and develop more detailed solutions on how to address them. There was consensus that a conference or another round table that brings together experts in government industry and academia is appropriate as a next step. I'm not going to cover all of the different kinds of vulnerabilities that were discussed in there, but I'll just highlight a few of them, and maybe share an idea, too. The workshop objectives for today — and, again, I just clipped — was to explore the risk of increasing reliance on wireless systems and access to spectrum and discuss ways to solve such problems, and also to focus on the radio link, then conventional cybersecurity issues. The challenge is created by radio receivers necessarily being open to incoming signals in order to function. I, as I was preparing for this, struggled myself to separate cyber because it's kind of a piece of it, but it's a whole subject unto itself. I think the intention here was to focus more on what happens with the radio portion, the new pathway into the devices that opens vulnerabilities. There were examples in the prep materials of spoofing presidential alerts, protecting GPS from spoofers, new security floor impacts in 5G, 4G, and 3G. At least 2G escaped. [Laughs] Most dangerous hacked medical devices and can Internet of the Body thwart cyberattacks on implanted medical devices. When you read these things, [Laughs] it certainly gets your attention. But I will tell you also that what these really signal at are lessons learned and things to think about going forward. One topic was interference, what do you do when your thing stops working, and you're not an engineer, [Laughs] you don't really know all about the spectrum and things. One of the challenges is we've got a lot more things out there that are relying on the airwaves. It's sometimes not appreciated because folks point to somebody else's product as generating noise, [Laughs] when indeed, every product generates some spurious noise and contributes to the soup. But it's a challenge with things that we have more of them, some of them are operating with extremely low signal levels below the noise floor. So, we continue to have that challenge. One of the issues is, how do you know if your product is not working as well, what's the cause? Is it interference, is it there's a little more noise, is it the loading on the network that you're not seeing as good a performance as you had seen at other times? We still have that challenge. The spectrum management, that it falls largely on the FCC and the NTIA, and on the NTIA side, working with all the federal agencies. It is not easy because we're always trying to put new things on the airwaves and allow for innovation for the new applications that you see coming out all the time. Which is a good thing. But for the incumbents, what they care about is it's not going to disrupt the services that they are doing and are important as well. One of the things they talked about is the challenge, "Well, how do you collect data on this stuff? How do you really understand what's going on?" And that's pretty hard. I think one of the things in the report was, things are somewhat lacking there for people to... But the questions become, "Well, what do you collect?" If you've got a phone and its throughput is reduced because of the noise levels, then how would you know, and who collects it? Because there are immediately privacy concerns when you start collecting this kind of data from folks. Then, reliability of the data. You'll often see people... One of the things I do with our engineers is... The data you're looking at, was it all collected the

same way, was it calibrated, do you really understand what it means, and then how do you interpret and analyze it? I don't know that there are easy answers there, but certainly, that was one of the things that was flagged in the round table. Then, identifying and mitigating causes of spectrum vulnerabilities. I think a great starting point is the system design and complexity. You have to build the protections against vulnerabilities into the design. You quietly see some of this with things that are out there and have been emerging over the years. For example, for some of the IoT things that go blip occasionally... Well, if there's a handshake, if the signal didn't get through, it goes blip again. Now, you got to balance that against... Well, what's your strategy? You don't want to do it maybe necessarily one right after the other, you don't want to keep doing it until the battery runs down, but it's one of the things that people do, recognizing that because they're using the airwaves, at times, there may be vulnerable interference and the signals might get through. There was some discussion in there about the advantages of what I'm loosely calling the dynamic capabilities. Most of these products that you've got — or at least on the commercial wireless side — they operate across multiple bands. There are probably more than a dozen different radio transmitters in your cell phone, whether you realize it or not. They are capable of operating in different modes that are stronger or lesser strong, making trade-offs for the signals getting through, and the network is going to manage it, that if you're not getting through one place, it may move it to another band. The robustness, as well as I think some of the features you're seeing implemented through software-defined radios, which have taken a long time coming but are better able to deal with some of these problems. Then, standard-setting. I think you see more and more now where the standards bodies are making a strong effort to build cyber into the standards. But how can you be sure that they got implemented the way they were intended? Maybe it's built into an industry certification process. But one of the things — and I'll talk about this at the end — is trying to anticipate every way somebody... Some 12-year-old who's up to no good [Laughs] has figured out a way to undo all your protections. The availability of harmful equipment. We have an equipment certification program at the FCC lab. I can tell you that we would not certify a piece of product that came in and said... I don't know why anybody would be so unintelligent to tell us, "Here's what I've got to spoof the president's emergency alert." [Laughs] The first line of defense is the products and just seeing if we have a public interest standard. And if we see something that is clearly out there to be put out for no good, it wouldn't get authorized. Then, there are enforcement actions that we can take. One of the things that makes it easier — having been a supporter of the enforcement for quite a while — used to be if you wanted to find out what was on the market that was illegal, you'd have to look through magazines and rely on complaints and stuff. It's pretty easy to find out now, it's right there on the internet, people selling it. But that's also the downside, people [Laughs] selling on the internet. They've got more avenues for distribution and volume, and it is a constant challenge. I'll also tell you just the process of enforcement... These aren't parking tickets, these are legal actions. Basically, our enforcement bureau has to first do the investigation, then prepare what's called a Notice of Apparent Liability or a Notice of Inquiry to build a case. So, jammers. Because there certainly has been concern about

things like GPS jammers and so forth. We really try to focus on them because it's safety-related, and go after them. But it is tough because of all the different ways people can find to get them out there. It's on our website, they're prohibited, so there's no question about those. So, some lessons learned from some past experiences... You can probably tell I've been at this for a while. [Laughs] And these are only a few of them. The garage door openers. And a lot of misinformation about what happened. In the early days, not everybody had a garage door opener, they didn't have to worry too much about... You hit the button, and your door went up. If you started to see everybody else's door on the block go up, you start thinking, "Maybe this isn't... Something's wrong here." [Laughs] Early on, what the industry did is put in something called dip switches. Basically, you would set the switches to a unique code for your garage door. It started to see some security, so to speak. Because a lot of people use their garage door openers to get into the house. But they were still — certainly, by today's standards — very basic. The protections have evolved over time. In this industry, I don't think I've heard a report about a door opener going up because of this sort of thing. They're using some pretty sophisticated codes now. But it's from the lessons of those early days. Cordless phones. I was directly involved with something, brand new products coming on in the market late-'70s or early-'80s. You'd pick up your phone, and not only could you listen to the neighbor, but maybe when they were dialing their phone, they were dialing yours too. [Laughs] They really didn't have any security codes whatsoever in them. There actually was a debate at the commission about whether having 64 different codes was enough. [Laughs] You can look at this and say, "This is going to happen." Sure enough, after two years, when we first started looking at the issue — people were careful, they didn't want to over-regulate — the phones were dialing 911. [Laughs] Because with the poor security, they would react to noise. So, the police, they were obliged to go out, and so it had to be fixed with more sophisticated algorithms. Wi-Fi. Wi-Fi was terrific. Came along, and probably in the early 2000s just started to hear about, "Well, wait a minute. Somebody's outside my house, tapping into my Wi-Fi system." [Laughs] And the industry has progressively built more and more security into these things. But don't get your device, not activate the security, and leave the password as *password* and the username as *admin*. [Laughs] When we started talking about what could a user do, there are things you can do yourself. But they started after this... Not always, but most people are using the security features on their routers now. Then, the first-generation cell phones. This was a fun story for me. [Laughs] It's a little bit telling if you can translate it into some of the challenges that we have today. The first-generation cell phones were analog. They actually used 30 kHz FM channels. [Laughs] You got assigned the channel you were on, but you could hear over [Inaudible 00:34:00]. So, Congress passed a law that said, "Radio scanners must not be able to tune the cellular bands." Through our equipment authorization program, every time somebody filed for — people thought it was a police scanner, a scanning radio because a lot of people liked to just listen to what was going on — the manufacturer would declare, "This device is not capable of picking up in the original 800 MHz cellular bands." This went on this way for maybe two, three years. All is good. All of a sudden, a high-profile political figure had a sensitive conversation eavesdropped and made public to the nation. The General

Counsel of the FCC — with me in the second seat — was testifying before Congress. [Laughs] And Tom Wheeler, who later became FCC chairman... Tom was the head of the Cellular Telecommunications and Information Administration, CTIA at the time. I still remember the demo that he did to start the conference. Congressman Billy Tauzin was the chair of the committee, and he came down, and Tom said, "Look at this," snip here, snip there, put a jumper there. [Laughs] And suddenly, you could pick up the cellular bands. What did we end up doing? We were brilliant. We said, "Okay, you got to put glue all over the chips so you can't get at the pins." [Laughs] Of course, the later generations were digital, and it's not that they're completely immune because there's always somebody out there. So, last slide, just some closing thoughts in the discussions today. Everybody has a piece of this, everybody plays a role. Government. And I use the term government because there are so many different agencies and departments that are involved in trying to deal with the cyber issues and the kinds of things we talk about today. It struck me... We were talking about the pacemakers, that they were hacked. The security is examined by FDA when they authorize them. [Laughs] So, even building in those protections with the government oversight didn't close every loophole that was out there. The network operators, the standards organizations, and trying to do everything they can to build security into the standards, the equipment designers, that they don't like the garage door opener folks think about this afterwards. Because then, it becomes a big problem and a very expensive problem to fix. And the application developers because sometimes that's the pathway into the hardware. We're going to always strive to eliminate the vulnerabilities but recognize that some vulnerabilities are probably inevitable. When you get in trouble is when you think that, "I'm good. I'm following the security standard. What could possibly happen?" [Laughs] It's a good thing, actually, I think, when you have groups or universities that are out there and announce publicly — or to the standards organization — that, "We found this hole," [Laughs] because then you can fix it before it becomes a problem, before it's out there and you've got a major problem on your hands. Then, prioritizing the attention to vulnerabilities is appropriate, particularly for safety applications. You try to tackle everything. It's probably less of a problem if my wireless thermostat didn't get through first try as opposed to GPS on a plane. [Laughs] Or things like that. Anyway, a few things to think about. I made it a little bit long, sorry about that. And should be a great day. Thank you. [Applause]

Pierre: Thank you very much, Julius. Julius is always willing to entertain questions. Since we're running a little bit late, what I would suggest is if you have any questions, please buttonhole Julius during one of the breaks, or not. [Laughter] The guy who's running down the hallway very fast is Julius. Thank you very much.

Panel 1 - Mobile Communications

Pierre: So, we're going to move on to the panel, the first panel. What I will do, I'll introduce the panel at this point. I'll ask the panelists to just come down, make themselves comfortable if you want. We're going to play two videos to start off with. So, if the panelists want to just sit in the front row, they can do that, too. The first panel that we're going to have is talking about the mobile communications industry. To give you a little bit of background... The topic of the conference, as you heard from Julius, is huge. We could have talked about any of a number of different industries. What we did was to pick two that, to some extent, bookend the problem. One is the mobile communications industry. This is a very mature industry, there are a few big players. It's something we all know about. It's actually a very deep and important infrastructure. It's very mature. So, that's this panel. The next panel will be Internet of Things, particularly in the healthcare area. That's relatively new and emerging. It's a very, very diverse industry, there are many players. There are lots of new and emerging problems there, and it's very different from cellular. So, we're going to talk about mobile communications first. What I want to flag to you is, we've had a lot of people drop out of the conference very recently as a result of health issues. One of the things I would suggest is work in the healthcare industry because we had two people drop off this panel, we had two people drop off the closing panel, but nobody dropped off the healthcare industry panel, so they're a very healthy crowd. [Laughter] We had two people that were going to speak for us on this first panel. Tom Sawanobori, who is the senior VP and CTO of CTIA, which is the Cellular Industry Trade Association. He was unable to travel due to a health issue in his family. He has actually very kindly sent us a short video. This goes against what we do at Flatirons because we like to have a conversation with people, but because we felt it was very important for everybody to hear that perspective...

Tom: I'm Tom Sawanobori, CTO of CTIA. I have over 25 years of experience with technology, network, and operations of wireless networks. The wireless industry is big security into our networks from the beginning, as we work diligently to proof security as we go from each generation to the next. Today's 4G LTE networks offer advanced security features, and 5G will be the most secure technology we have to date. 4G and 5G technologies have more sophisticated security than other technologies such as Wi-Fi and Bluetooth. While Wi-Fi is improving, it also depends on who manages the network, how well it's engineered and secured. Thanks to wireless, we're more connected than ever. There are more than 400 million wireless connections, joining people, devices, and the internet, and that's only going to grow. Tomorrow's 5G networks will offer very fast speeds, improve latency, and support massive IoT. This will enable entirely new services and applications from industrial IoT, transportation, healthcare, and public safety. Meanwhile, however, cyber threats continue to grow, both in number and sophistication from sophisticated hackers. While radio systems may be jammed or spoofed, that's relatively unlikely to occur, and more likely to occur in isolated areas. There are multiple spectrum bands being used also, which mitigates the risk of a spectrum vulnerability. Our entire wireless industry must continue to work and innovate

to advance security as we move to 5G and beyond. Our industry works collaboratively to understand improvements, leverage standards bodies, and drive standards improvements, and employ best practices. Every part of the ecosystem has a part to play, starting with a device. Device uses things like SIM cards, which provide one end of mutual authentication with the network. We also use temporary identifiers, roots of trust, coding, and encryption. In the operating system and app store, we also want to make sure we have antivirus and anti-malware. We also want to validate applications to ensure they're secure before they are downloaded to consumers' devices. On the network side, we use the other end of mutual authentication in the core network with sophisticated authentication keys. We use IPsec, and of course, robust access controls to make sure only the people who are accessing the network were authorized to do so. As networks become more virtualized, security must be more distributed. That will make for a more adaptable security environment. And of course, tools. Secure firewalls, VPNs, intrusion detection systems, these are, of course, table stakes. But if we move forward, things like artificial intelligence and machine learning are important tools to be able to find more sophisticated hacks. As we move towards 5G, networks are being deployed, and actual security capabilities will be enhanced. First of those is enhanced privacy protection. With encryption of devices, unique identifier, known as the IMSI will further secure communications and minimize the risk of eavesdropping. Secondly, the ability to leverage 5G home wireless security when you're roaming or when you're on a Wi-Fi network. This better protects the devices, consumer data, and even the network. And number three, we have device security-specific updates. This allows consumers to receive the specific technology updates meant for their device, whether they're on a smartphone, a tablet, or an IoT device, and provide native support for plug-in security. Of course, cybersecurity is a team sport. CTIA and its members collaborate across government, academia, and amongst each other. Chief among those is the Department of Homeland Security's National Risk Management Center, where the COMSEC [Phonetic 00:44:59] is headquartered in Arlington, Virginia. Here, we share information about the risks and vulnerabilities in the 7/24 operational environment. CTIA also collaborates with NIST, NTIA, and organizations like the FCC. We're currently talking to NIST about a 5G security project. In addition, with the FCC, we convene the CSRIC groups to work on involving security recommendations. Recently, we worked on things like SS7, the diameter protocol, and border gateway protocols to increase the security of networks. We're currently working on... The new groups are focused on both the transition from 4G to 5G as well as 5G security. In summary, for the US to continue to serve consumers and businesses and to provide innovations for vertical markets, our networks must be secure. And that's what our industry does tirelessly every day. Thank you.

Pierre: Thank you very much to Tom Sawanobori for that. The second short clip that I'd like to play you is from Jeff Reed. Jeff actually woke up with a medical condition, and his doctor said he wasn't allowed to fly. He sat down and actually recorded a presentation for us. The link to the presentation should be up on the event website. I strongly commend that to you. Jeff is one of the leaders in the US and internationally in wireless research.

He's a professor in the Department of Electrical and Computer Engineering at Virginia Tech. He's a founder of Wireless at Virginia Tech. He actually was one of the key players in the round table that Julius referred to. To get his perspective, could we have Jeffrey, please?

Jeff: In summary...

Pierre: Nope, we don't want to start with a summary. We want to start with that.

Jeff: Hi, my name is Jeff Reed. I'm a professor at Virginia Tech. Unfortunately, I wasn't able to be at today's conference due to illness, but I put together a few slides that I hope you will find to be informative. Hi, my name is Jeff Reed.

Pierre: And there we go, second slide.

Jeff: So, here are some of the key points that I'd like to make. First, attacks on 4G and 5G can occur at any layer, including the physical layer. These systems are extremely complex. The complex to analyze and enhance. It becomes pretty easy to overlook vulnerabilities that may be built into the system. And jamming is always a possibility. But you don't want to make it so easy that protocol or jamming can take the system out with very little power. There are certainly a number of reported hacks on 4 and 5G systems. A lot of them were reported at the Blackhat conference. That said, as we'll see, 3GPP, the standardization group for 5G, has really brought security to a new level of consciousness. They've done a lot of work in trying to root out potential vulnerabilities before these systems were ever deployed. In the way that 5G is put together through using such things as network slicing, you can develop your own authentication and customization of security. Nevertheless, we have to look at new ways to address security. These systems are so complex that we need to find, for instance, automated approaches to root out vulnerabilities. But there are some difficulties in doing research in this field, as I will explain. If you take a look at some of these pictures... I extracted these off the web. Here's an LTE jammer that you can buy on the internet. And here's an example of an IMSI-catcher. This is the ID catcher for a GSM phone. This is put together by a group at the National Research Nuclear University in the Russian Federation, and it consists of two RTL-SDR dongles. These things cost about $16 each, and they put them together to create an IMSI-catcher. So, you can see that this is not something that nation-states can do, but it is something that college students could do. In summary, there is a lot of great new security features in 5G, and more coming in release 16. We'll see further refinements in subsequent releases. There are still some known vulnerabilities in 5G, including some of those that have been identified for 4G. AI can have an important role in finding and mitigating these vulnerabilities. Finally, researching this area is important, but it's expensive and difficult to do. It's something that needs to be addressed by the research community.

Pierre: Very good. So, let's get into the conversation. Something fell off.

Staff member: It's on the ground.

Pierre: I'm dragging. I think you'd probably prefer not to hear me, but we'll see. All right. Do the soundcheck. Can everybody hear me? Can you hear me in the back? Yes. Thank you, Dan. Actually, the first thing I'm going to do is I'm going to break the rule of no introduction since we have somebody who has stepped in. Scott Fox has actually stepped up to join us on the panel. Scott is a veteran of the wireless industry. He's been in the industry 40 years. He's been in a whole range of positions as an executive. He was CTO and a senior leader at BellSouth. He's actually been very active in trade associations. He was chairman of the Global GSM Association. And also, he's worked in public-private partnerships. He was a lead advisor for FirstNet. Actually, both of the first two speakers, you heard talk a lot about 5G, which is the evolution of the cellular network, something which I imagine all of you have heard about. Something that not everybody may have heard about is FirstNet, which Scott has been very active in. Scott, do you want to say a little bit about FirstNet and what you think we should know about that?

Scott: Sure. Thank you. Thank you very much. It's nice to be here. It's nice to be at a conference in the town you live, it's really special. But at a high level — and I'll keep it very simple — FirstNet is a federal agency whose been tasked by Congress to develop, deploy, and operate the next-generation wireless network for our nation's first responders. Congress came up with this conclusion years ago, and wanted the first responders who have a number of kind of challenges with their existing systems to be able to take advantage of global economies of scale for devices, to be able to keep on the leading edge of technological development. Whereas, previously, they had used what's called kind of dedicated spectrum, largely proprietary solutions around what we refer to as LMR or land mobile radio. Again, FirstNet was largely created as a result of 9/11 and the realization that inter agencies... And I think there's something close to 50,000 public safety entities in the US. By public safety, I mean police, fire, emergency, medical, largely, and it can go beyond that. But FirstNet is the federal agency, was tasked with coming up with a plan. They were given $7 billion to do it. Not nearly enough. The conclusions were that they didn't have the time or money to build a dedicated nationwide network quickly enough, so they took the next best approach, which was to create a partnership with an existing wireless operator. In this case, AT&T was the one who bid and won that relationship. You'll see, FirstNet built... So, there's really two entities... AT&T — who we'll talk about — is delivering the services across the network. And FirstNet, the government agency who is really directing and overseeing their activities.

Pierre: What we have here is a public safety network, which is being delivered largely over the same network that we use as consumers. So, there are clearly upsides in this. Are there any downsides?

Scott: Well, sure. Ideally, it'd be great to have put a lot more money into it, built a network, which is "hardened", which means the towers are really hard to take down, the fiber connections are highly protected. So, to upgrade an existing network is quite challenging. But again, it's a reasonable compromise. It was a compromise to get out there quickly, to take advantage of existing assets that were out there. Not just physical assets at the network layer, but also the resources to build, design, evolve the network. It's going to take time to continue to harden the network. In this case, AT&T is investing lots and lots of money into it, funded by FirstNet largely. So, there are a lot of trade-offs. But at least the public safety has the advantage of having voice, data, and other super-fast connectivities right away.

Pierre: One of the things that comes to mind is that, in the past, public safety as infrastructure, and still a large part of it — Jay knows that very well, he can tell us more — was completely independent of the LTE cellular network.

Scott: Yes.

Pierre: When you're trying to secure a system, make sure that it's always available. You really don't like single points of failure. So, have we built ourselves a single point of failure?

Scott: We have... Virtually, it's a virtual single point of failure. On one hand, public safety is now in the process, and we hope faster than slower is moving on to FirstNet as FirstNet's capabilities continue to grow. This is very public, everybody knows this is where first responders are going to be. Previously, these land mobile radio networks were dispersed, they were hard to find, perhaps. But if there was an outage, it would be localized as well. So, this consolidation to a single network does raise the risk profile. But there are also ways to mitigate that and offset that as well.

Pierre: Right. So, we'll come back to some of those kinds of issues. I'd like to change gears. You would have heard... Actually, both Julius and Jeff talked about IMSI-catchers, also known in the traders as StingRays. We have one of the international experts on this here. Yomna's going to, hopefully, tell us what IMSI-catchers are and why we should care.

Yomna: Yeah. I have a bit of a cold. Can you hear me in the back? Because I can't project too much. So, IMSI-catchers — also known by the brand name StingRay — are devices that sort of mimic cell towers, and phones connect to them because phones are not great at that part of security. They have three main capabilities. You may have heard of... IMSI-catchers are StingRays in the news. So, a lot of people are confused about sort of what their capabilities are, but in general, there's three. This isn't perfectly accurate anymore, given some attack details that were published within the last year. But generally, they're capable of doing location tracking. So, either figuring out if a specific phone is either in a geographic area or absent from that geographic area or figuring out the exact GPS coordinates of a phone. In fact, the worst location tracking attacks are only possible in later versions of LTE. Then, there are communication interception attacks. This is what

you hear people worry about the most often. They think like, “Oh, someone will set up an IMSI-catcher and intercept my communications.” But as far as we know, those kinds of attacks have not been possible since GSM, which is used very infrequently these days, most of us are using LTE or 3G. Then, the final sort of class of attacks is signal jamming and protocol downgrade attacks. That’s sort of what IMSI-catchers are, in a nutshell.

Pierre: Could you say a little bit about what protocol downgrade attacks are because they show up in a number of different places, and I think most people won’t have heard that term before?

Yomna: Yeah. So, say you’re using LTE and you connect to an IMSI-catcher that’s pretending to be a cell tower. During the connection setup phase, the IMSI-catcher will be like, “Oh, I only support communicating over GSM,” and your phone will be like, “Okay, I guess I have to use GSM.” So, the protocol that ends up being used is GSM. That’s what downgrading means.

Pierre: Does that mean that if there is a 5G system, and I’ve got a 5G phone, and 5G has hardened itself against the kinds of things that IMSI-catchers can do, if the IMSI-catcher can do a protocol downgrade, I’m vulnerable again?

Yomna: Yes. I think a big part of deploying these big complex systems is you want backwards compatibility because you’ll have people coming to areas where there are 5G networks, they’ll have older phones, and you still want them to be able to connect. As part of that, that’s sort of where protocol downgrade attacks come into play. Yeah. Another thing I want to say sort of tangentially is a lot of the IMSI-catcher style attacks that we know of, the root cause is sort of what we refer to as pre-authentication messages. Phones cannot authenticate the towers they are communicating with during the very early parts of connection bootstrapping, during the setup phase when they’re picking what tower to connect to. That lack of authentication means... Sorry. That lack of authentication has not been fixed in 5G. A lot of the attacks we saw that IMSI-catchers were able to pull off in LTE and 3G, they’re still there in 5G, they haven’t been fixed.

Pierre: One of the things that I really commend to you is that... Yomna wrote a paper on IMSI-catchers for the rest of us to understand what they are in a lot of detail, in a way that I found very understandable, and I strongly commend it to you. One of the things that I picked up from that is, we, the public, don’t actually know what IMSI-catchers do, we only have what the researchers have been able to figure out because it’s commercially confidential. And there is a trade-off that I want to put to you, which is IMSI-catchers have an important social use. They’re used by law enforcement, they’re used by national security agencies. Is a community of researchers exposing how you can block them, the kinds of risks that you run through the existence of IMSI-catchers, are we giving the bad guys an advantage that they shouldn’t have?

Yomna: I think, in general, there is no way to block IMSI-catchers. I recently decided that it was too depressing to go around and keep giving academic talks on IMSI-catchers [Inaudible 01:02:06] [Laughter]. Because afterwards, in the Q&A session, everyone always asks repeatedly, "What can I do to protect myself?" I'm always like, "Nothing. There is nothing you can do." [Laughter] Of course, I believe law enforcement and people who are trying to hunt down criminals, whatever, should have ways to be able to catch those criminals or whatever. But should the way that they be able to do that be because our cell network security infrastructure is so broken absolutely anyone can take advantage of it? It doesn't seem like the best solution to me. I had something else to say, but I've forgotten.

Pierre: Well, we'll get into a conversation soon. And actually, both you and Scott have teed up some interesting questions about standards and the role that standards bodies can play in addressing these issues. We'll come back to that. But I want to turn to Jay. We had Scott talk about LTE as part of FirstNet. So, Jay, for those of you who don't know, is sort of the dean of interference hunters in the US. He does a lot of work looking for interference, trying to understand what interference is. Some of the things that we've been hearing about so far are malicious attacks or sniffing. How would you compare the risks of malicious attacks and just interference?

Jay: Sure, I can answer that question. First of all, my wife calls me the king of radio, not the dean of interference hunting. [Laughter]

Pierre: Okay, king.

Scott: She's not here.

Jay: I prefer king of radio. And my pronoun is your majesty.

Pierre: Yes. [Laughter]

Jay: So, we used to have an expression in the Air Force when I was an Air Force officer that of all the RF problems that we have that prevent us from using our radios, 90% of them, we were doing to ourselves. And that category is called interference. If it's jamming, it's intentional, if it's interference, it's unintentional. That's the definition that the military uses. And it was basically true. There's a lot of interference out there. The public doesn't see it, the public doesn't even understand what's going on behind the scenes, but our company spends a lot of time working with AT&T, tracking down interference so those cell sites will stay up and work. When you had coverage one day, you didn't have it next day, it could be due to a lot of things, but it could also be due to interference at that cell site that serves your neighborhood.

Pierre: One of the things that the Julius raised was... Your service stops working. Why is that? Are you able to help your clients understand what the root cause is, or is that often black magic?

Jay: Mostly black magic. It's actually not black magic, it's some tools, test equipment, computers try to track down interference, but mostly, it's experience. I'll give an example. 700 MHz cell phone use is relatively new, maybe the last 10 or 15 years. Before that, we did 800 MHz. Now, we do 800, and 700, and a bunch of other bands. But it turns out that there's a cordless phone that all the hotels use. They all use the same brand of cordless phone in their hotel rooms. And that cordless phone puts out what we call a spur. Spur is interference, it's only on one frequency, it has no bandwidth to it. It took us a while, but we figured out that that spur was almost always present, and if you put a cell site too close to a hotel that has those cordless phones, that spur is likely to be there. It's not there from every cordless phone of that make or model, but it's there for a lot of them. One case, I set one of my technicians out to track it down, and he very quickly located where it was. He even knew which hotel room it was. That was a combination of looking from outside and actually going up and down the halls and finding it. He went to the manager and he said, "We need to reset that phone." Because the solution is actually to turn it off and on, believe it or not, just like computers. The manager said, "There's a guest there, we can't ask the guest to leave." It's just a rule, you can't ask the guest to leave. So, he waited two more days, and then when the room was empty, we reset it. That's just one example. But the bigger problem is not the cordless phones, the big problem is the LED lights. Has anybody heard of LED lights causing radio interference? Okay, some people have. I'll give you an example. Every night, when I come home and it's dark out and I try to get in my garage with my garage door opener, it does not work. I have to actually get out of the car and hold it right up to the garage door to get it to work. Took me a while to figure it out. But my neighbor who's right across the alley has got LED lights on the outside of his garage, and he has them on all the time. That's one example. But a bigger example is Las Vegas. Las Vegas is all about LED lights. And every LED light bulb is not really a light bulb, it's an LED with a power supply. And the power supply is what causes the interference, specifically, switching regulator power supplies. When you put thousands of those up over The Strip in Las Vegas, you're asking for trouble for cell phone coverage. AT&T and Verizon have both asked us to track down those problems in Las Vegas. It's really difficult to fix though.

Pierre: I want to pick up on something. And by the way, this is just an open invitation to the panelists. You should feel free to ask each other questions, too. You mentioned that when there is a problem, it takes somebody to go out and figure out what it is.

Jay: Right.

Pierre: We heard Jeff Reed, actually... And again, you only saw three out of more than a dozen slides. There are a lot of great stuff in Jeff's deck, which I commend to you. He talked

about artificial intelligence in the deck. You said more about using AI and machine learning. Do you have a view on whether machine learning is going to help us? And actually, sort of a follow-on question for you, Yomna... There are apps that are supposedly going to help you know if there are IMSI-catchers. Are they any good? So, Jay, first you.

Jay: We hope so. We've done some work for one of our clients to test AI algorithms to identify, believe it or not, whether a truck driver is using his cell phone. But that same approach could be used to identify whether there's interference. You can imagine why trucking companies don't want their truck drivers using their phones and texting. It's dangerous, you're distracted. So, they take this very seriously, and they took it seriously enough to pay us to analyze whether that could be done. It's a difficult problem, though. It's a very difficult problem. So, right now, today, our company... We like to think that we're the leader in the US on tracking down this interference, but it's really pretty manual. We go out with a spectrum analyzer and a directional antenna, and we search around for the interference. Because when AT&T calls us, they don't know exactly where it's coming from, they just know that this sector is not working, and all the calls are dropping, and management is very upset.

Pierre: So, the robots are not coming for your job anytime soon?

Jay: Not yet. I had a professor that... I asked him why he was working on Bayesian analysis, and he said, "Because I won't be replaced by a robot." So, you have to find a job that a robot can't do. It's harder [Crosstalk 01:09:32].

Pierre: That's a challenge for all the folks sitting in the back of the room. Old guys like me, doesn't matter anymore. [Laughter] Yomna, to go back to IMSI-catchers... Are those apps any good that you can download?

Yomna: So, there are reportedly quite a few apps that you can use to detect IMSI-catchers. The general consensus from the security community and the research community is that most of these apps don't work very well, they're not trustworthy, there's a very high false-positive rate. So, a lot of these apps...

Pierre: What does false-positive mean?

Yomna: It just means like false alarm. The app will go off and be like, "IMSI-catcher nearby," but there won't actually be anything significant. That's just because, I think, the people who design these apps didn't know how much... There's constantly maintenance going on [Inaudible 01:10:20] works. Sometimes, the software on cell towers will reboot, and during the rebooting process, the tower will broadcast weird parameters. Then, the app will see that and will just freak out and be like, "Warning, warning." But also, speaking a bit more technically, a part of why it's hard to do accurate tower fingerprinting with software running on a phone is simply... The Android and iOS APIs don't give you low

enough level access to what's referred to as the baseband APIs. Sort of explaining this simply...

Pierre: What's an API?

Yomna: Oh, what's an API? It's sort of how you interact with other parts of software and hardware. It stands for application programming interface. So, you can't get enough information from the hardware parts of the phone. So, what's called the baseband. And that's sort of where you get information about the phone's radio stuff. It's hard to do that accurately, and a lot of people don't realize that.

Pierre: Let's jump all the way from the baseband to institutions. I want to circle back to talk a little bit about standards. And you have something about that, too, Yomna. But you've actually been the chair of an organization that was very closely involved with standard-setting, 3GPP, which is the industry organization for the cell industry has been working very hard on a series of standards. And if you want to know where we are on those standards for the topics we're talking about today, go and look at Jeff Reed's slide. What's your experience of standards?

Scott: A couple of things. First, just a minor correction. The GSM Association is largely driven by operators, and they come up with requirements. Then, the standards bodies convert those requirements into detailed technical specifications that are then broadly agreed, and then accepted and implemented. But generally, the standards-setting process is very complex, involves many diverse players, takes a lot of time. There are big original equipment manufacturers, there are intellectual property holders, there are operators, there are product companies, and it's largely a negotiated settlement, and often, it can be a compromise. It's a very, very complex process. The bottom line is that time is not your friend because these things take a long time, and many of these things are attempted to be done by consensus as it begins. It takes a long time, which is one of the problems with how we evolve things. There are so many voices, how do you pull in the right ones? The bottom line, though, just at a high level, as I see it, is the end result is typically not necessarily the best technical solution for the problem. It is one that is implementable and agreed by the parties. That's a bit of the bad news. I think, though, that the good news is that standards continue to evolve, and when they find a problem, they're able to come back and fix it again. But it can be a mind-numbing process, it takes a long time. Years ago, I was deeply involved in the process. And it's painful, it takes a lot of time. Largely, even a big company, for it to get its voice and its way, you really have to create a consortium of other people as well. And there are so many diverse voices now from the operators to the social media companies who play an incredibly loud and strong voice these days.

Pierre: One of the things, as I understand, that happens in these standards bodies is they are faced with a feature request or a problem that they have to solve. You have all these different stakeholders get together and, being engineers, they immediately agree...

Sorry, no. Being engineers, they will then all have solutions that they think are perfect. [Laughter] If there is enough time, you can get to consensus. If you don't get a consensus, there are options.

Scott: Yes.

Pierre: So, how do these options in standards affect what we can depend on them to do?

Scott: That's a great question and a great point. These options can be very valuable for those that want to implement them and those that know how to implement them. But one of the challenges with, for example, the 5G standard is there are so many aspects to it that — as Pierre has said — in order to get to a decision, they'll say, "Listen. This isn't a required portion of the specification, we'll call this an option, and we'll put it over here." And there are many, many, many, many options, but there are also many, many operators who will buy this version of the software, implement it, and might turn on certain options or not. But then, they have to interoperate with their neighbor, and for that matter, every operator around the world to be able to send traffic back and forth. With so many options, it's almost impossible to test them all, it would just take forever. There's been an attempt to reduce it way down, but it tends to swell back up again. But it leads to an interoperability problem, and in our case, it leads to additional vulnerabilities. With so many options and the lack of time to thoroughly test them all in great detail, by definition, they lead to some vulnerability opportunities.

Pierre: Yomna, you have worked with IETF, which is a different standard organization. How would you compare and contrast that with 3GPP?

Yomna: I've done some work with the IETF, which is short for the Internet Engineering Task Force. They're the organization that put together the standards for things like HTTP, HTTPS, TCP, things like that. I think the thing that strikes me the most about the difference between the IETF and the 3GPP is literally anyone can join an IETF mailing list and start contributing. They can send emails, they can propose changes to the SPEC. Generally, of course, it's encouraged first to sit and watch for a while and wait until you really understand what's going on. Otherwise, people won't take you seriously. But it's quite different with the 3GPP. If you want to be able to contribute, you need to be able to pay tens of thousands or even hundreds of thousands of dollars, depending on the size of your organization. Of course, that cost makes it quite prohibitive. So, advocacy organizations can't join, the independent security researchers can't join, university labs that can't afford that fee can't join. I think that, as a result, the set of groups participating in the 3GPP standardization process is not anywhere near as diverse as it can or could or should be. And recently, there were efforts by the IETF where they started a Human Rights Protocols working group. And what this group does is they work with other parts of the standard organization, and they evaluate the standards to be in all these various human rights abusing scenarios, like will these protocols hold up to

attacks by nation-states that we've seen. I think it would be really good if, years from now, the 3GPP could do something like that.

Pierre: Right. So, what you're saying is that there is actually an impact on the quality of the standards that are produced if the diversity of participants isn't so great.

Scott: It's very true. This is a fact, and it would be helpful. But even then, there's this problem of... When I was Chief Technology Officer at BellSouth, we had a lot of clout, we had a loud voice, but we could never get anything through unless we could create a consortium of other like-minded operators. Then, we would strong-arm our vendors to support it, as well, across the whole value chain. Then, it was still a struggle. Even when we were absolutely convinced that the solution was vastly technically superior, had no intellectual property wars to wage or gain or lose. So, there are a number of problems with the standard settings, it's an imperfect process. But there are a lot of people working around the clock to make it happen, it's a thankless role.

Pierre: Before we turn to Q&A — and just for the students in the back of the room, now is the time to start thinking about what your question is — I want to just turn to Jay. There's so much more, I just wish we had another hour. I want to jump from 5G standards to, in a way, the other end of the spectrum. You do a lot of work in public safety, you work with organizations, utilities that are using systems that are like pre-'90s or '90s era technologies...

Jay: They are.

Pierre: ...that don't have these kinds of things. What does that mean for the risk profile?

Jay: Well, I guess there are a couple of things going on there. One is that they're using old technology. So, if you think about public safety, and specifically, the public safety standard — which is P25, Project 25 — that is essentially 2G cellular technology, it's not too different from that. It's different in the sense that it's tailored for public safety, which means it's a one-to-many type of call as opposed to one-to-one type of call. And it also has the ability to be able to talk from subscriber radio to subscriber radio. Which cell phones don't do, they'd have to go through a base station, then come back. But other than that, it's basically 2G. Well, 2G is early-'90s. AT&T just turned off 2G several years ago, the GSM system, they don't even offer it anymore. You have to go to some remote parts of the world to use GSM phones. So, that limits what you can do because it's old technology. The biggest limitation is data rate, bandwidth. These are narrowband channels, you can't do what you can do with your cell phone. But there are other problems, and the other problems really are a consequence of economies of scale. With cell phones, you have these enormous economies of scale, so you can put what is very expensive technology to develop in a cell phone, and it will be cheap because you're going to sell millions and millions of them. Well, the vendors of public safety radios, there's only a handful of them... Motorola, Harris, Tait, Erickson, and Kenwood.

Those are basically the main ones. Those vendors don't have that advantage of economies of scale. So, they can't afford these large development costs because they'll never be able to get their money back. So, there are features in those radios that you would like to have that you can't have. Now, despite all that, believe it or not, P25 has a good encryption scheme, and it was approved by the federal government. And federal government users use P25 as well as police departments and fire departments. So, they've got the encryption down pretty well. But one of the problems you have is a police department buys a new radio system maybe every 10 or 15 years. Hard to believe, right? Because we replace our phones every two years, or maybe even sooner. But that's what they do because the capital costs are so high, that's all they can afford to do. And when they do that, they have to hire outside experts, and that's where we come in to help them. Because you can't have staff on your payroll that you only need every 15 years, it's just not going to work. So, you hire experts to come in and help you, and the experts then have to tell you all the things that you're doing wrong. For example, we had one police department in Colorado that wanted to buy a new P25 radios system. This was before FirstNet was available, so it was a few years ago. And the encryption cost extra. Specifically, the encryption for the GPS coordinates. So, we said, "Well, you really want the encryption." And the police chief said, "Well, it's too much money, I don't have any more money in my budget." I said, "Okay, chief. Let's say you've got a SWAT team surrounding this criminal domicile, and you're trying to be stealthy and sneak up on him, but the criminals are very sophisticated, and they got scanners in there, and they notice that all the cops are around their house. You don't want that to happen, obviously?" He said, "Okay, we'll buy the encryption." [Laughter]

Pierre: Wonderful.

Scott: But you had to go through it. And just to put it in perspective. In terms of numbers... Because we talk about the global economies of scale. But very, very quickly. In the US, there are 320 million people, and there are more cell phones than that. But depending on how you count it, there's close to maybe three to four million public safety. So, their use of proprietary networks and solutions, they paid a huge price for it because they could never get out of it. And thus, one of the huge justifications to move to the latest and greatest technology and get there, so they can actually take advantage and solve some of these problems.

Jay: I think almost everybody in public safety agrees that FirstNet is where they want to be. It's going to take them a few years to get there, but that's where they want to be because they want that modern technology. They have all kinds of apps that they can use on broadband devices, but they can't use today because they don't have broadband.

Pierre: Good. So, let's turn to questions. We have a custom at Silicon Flatirons that the first questions go to students. So, any students... Can you just raise your hands to see how many students we have? We have two here. So, could we just have the mic in this row?

And actually, let's just get both your questions. And actually, there's another question behind you. Let's just get all three of those questions out, and then let the panelists answer them since we're trying to catch up on time. Please, go ahead. Identify yourself.

Kennedy: My name is Kennedy Smith. I'm a student here at CU, I'm in the Tech Law Clinic. My question... I want to go back to the 3GPP just for a second. We were talking about kind of balancing different interests, and I was wondering what the opinions on the panel were about whether the 3GPP has been sufficiently prioritizing these known vulnerabilities over things like going to market and the other interests of the organization?

Pierre: Let's just get two more questions, and then we'll turn to the panelists.

Male student 1: [Inaudible 01:24:54].

Pierre: You [Inaudible 01:24:55], okay. So then, [Crosstalk 01:24:56].

Male student 2: I was one more. My name's [Inaudible 01:24:58], also in the Tech Clinic. Also interested to hear about kind of... It was discussed that the 3GPP standard-setting process was kind of an iterative process, and kind of understanding though that it's quite insular, I just was interested to hear about kind of the timeline for when a new vulnerability is discovered, how long it takes for the 3GPP to kind of address that vulnerability in a meaningful way.

Pierre: Great. Thank you. And another question. Lady in the white. You're good? Okay, fine. So, a couple of questions.

Scott: Let me respond to the first question, "Do you believe 3GPP is adequately focusing on these things?" I don't, and it's one of the reasons I'm here, because I believe that... With 5G, there's been a significant focus on super-fast, high-speed, ultra-low latency, and there are great reasons for that. Who doesn't want super-fast? Who doesn't want to be able to experience this low latency? How are we going to control autonomous vehicles going 60 miles an hour in opposite directions with no... You can't afford what's called jitter or delay. So, I don't believe the prayer has been there, but by definition, it's been at the expense of resiliency. But it's not that the sky is falling, there's been a ton of work that's gone into it. And I'm here speaking up now because I do think that there's more work to get done, and the priorities need to shift now. The products are rolling out into the marketplace, we have to be very prepared to deal with the problems we already know about and the ones that are about to really hit us in the face.

Yomna: I'd say I agree with Scott. Just as an anecdote... So, in the reading that was put out before for this event, one of the papers was on how easy it is for someone to send out a fraudulent presidential alert. That paper, I think, comes from the University of Colorado Boulder. There was a similar paper that came out of a group called Kist in Seoul, South

Korea, a very big mobile security research group where they described an even broader attack where the fake presidential SMS alerts is sort of a subtype of that attack. And they took it to the 3GPP, and they were like, "Look at this awful attack, it would be trivial to pull off in a sports stadium and freak everyone out, put this fake emergency alert." As of a few days ago, the 3GPP's response was basically like, "Yeah, we don't really think this is applicable to real-world scenarios." That's clearly not true, especially given... If you think about what happened in Hawaii. I think it was last year, in early 2018, when there was that mass fake emergency alert about the incoming missile. That really freaked people out.

Pierre: Very good. Any other questions? Let's see if we have... We have time for, let's say, three more questions. Let's just bundle them together. That lady, and then those two questions over there, please. Then, we'll have to wrap up.

Shannon: Hi. My name is Shannon, I'm a first-year TCP student in the engineering school. Does FirstNet... Is the purpose behind that to solve the problem of Verizon throttling fire departments in the midst of responding to terrible, terrible disasters? [Laughs]

Scott: Next question.

Pierre: Thank you, great question. Then, two more questions back there. The gentleman there in the teal shirt?

Grayson: Hi, I'm Grayson. I'm a 10th-grader in Longmont. I was wondering in kind of the ideal world, how would a standards organization kind of operate and develop these standards that are universally used?

Pierre: Great. Thank you.

Jay: Grayson, why aren't you in school? [Laughter]

Pierre: Very simple...

Jay: You'll learn more here.

Lex: Hi. I'm Lex. I'm a junior over at Silver Creek in Longmont. I was wondering, is there a natural way they can develop an app or a program to detect these IMSI-catchers and StingRays?

Pierre: Very good. So, go ahead. What problem was FirstNet solving?

Scott: The problem with Verizon deciding to throttle the police department during the disaster, in my opinion, is not something FirstNet is actually responsible for, from any official perspective. But you can believe that FirstNet was actively involved in

responding and putting leverage on so that this didn't happen again. It's not really FirstNet that's responsible for this, there are other agencies. But the public outcry, I think, was what really got them to change it pretty quickly.

Pierre: This is probably something you could write a dissertation on. By the way, the reason why we have this rule of students go first is that they always ask the best questions. [Laughter] So, how should a standards organization work in the ideal world? That's a dissertation right there.

Scott: Yeah.

Pierre: Any quick thoughts on ways in which we might be able to improve these standards organizations to do a better job at this problem?

Yomna: One thing that I think could make things better is if security researchers, public interest security researchers were included in the standards process much earlier on. The common problem, especially in software engineering, is developers will write all their code, and then they'll spend like eight months on it, and then the last two weeks, they'll be like, "Okay, security people, come in and look at it," and by then, it'll be too late to fix the structural problems. That's one thing. Also, more diverse stakeholders involved in the standardization process, which is definitely something that 3GPP could do.

Pierre: Right. And to the question on are there apps, there are. And I think you actually discussed them in your paper. So, go to the EFF website and look for the paper on IMSI-catchers that Yomna wrote.

Yomna: Yeah. It's called *Gotta Catch 'Em All*. It's a Pokémon reference, so it's easy to remember. [Laughter]

Pierre: Very good. Actually, I have had to shut down my friend and colleague here. He had another comment, but we are way out of time. I would like to thank this panel. We're going to go into a break. Could I ask you to try and be back here by 10:02 if you can? Just a word to the wise... The restroom's out the end of the long corridor. If there is a line, go up one floor, there's another matching restroom one floor up, and then another floor up. See you at 10:00. Thank you. [Applause]

Panel 2 - Health Care

Pierre: All right. Our next panel is about health care and we're very pleased and honored to have Liz Harding, partner and shareholder with Polsinelli, to moderate for us. Over to you.

Liz: Thank you. Well, I'm equally delighted to be joined by our panel here today. I'm going to do a really quick introduction of everybody. We've got Stephen Berger who is President of TEM Consulting, Phil Englert who is Global Leader of Healthcare Technology at Deloitte Advisory, Erin Kenneally, U.S. Department of Homeland Security. Erin is the Portfolio Manager of the Cyber Security Division-

Erin: Not the entire division. I won't take that credit. Three programs, the Data Privacy, Data Infrastructure and Cyber Risk Economic.

Liz: And then we have Shreyas Sen who is Assistant Professor in the School of Electronic Engineering and Computer Engineering at Purdue University.

Shreyas: It's EC, Electrical and Computer Engineering.

Liz: Wonderful. So, we're going to talk about health care and the implications following on from the discussions earlier this afternoon on the issue of health care. We're going to jump right in but just a couple of things to say first of all.

We talk about the Internet of things. I think in the health care field, we talk about the Internet of medical things, the IOMT. That can range from pacemakers to continuous glucose monitors to smart monitoring systems that are in swallowed form. So, there's no end of technology to discus.

But starting with my first question, I'm going to ask this to Stephen. So Stephen, what are the particular concerns you have with spectrum vulnerabilities, specific to the health care field and then what are the worst case scenarios? What are we not thinking of and what's keeping you up at night here?

Stephen: All right. Well, I want to keep it interesting [Inaudible 00:02:23] are we thinking enough and talking enough about our beliefs? And it goes into a number of areas. We all reflexively believe the past is the future and that what we will experience in the future is going to be a normal distribution of our experience but that's not necessary true. There are non-normal distributions. There are black swans, Fukushima happens, the 2000 election Bush v. Gore happens. Things happen with monumental impact.

So, when they happen you have to bring a group of people together from various aspects and various expertise and what I find in a number of these is it takes three to five years. And ultimately what's happening is you're coming to a shared belief system and a shared

value system and then you find solutions that work in multiple disciplines and multiple levels. That's too slow.

As one example of the past not being the future, if you look right now in the FDA Instant Database, the number of wireless interferences incidents being reported with medical devices is exploding exponentially going up. Patients are being injured, patients are dying but as you start looking in closer, what you'll find out is the reason this has been going on for about two and a half years, the reason it's going slowly is those who need to work together on the solution have different values and different belief systems.

And so, you've got to work all that through and it takes time. So, let me just leave it there but I can think of three quick incidents where we've had these problems. One of them was hearing aid compatibility, another was a problem with portable oxygen concentrators that caused a lot of problems in this current one and they all seem to take this kind of three to five years of a lot of thrashing before people effectively get working together so that's … I'm not sure we're always going to have that three to five years.

Liz: And that feels like a very … that's a reactive. That's the problem and then the fix, which I know is sort of human nature but I'm interested from others on the panel can we flip that? Can we look at vulnerabilities in advance or do we have the foresight to do that?

Erin: Before I answer that, can I tea a little bit on your first question? And I appreciate your response there. The thing that worries me with the medical device spectrum security is kind of two fold and there are two ends of the spectrum, no pun intended.

So, one is we're increasingly moving into the W-bands so, Wireless Body Area Network. So, think of the implantable device speaks to the wearable, speaks to the data center. And we're also living in this world, as we all know, with regards to social media, fake news, our ability to trust the information that we receive. Well, what about this scenario where we proliferate these W-bands and we've all got these little Wireless Body Area Networks around us that are connected to centralized servers and what if we can no long trust that information?

So, that's kind of a horror scenario to me in terms of information chaos. It's one thing to not trust in the news. It's another thing to not trust in the diagnoses that your physicians are providing based on the sensors and the actuators within your body. The opposite end of that that I think worries me is this notion of systemic risk and this comes up, I may touch upon later.

This comes up in the context of Internet infrastructure risk, which is to say it's certainly problematic to have vulnerabilities and threats to individual devices and absolutely if they affect life and limb, that's a huge problem. But when you talk about sort of the complete health care monitoring system, groups of W-bands together that fail, I think that's something that we need to be concerned about as we create.

And this is the case with IOT, with cloud computing. We create these efficiencies, all these efficiencies come with dependencies, those dependencies lead to systemic risk and then eventually cascading harms and I think we need to be concerned about that as we build out these medical systems.

Liz: Interesting.

Shreyas: Maybe I would like to add an anecdotal story to it to talk about the vulnerabilities. So, how many in the room knows about somebody by the name Barnaby Jack? Okay. People know about it. So, what keeps you up at night, I want to steal the story.

So, Barnaby Jack's work, he was a expert in cyber security in medical devices between 2011 and 2013, changed the threat that people think of. So, in McAfee FOCUS 11 in 2011, he showed with a insulin pump on his friend and another one on a desk that without any previous knowledge of the serial number of the pumps, he could hack into it with a high-gain RF antenna and can keep on proving amount of extreme levels up to the level that it is lethal. He then later showed that in 2012 at RSA Conference and also showed at attacks in 2012 on the pacemakers.

Unfortunately, before presenting his work at Black Hat in 2013, he himself was found dead to drug overdose in his hotel room. So, this is just a picture of him educating us what is possible and people are not thinking about in a very short amount of time because there are many people who know such things that can be exploited and may not come out and say it and exploit it at the right time. That keeps me up at night.

Phil: And that's a great example of purposeful exploit where somebody intentionally does that and this was what makes the news regularly, whether it's a implantable defibrillator, whether it's a infusion pump or regulating glucose in your body. But the other element that we have to deal with is the interference that happens because we have systems in hospitals that are not built and tested to go together.

So we have things like a noisy DC motor in a paper shredder interfering in leading artifacts on an ultrasound image. We have door closure systems that interfere with the [FD amount 00:09:50] monitors for infants and items like that. So, items that are not designed to be together, are not designed in the presence of each other can interfere and cause difficulties and challenges.

Liz: So, it's almost that develop of technologies in a silo with a broader thought process about the kind of wider ecosystem in which they're going to be operated.

Phil: Exactly. Exactly and these are systems of systems, one of challenges. We created this wealth of data that allows us to do amazing things in health care. We've got predictive analytics that instead of now where your physician will try this medicine to see whether

it puts you into recession for cancer, now they can look at your proteomics and your genomics and say no, medicine A is not going to work, we're going to put you on medicine B because we know you will respond to that and we know that you'll respond with less side effects.

And that kind of benefit that we get out of this interconnectedness and this building of these big, rich data sets is greatly beneficial but, I forget the gentleman that says it but another researcher, with great interoperability comes great responsibility. [Laughter]

Liz: So, how do we … well, why are we not doing a better job at identifying these vulnerabilities? What are the challenges to identifying these vulnerabilities and then what can we do about them in the short and long term, Shreyas?

Shreyas: Sure. My answer to your first question is kind of more philosophical. So, security is always like that, that a group of people are trying to secure a system they are building and then the whole world could break it with time in their hand after it has been deployed for next 10, 15 years.

So advanced technologies available for breaking later and the sound minds that are available out there that can hide and try to break it makes finding … what are we going to predict against? You've got only way to prevent things that you have thought through. What if there exists a vulnerability that you haven't thought through like you mentioned that because of systems of systems are coming together.

And hence, I think it is always going to be a very hard problem but the things that people have thought through, we need to be extremely prompt about taking countermeasures about those before we deploy. So, that's to the first question.

On the second one, what can we do about it? Our work, I would like to point out here and there are some other works also. So, first thing we can do is we should encrypt. There are still devices out there that are not encrypted that does not make sense in today's day and age.

But then you'd say okay, symmetric key encryption, the keys are there in the device. One might do something like a side channel attack where you get the key out and then even you can break encrypted systems. To that end, we should start adopting public key encryption kind of a framework where you have only a similar key that you are developing for some time as a certain key.

Now, those are harder to do for resource and energy constant devices like a pacemaker or which doesn't have that much battery because you are now trading off your battery lifetime of some N years to a shorter time. Today, there are better solutions for this subset of Internet of things which relates with the body. We and others are calling it the

Internet of body that exist a better solution by thinking ground up. Why are these hackable?

And as it was mentioned in today's primer that radio signals are very hard to protect because the signal has to be available to everybody. That's how we communicate. But the fundamental question we should ask that if I'm trying to communicate from my pacemaker to my watch, does the signal have to be available to everybody in the room here?

The way we do this communication today is electromagnetic waves where I'll put my signal on top of a electromagnetic wave radiated so that it goes through the airwaves, goes to my watch for example but also goes to everybody else and then it becomes the … because the physical signals are available, the mathematical encryptions can be broken with an intelligent hacker.

What we are trying to champion is thinking of the fact that you can use the body as a wear. You have all of these devices on your body itself and the body is conductive. So, if you use the body as a wear, you can connect all your wearables and implantables for your internal body using the body itself and then the signal doesn't go outside and anybody in the room cannot hack.

Your signals are private to yourself. We are calling it the electro-quasistatic human body communication because this is in the electro-quasistatic range just before the electromagnetic range when the signals radiate out. I don't want to take longer time but what I'm pointing out is for the subset of internal things that is inside the body that is relevant for health care. There exist a better physical layer solution, which I'm hoping [Inaudible 00:15:21] efforts will start that can make signals private.

Liz: Almost using your body as a network.

Shreyas: Yeah. Your body's your internal network or the wear for communication.

Liz: Interesting. Lot from that. [Laughter]

Phil: I can't go there but one of the things is medical devices were designed, purpose built, for clinical functionality and they really weren't designed to protect themselves. They really weren't designed to even analyze themselves.

It's an interesting phenomenon. I point this out to manufacturers quite often that I can turn on a medical device and if it doesn't pass its internal self-check, it won't operate but there's no protection to know that that self-check is actually run on verifiable code. So they haven't thought about that.

They don't data log. If we log security events and then we have the ability to use machine learning and AI to analyze this information and determine or identify things faster so that we can respond to them faster. That's one of the elements that I think is going to be very, very important.

So, we talk about how difficult it is because radio waves are out there and receivers are always open and it's difficult to know whether your signal got to the right place or not. But think about they talked about the exploit on the cellphone. If your phone downgraded its service and it recorded that log and then sent that to a central server then that could de-analyze and say wait a minute, 5G was available in that location.

That was a spoofing attack and we could begin to do that and then recognizing those patterns, we could then begin to build resilience and response and recovery into the devices themselves. That very same principle can be applied to medical devices as well, make sure that they fail in safe ways, make sure that they're resilient and they can recover fast.

Erin: I would just add, with regards to the wireless body area networks, think the vulnerability's very in scope based on what kind of tier you're talking about so, whether it's micro devices entirely within the body versus the in-body to the on-body devices like ICDs versus on-body to off-body wearables and then there's the entirely external, which is beyond the communication gateways.

But in general and as commented earlier, I think the major vulnerabilities with these devices is the limitations, the constraints, the power, memory, computational constraints really impede the ability to implement state of the art encryption frameworks. Key management becomes an issue as well.

And then you've got issues like securing a protocol where vendors are just not doing that. We know how to do that to a certain extent in certain cases but vendors lack incentives to do that. It's all about time to market. So, we get in the discussion about incentives and how do we better force their hands to make sure that security is built in, it's part of the design model of the devices.

And then lastly, solutions were past forward. So, yeah, I think building better batter capabilities for these devices, whether it be in-body or off-body is important, developing the equivalent of what we're used to in the network world, IDPS, Intrusion Detection systems for [hyper serial 01:28:00] attacks on these devices is important. Those are kind of the top of the mind approaches to deal with this.

Stephen: Yeah, there's another dynamic that I think makes a lot of sense but it worries me a lot and that is the developing of the application of a device. There's a lot of devices come on the market as … they're not medical devices. They're health and wellness device. I'm wearing one. It's my Fitbit. It tracks my steps.

The requirements that this got qualified to as a track your steps, help you do a better job at staying in shape, not that I'm doing a good job of that but is one thing. But if you go on, to use them as an example, on their website, you'll see they're exploring how this can be used in health care and they've got a Fitbit Care site and they're going in that direction.

Many examples of this where a device gets introduced as fairly benign and then people are creative and they find new applications and suddenly it's being used in very sense the medical application but it was never tested to the levels that we would expect things used that way to be tested. It was not deigned to that and I see that progression a lot. I'm not sure how we get our arms around it but it's an interesting view point.

Liz: We see it with the Apple watch.

Phil: You do and Apple watch is a great example where it tells time but it can do your ECG. And I was just at a conference. This was amazing. There was a physician on board, there was somebody, there was another passenger that was having a cardiac event and this physician took her watch off, they let her enable the Bluetooth on this so she could read it and she could determine that this was not an emergency. And so, the flight could continue onto its destination and not return to base and interrupt travel for 400 passengers.

So, this is the kind of advantages that these technology opportunities present. And on a one to one basis, they're such wonderful stories but when we talk about in mass, they can be very, very frightening.

Stephen: Think about the security. What security level was it originally designed to?

Phil: Right, right. Apple is interesting because the FDA is going through this change. How do we do this? The FDA's purpose is safety. They really weren't about security, they really weren't about confidentiality or privacy and they're beginning to see that these have impacts on the holistic health of people and so now, they're going through this evolution and they're building things.

And so, you not only have to build devices that are secure. You have to build devices for privacy as well and like not every squash is a pumpkin but every pumpkin is a squash is how privacy and security fit together. So, security supports privacy but there are elements of privacy that don't fit into security at all and that has to be really well understood to really get that we're building data systems.

I'm not building a watch anymore. I'm building an element, a device within a data system. And so, we have to begin to think about how do we do that, how do we build that, how do we make them resilient, how do we make them secure, how do we make them private, how do we make them so that they can recover quickly.

Liz: Now, what's interesting and to that point, I always come back to this issue with the wearable technology such as the Apple watch, et cetera and the information that that's gathering about your health. That's also to the privacy point. That's outside of the scope of PHI with [Hiper 00:23:25] because we don't have enough and as I look at this from, okay, what's the regulatory overview. You have this whole bucket of data that in a different circumstance, would be heavily regulated and protected and is really not, at this point in time.

Phil: So, health care has an interesting dichotomy. If I go to a hospital and I ask them for my MRI and they put it on a desk and they hand it to me, that's perfectly acceptable. If by mistake they hand it to you, that's a data breach. If they hand it to me and I hand it to you, that's perfectly acceptable even though the end state is exactly the same.

So, you're absolutely right. The policies need to accommodate the great variety of stakeholders that are involved and I think take modification into or be modified to account for that. If we think about accountable care, it was really about improving the outcomes. So, they said let's connect all of these things. So, what we had was unintended consequences of creating these super high value data sets.

Stephen: I have a friend that works in voting and election systems and he says this is a field where you think about how you're going to solve the problem for a week and then you think about all the problems you've created unintendedly for a month and I think we've got the same issues.

You do this and then you've got to start thinking about what are all the barriers you just created as you protected privacy where the data's not getting where it needs to and you're now impeding the health care because you've created barriers to flow of information and people on the medical team don't know what they need to know.

Phil: I agree. And it's interesting. Health care, really if you think about it, this is a risk management challenge and health care is nothing but risk management. It's what physicians do day in and day out. A patient presents, they analyze the symptoms, they look at the treatment options, they determine here's the treatment that in my opinion will produce the best outcome with the least side effects and that's the choice they make.

And this is what we have to do here. So, when we think about what is the function of the device as we're thinking about the design and implementation of it, what is the function and the ethics of whether we can't, whether we should even if we can but what's the function? Then we think about what can go wrong with that.

So, in a medical device, we can have a defibrillators that shocks at the wrong time or shocks repeatedly or doesn't shock at all. These are the things that go wrong. So then you look

at what are the mitigations. How can I prevent that? I can have code integrity, I can have data integrity, I can have alerting if my battery discharges to a point that it won't deliver the therapy that's expected and then I have to test those mitigations to determine whether they're effective.

It's risk management. It's a challenge because, as Stephen eluded to, we think about all the problems that can be out there and it seems endless but if we don't start somewhere, we won't get anywhere.

Erin: Yeah, and I would just add on the backs of all these comments that solution interventions for this type of collective risk because that's what we're talking about here is collective risk and in an environment where we've got a lot of information. Asymmetries is a lot of unknown knows and unknown unknowns and we've also got a marketplace where there's really not a great demand signal.

So, all those are combined to make this perfectly situated for pre-competitive RND tasking. I think we need a lot more thrown at these issues, at these unknown unknowns, collateral or unintended consequences on the backs of research and development. And I think there's some responsibility from a government perspective certainly to help bankroll that.

Liz: And that leads me to the next question.

Phil: A question too. [Laughter]

Liz: We talk about RND and how do we incentive this? Because as I see it, and I see it as an attorney advising clients that often the issues of security and privacy are kind of the after though in the products about to go to market and I get a call saying, Oh, well, we hadn't really thought about what are the privacy implications here. And by the way, it's going to market next week." So, how do we incentivize? Do we need a stick in terms of more regulation? Do we need a carrot in terms of funding? How do we do that?

Erin: So, I'll jump in on that real quick. So, if you think of kind of the major forcing functions on individuals and organizations, it really boils down to the law and the market place. And I think of the incentive structure and I think a lot comes back on governments of all shapes and sizes but you can think of law regulation, policy and the ensuing liability that comes there from.

That's definitely a stick and it definitely causes organizations to move and move quickly sometimes. Standard is another one. If people one to do the right things and they're motivated to, often time if there's not standards to galvanize around, that could be an impediment. So, it acts as an incentive as well.

You've got things, as I just mentioned, RND, testing and evaluation, pilots, test beds. All that kind of falls under the umbrella of precompetitive research and development and then you've got market place mechanisms. Insurance helps. And you've got things like procurement. So, I'll give you some concrete examples specific to this space. Let's see.

So, I might get to speak about one of the programs that I run and I might as well just briefly discuss it here. So, it's called Impact. Basically, I bankroll researches and developers to go out and find and curate and make freely available research for cyber security RND kind of it large across industry, government and academia.

And so, what we're doing there is we're creating medical device repository of data, risk profiles for devices. We also deal with a whole swaff of other cybercrime and cyber defenses and whatnot. People come to me and they say well, why should the government be funding this?

We're living in this big data world. Data's falling from trees, why do we have to fund this? Well, it might fall from trees but it's still going to be picked and sorted and trucked and filtered and bottled and that is not cost free. Someone's got to pay for that and unless you've done research and you've tried to roll your own data, you realize the pain points there. It doesn't come ready to perform research to develop and test and evaluate these technologies.

I'll leave it at that. I think there's some other aspects to that as well but again, the examples real quick. [DARPA's 00:31:30] got a spectrum collaboration challenge going on right now where they're basically paying two million dollars to the winning team to use AI and software to find a radio to help automatically and dynamically manage spectrum. DARPA also has a nice test bed for spectrum security. I think it's called Coliseum. So, there's things like that that I think can go far in incentivizing addressing these issues.

Stephen: Pick up on one point there. Something I find happens over and over again when you get into these risk discussions. A fundamental issue of risk is what's the probability of a current and when you get the potential consequences of an event and the probability to the place where the risk is acceptable, you move forward.

The consequences are generally agreed on but probability of a current is really tough and especially in wireless. And I think that's the place where the kind of research you talked about can be enormously helpful if a high value, highly trusted organization would say here's what's really going on in spectrum and then whatever we're worried about, here's how you can really look at the probability that this will happen. I find a lot of times that's where things get narly.

Erin: And I thin incentives to improve upon spectrum security greatly … to invest in spectrum security, I think they greatly improve when you've got risk measurements and modeling

capabilities. It goes back to the old adage. You can't manage what you don't measure and it's a warned trope at this point in time but it became a trope for some reason.

There's some truth behind it. And we just don't do a good job of measuring and modeling the risk in this space. Certainty we don't do a good job in the traditional Internet infrastructure space and this is even newer.

Shreyas: I'd like to add something to that. The question is who cares about security and who is paying for it. If you as a random person, they'll say yes, I care about security. Are they willing to pay for it? No, I expect it to be for free rolled into.

For the connected cares and health care, maybe it's a little bit better that okay, I might die so I'll pay a little bit for security but for the general ILP infrastructure people are not willing to pay for security, that extra amount. Now, you have to go and think about the dollar value chain where the valuable devices are often the end notes and the companies making those are making the least amount of profit because from one note, you don't generate as much value as what you do from the aggregated data.

Aggregation companies like the Facebooks and the Googles of the world are getting the value out of all of these devices but because these device makers don't have that much margin and they are under the pressure, they don't have the opportunity to test out everything.

So, I think going back to what she said and also the philosophical nature of this problem, I think there are two possible solutions, that A, we have to hold the moneymakers accountable even though they are not making the devices and not making the vulnerabilities. Eventually, they are making money from these devices where the vulnerability exists.

So, to fix the vulnerability upfront, they have to put in the thought process and in many cases, all of these companies are doing that but more focusing kind of what can go wrong. The modeling framework has to be developed so that you can guess most of your problems ahead and then whatever is known, we have to be prompt about adopting those solutions. So combine these two, you'll reduce the risk space significantly but I don't think it will ever be zero, given the nature of the problem.

Phil: And I agree with everything that was just said by all three of my colleagues here. The only thing I would add is that this is not just a problem of will. It's a problem of bandwidth. Right now in the US, there's over three hundred and thirty thousand open cyber security positions in IT.

And so, we've got to develop the human talent to even have the hope of having the capacity, the resources necessary to develop, deliver and support these into the future. Because even though we can build secure devices, the world is constantly changing and we will constantly have to apply resources to adapt to it.

Liz: Do you think, as a panel and I'm going to throw this in here that the consumer of these devices, the patient or the user has an understanding of the risks and do you think that there is an ethical obligation to raise that awareness and with that drive addressing these vulnerabilities? Or do you think it's a similar thing to … not to berate Facebook but we're privacy folks, we all berate Facebook for their privacy practices and yet, how many of us still use Facebook.

Erin: So, the notion of ethics as a forcing function, I'm a huge believer and I've done a bunch of work on that in the context of ICT research. So, anyone hear of the Menlo Report in the room? At least one person. Dan, you should know this.

I'm an attorney and people disagree with me but I think that we start with ethics. What can we all kind of … look, we all know that we have different laws. We're never going to have unified laws across the country, across this city, across the world but we ask ourselves, from a bottom line perspective upon what can we all galvanize and agree is right and wrong.

And that's ethics to me. And if our laws are done correctly and codified correctly, they should be a codification of our ethical beliefs. Does it always happen like that? Absolutely not. So, I'm of that mindset. We're hearing a lot more about ethics above the fold in mainstream media. I think it's a great thing.

It's still treated somewhat shallowly because people can't really define it or wrap their arms around it. It's a tough nut to crack. But you've got companies now talking about it, creating review boards and what not. I think that's great. I think we need to move on that as well, especially in the context of artificial intelligence and autonomous systems. What I worry about is that ethics is being used as a foil to maintain control structures. I think we have to be very wearing of that as we move forward.

Stephen: Yeah. There's a dynamic that fits in there and I think we have to be honest to it. It's often much more effective and cheaper to advertise and market that you have a solution as opposed to actually developing a solution. In the area of disability access, there was a major company, I won't name the name, but under a lot of pressure from one particular attorney general.

They formed a whole department to do a better job of dealing with making their products accessible to people with disabilities. They put seven people in that department, one software engineer and six PR people. [Laughter] I hear that happen in security a lot.

I do certifications in certain areas answer every company that comes in tells me they got world class security. And I know enough to be dangerous and it's laughable but boy, they're confident and they've got all the buzz words. So I think that's a dynamic. That comes back to the ethics of it. We've got to figure out how to do the hype more effectively.

Erin: But Liz, this was the case with privacy years ago, right? It was a hand wave until things like GDPR and CCPA come down to bite where there's real monetary stakes and then companies sat up and said oh yeah, maybe we really should, instead of darting eyes and crossing teas on privacy, actually implement what these controls are calling for.

Liz: Yeah. I think that's right.

Phil: Right, right. [Laughs] The classic example in health care was Hiper. Hiper came out and it was supposed to protect privacy and 10 years later, the came out with high tech. So, they put teeth in the laws to get people to actually do something about it.

It was interesting and just a quick anecdote. Back in 1989, we talk about the spectrum. An HDTV station fired up in Dallas, Texas and took out the telemetry system at Baylor Medical Center and it took them forever to figure out even what was going on and how that happened and how this could be allowed to happen. But the telemetry system was utilizing a space that had been allocated to television and the whole industry had done it. The amazing thing is it took them to 2002 to come up with WTMS, the protected medical telemetry bandwidth. So, it takes a long time to turn the ship sometimes.

Liz: Change is slow in coming. I'm conscious of time and so, I do what to open up questions to the floor and open it up to student questions to start off with. Yeah, they got burning thoughts.

Presenter: Blake will actually point somebody out. Then I'll be the one here. [Laughter]

Audience: Hi. I was just wondering if you could talk a little bit about the way that you see the role of different government regulatory agencies in addressing some of the concerns you brought up and do you have any … I know you were just talking about an example but specific examples of things that they have been doing that might have been somewhat effective or if they haven't been doing anything effective in addressing the concerns that you've brought up.

Erin: So, I'll point out that the way the government traditionally works is we've got swim lanes and swim lanes are usually assigned by issue topical areas. This IOT spectrum is really challenged that notion and so, I think it's also a reason why some things haven't progressed as fast as they should have because folks aren't sure who own it.

There's been a lot more work in developing more contortion based cross functional efforts within the government, which I think is the right thing to do in this regard. Can I speak to … I know there's a bunch on the supply chain, I think, which is an issue that runs across critical infrastructure risk and I think it's somewhat tangential to spectrum.

There's a group, bought a DHS that's working in that. Certainly 5G is a hot topic in that regard as well. I forget was there a second part of that question. One thing I also wanted to comment on, I know you asked the question about the government and it just occurred to me … sorry about this but I didn't answer this earlier with the question of incentives because really, you're getting it. What can we to drive this forward?

And I did mention this notion of procurement and the government is probably the biggest procure of technologies, certainly can wield and does wield that power. I know they're doing it in the IOT space to not procure secure devices, for instance. On the private sector side, there's something similar so I'll give you a specific with regards to medical devices.

So, there's things called GPOs, group purchasing organizations and they're member driven, health care risk management organizations. And there's one of my performers that I fund is Mass General Hospital and they're part of one GPO that represents a hundred billion in annual purchasing power. That's huge.

And so, what they're doing is, with regards to the safety of medical devices, they're saying look, if you don't pass certain criteria, we're just flat out not going to buy your devices. So, that's a huge forcing function. I think it's a great model to look to as well.

Phil: So, if I could jump in on this because there has been a lot of activity and it's beginning to gain inertia in its effectiveness there. In 2014, the FDA came out with what's called premarket guidance and said hey manufacturer community, cyber security is a real issue. You need to start addressing it.

And in that, they set out some very basic guidelines, the risk management guidelines that I posted earlier, some of the basic controls. They actually looked at tiering medical devices. Medical devices are classed from a safety perspective class one, two and three, one meaning that it's not really going to harm anybody. It might be inconvenient, might do minor harm. Two can cause some damage, physiological damage and three can cause catastrophic physical harm.

And so, they looked at tiering the medical devices and those that could cause harm and those that couldn't. And with the tier one devices, the higher risk devices, they said here's thirty seven controls that we would like to see in here and if you don't have them, there's no exception. And because if you think about the spectrum of medical device technology, it's so vast and there's not one set of controls that's going to apply to everything. You cannot do that ubiquitously.

So, in the 2018 revision of that, they said here's some headers that we want. We want to see authentication. We want to see authorization. We want to see encryption. We want to see devices that cannot do multiple harm so we want them to fail in a safe way. We

want them to be recoverable. We want them to be auditable for security events, meaning if I patch a device, the device should know that it was patched.

It should be able to tell you what's in it, what's the C-bomb or what's the cyber security bill of materials. What is this device composed of so that when the CBEs come out, the common vulnerability exposures. When that comes out, I can say oh, this Adobe product is in my medical device and I need to be able to manage that and respond to it.

So, they're doing a lot of really good things. Another effort that they have and the government looks at this as a public, private solution and manufacturing included but they formed the health care coordinating council that is looking at all of these, supply chain involved. So, I'm working on the supply chain thing that says here's how you can purchase devices and change contract language and evaluate vendors for whether they're secure.

They're saying here's the common vulnerabilities that we find in health care and here's what health care systems can do about that. And they're telling manufacturers here's how to look at risks in medical devices and here's the kind of protections you should have, two of the mitigations to apply to those risks and vulnerabilities.

So, the Health Care Coordinating Council has about 17 different channels. One of them is future gazing. Let's look at where technology is going and let's plan ahead and see if we can't get ahead of the curve on that. So again, I think we took a long time to get the ball rolling with the mosses falling off the rock and it's beginning to pick up speed.

Stephen: There's one other thought I'd like to throw out on that and at the end of the day, there are no organizations, there's just people. I think I first met Dale Hatfield on the Hearing Aid Compatibility issue and when people can find a way to work together effectively, magic happens and if they can't, it's painful and typically, nothing good happens. So, I wish I had heard this much earlier. I spend a lot of time working on how to build relationships and just go get to know people and your organizations will follow.

Erin: Let's hope.

Liz: I think if we've got time for one more question. Okay. A couple more.

Audience: Thanks. It's Richard Bennett, one of the people that created Wi-Fi. Good overview of the issues with IOT security, Internet security and everything but I didn't really hear anything that was specific to the radio layer in health care devices except for the body conductivity issue. So, could you kind of deliver on the promise of the panel and tell us about a vulnerability that is unique to the radio layer that affects health care?

Shreyas: I can start with that. So, till date, there are many devices out there, both pacemakers and insulin pumps which use unencrypted radio communication, which means anybody around can snoop onto the data. If they know the serial number of the devices, it's very

easy to attack but as I referred to the Barnaby attack, even without knowing the serial number of the devices, you can still attack because you can listen to all of this.

So, the radio layer is extremely vulnerable today for those devices which are unencrypted. And going forward, many devices has already, like he mentioned, have already embraced that authentic encryption, authentic essence should be there. It should be expedited so that no device should exist and this year, department of homeland security and FDA issued a couple of recalls at least on those pacemakers and insulin pumps so that many devices were recalled.

I think those activities has to be done significantly because these devices have 10 years of lifetime so, if we don't recall these and in the age where the exploits are very easily deployed, this is a very vulnerable system. Now with that in going forward, I would like everybody in the room and in the online audience to think why do I need the radio layer to communicate from one location to another on the body when the body exists as the medium? So, in the long term, I would encourage people to think of the problem differently where exists. Why communicated wirelessly and send my information to some other people around? Stop here.

Stephen: I'll throw one other comment on that. Over and over again when we find vulnerabilities with medical equipment, the built in security of the protocol is turned off or in properly implemented. So, we see this so often. It's not that the protocol can't be made secure. It was poorly implemented. That's probably the easiest way, these 20% to guess 80% of the benefit on this. Then there's some difficult problems down in the 20%.

Erin: I got a quick question to your solution, which I think that makes sense. We need to move in that direction. What's the threat model in that situation, feeding people the wrong medication so that basically, you send an infiltrator into the body to disrupt or intercept their inner lobe and they can-

Shreyas: Yeah, that's a great question. What is the threat model if somebody hacks into my last network? Imagine it's the insulin pump. They can keep on delivering higher and higher level of insulin dosage and up to a lethal limit.

Erin: No, no, no. I mean in your communications scenario solution, I should say, not the current thing. I understand that the-

Shreyas: In there, what is the treat model? The threat model is your signals only stay within your body. It doesn't go more than one centimeter off of your body.

Erin: How is that attacked?

Shreyas: The only way you can attack it is by physically touching somebody. You cannot, attack sitting there, my network. So, I have my own private network.

Phil: Now I-

Pierre: Good. [Laughter] Actually, we've managed to end on an up note. It sounded like we were going to end on a down note. So, please join me in thanking Liz and the rest of the panel for a great discussion. We will reconvene at the top of the hour for the closing panel and that will be directly followed by the keynote.

Panel 3 - Solutions and Next Steps

Keith: Last panel here. I'll introduce briefly some of the panelists, but we have a guest here substituting. First of all, on my far left here is Clete Johnson. He's a partner in the Wilkinson Barker Knauer Law Firm and works with clients at the intersection of technology and security. You can read more about him in the book. And then, Monisha Ghosh who is going to play two roles here. She's a research professor of molecular engineering at University of Chicago but also an NSF Program Manager where she manages a portfolio of wireless networking programs. Our special guest star here is Rebecca Dorch.

We had a cancellation this morning due to a medical issue and Rebecca was able to step in. Rebecca is currently a Senior Spectrum Policy Analyst at the Institute for Telecommunication Sciences which is part of the government labs right across Broadway from us. Her focus is on spectrum sharing. She recently managed the conformance testing program for the spectrum access system and environmental sensing capability of the components of the 3.5 gigahertz citizen's broadband radio service. In 2018 she was the Vice-Chair of the International Symposium on Advanced Radio Technologies and prior to joining NTA in 2016, I hired her by the way, Rebecca served for 13 years as the Western Region Director of the FCC's Enforcement Bureau where she oversaw the resolution of harmful interference effects on communications. With that, let's start off talking about things.

So we're kind of batting clean up tonight trying to summarize everything that's gone before and hopefully let everybody leave with a sense of hope, not a sense of pessimism. Let me start off with Clete and just start off with, what's the view from DC on these issues? Are the right agencies paying attention?

Clete: That's the question of the era in some ways. Not to jump ahead but I really look forward to hearing what Dr. Porter has to say about this from the DOD perspective. What I'll do to start off, Keith, is just say, first of all to admit I am not an engineer. I'm a lawyer and policy maker and I have spent my most of my career in the national security arena, the US Army, Senate Intelligence Committee and so I'm sort of an interloper in this communications world with a couple of stints at the FCC and the Department of Commerce. What I will say, just to level set here and talk about why are we even talking about spectrum vulnerabilities and saving our spectrum. Something I like to do in a discussion like this is just to make this abstract cyber threat concrete. It just seems like this nameless, faceless abstraction.

But what we might do is think about it in terms of concrete adversaries. In tier one intelligence services; China, Russia, North Korea, Iran in particular and then a whole host of other non-state criminal groups or proxy's that work with and for those intelligence services. We're really talking about tens of thousands of people who, like all of us here today, here in the audience, go to school, go to work, they provide for their families, they find

fulfillment in their daily life by trying to figure out how to get into our networks and devices. This is what they do. It's their job. So it's not some abstraction. It's a concrete set of forces that are out there working on this every day and I think that one of the reasons that the defense and national security establishment has, in recent years and with a really steep curve toward urgency, has awoken to the concerns in the 5G world in particular is that the more that everything is connected, the more you cannot secure your battle space, to put it in defense terms, through geography or through a perimeter. If everything is connected, then everything is vulnerable.

That's quite a cliché and sort of...it simplifies things too much. But that's the...moving from a wired environment to a mobile environment in the 2G, 3G, 4G world to a 5G environment where everything is connected and every sector is part of this connected environment and there are no...there's no government agency that can focus in on the health...we were just talking about the healthcare sector. That the FDA can't secure the entire environment or NTSA can't secure the entire environment even if it's got jurisdiction over connected cars and on and on down the list. We need multi-disciplinary interagency and also public/private government and industry because if everything is connected then all of the solutions need to be connected.

A short answer to your question, Keith, is are the right agencies looking at it? In some ways, the problem is everybody's looking at it. In some ways it's like the three-year-old soccer match where 5G is the ball and everybody's running to it. The good news is that things are starting to become much more coordinated with key domestic agencies; DHS, the Department of Commerce both NTIA and NIST and FCC backed up internationally and, in the defense, and international realm by DOD and the State Department. Of course, DOJ and FBI have a very significant role to play. And then, in each of those sector regulatory agencies and sector specific agencies, there are a number of players looking at these issues, as well. We at least have a chance to have the right team on the field. It's still early pre-season.

And the bad news is for the bad guys, they're well into the playoffs. So we've got a lot of work to do but at least the right team is coming together and I think the next frontier is really fully cohering that federal interagency team, linking it up to their counterparts in other allied governments and then the final frontier will be getting all the disparate actors in the private sector of whom nobody is in charge at large, to be part of the solution set. It's going to take a holistic effort in the same way that the connected world is a self-holistic and multidisciplinary.

Keith: Sure, would you like to jump in on that?

Monisha: You left out our agency, the National Science Foundation.

Clete: It's been a huge part of it, right.

Monisha: This is what I put on my NSF package. Absolutely. I think [inaudible 00:07:28] coordinates the wireless spectrum R&D group which is interagency working group that we meet every often...every month or so and then we have an annual meeting where we exchange what's going on. So from the NSF perspective what we are very interested in finding out is what are the real problems on the ground that the other agencies are seeing, the DOJ's and the Department of Commerce. But the FCC and NTIA, we have a better connection as to what is going on and what are the issues that we should be focusing on. And when I say we, I mean the entire academic community of researchers that we fund. Which is a huge resource which sometimes I feel is under utilized in the sense that there is very exciting research which is going on.

A lot of the news items that you see of threats being discovered or solutions being proposed are coming from the academic community. And I think we need to get that community much better connected to both industry as well as the federal agencies so that all of their [inaudible 00:08:36] will be able to play in this environment.

Keith: Thank you. Did you have anything to add on that?

Rebecca: [Inaudible 00:08:42].

[Laughter]

Clete: She's already playing her role.

Keith: So Monisha, can you riff on that a little bit more? I mean, what kind of programs are there? Are they funded adequately or, you know...

Monisha: Well, funding is never adequate, right? I read a letter to the editor once coming from an NSF Program Manager saying NSF stands for not sufficient funds.

[Laughter]

Monisha: So, yes. We could do more. We could always do better and if there's anybody here who has clout with Congress, yes, please. We are well funded in the sense that we think we do a pretty good job of funding the best research that's out there. We get very high-quality proposals. We have special programs surrounding security. We have a huge program called SATC, Secure and Trusted Communities, which is across departments including the behavioral and human sciences because security, as a number of you have alluded to, includes the human in the loop. So at the end of the day, even with things like two factor authorization and all of the other techniques that have come out, you need the human in the loop to be aware of why they need to be secure and to take some actions to make whatever applications they're working on more secure. Within the wireless group, again, we have a number of programs that deal with it.

There was mention made in the past...one of the past panels about testing and that is definitely a big hole. Security holes can only be discovered by finding them in practice. It's very hard given the complexity of systems today to analytically figure out that, yes, this is a security hole. And there aren't any adequate testing facilities. 5G is going to roll out as a production system. It's not being experimented with at the scale at which it's going to roll out. And so, yeah, when it rolls out is when you're going to find the holes that are buried deep in all the layers of the specifications. So we are trying to put money behind building experimental platforms. NSF has a program called Platforms for Advanced Wireless Research.

This is a public/private partnership of about 30 companies and universities which is setting up open test pads that will allow researchers from academia, industry and federal agencies to perform experiments, to break systems, so you deploy a system and you break it and you find out what the solutions are. Somebody mentioned the DARPA Colosseum. So after the big finale in a couple of weeks in Los Angeles, NSF is actually going to take custody of the piece of hardware and software that was built, the Colosseum and that's going to be stationed in Northeastern University and we're going to open up that platform to the research community for spectrum co-existence, spectrum sharing, security. That's a really, really powerful platform that can be put to use for many research problems.

Keith: All right. Anybody else want to add anything to that? Okay. So we've been optimistic for a while. Let's go get pessimistic here again. Let me toss out to Rebecca, I warned her about this. Do you have a nightmare scenario in this spectrum world?

Rebecca: Well, I did but after the panels this morning or this afternoon, I think I have a few more things to potentially worry about. Especially on the medical panel. There's things that were mentioned that I was not fully aware of. But, as you mentioned, I recently oversaw for ITS, the conformance testing of the spectrum access systems and the environmental sensing capabilities sensors for the new citizen's broadband radio service. That is just being deployed right now and my nightmare scenario on that one is that notwithstanding all of the careful analysis and the dedicated work of all the people involved starting with the FCC and through the testing that we've done, is that something unexpected or unanticipated could occur within that entire ecosystem that could actually cause harmful interference. And that used to...well, I was going to say, I don't currently lose sleep over it since my part of the project is pretty much done.

[Laughter]

Rebecca: But the other thing is that we did do our best to identify unknowns during the course of the entire process. And it was part of the risk assessment that was undertaken by all parties that were involved. Including...I mean, all parties involved and starts with the FCC, NTIA's OSM and our new Director, Charles Cooper is in the audience somewhere also. Or was earlier. And, of course, DOD. Then the SAS administrators and the ESC

operators and the Windform Standards Group and then the carriers. Oh, I'm sorry, SAS or Spectrum Access Systems.

[Laughter]

Rebecca: So I will SAS from here on out. ESC is the Environmental Sensing Capability operators and so I'll probably end up using ESC from here on out. But everybody really worked to mitigate throughout the course of the entire process. For example, some of the mitigation things that I think that have actually...that are going to save us from a potential nightmare scenario is that the propagation models that were adopted by the Windform Standards Group for CBRS have a fair amount of cushion in them. The testing the ITS did, we did our best to do as rigorous testing as we possibly could. The FCC is currently doing field testing through the initial commercial deployment which I think is also going to help pull out potential issues that might be out there.

And the SAS operators and the ESC...SAS administrators and ESC operators both did plugs out tests at different times. So everyone has tried to do their best in this brand-new spectrum sharing situation to be able to help mitigate the risks. But beyond CBRS, the whole dynamic spectrum sharing that we're...dynamic spectrum sharing between very, very different types of communication systems, as that increases and the density of those devices and systems, as that sharing and density increases, that's where I think that we really haven't fully tackled the potential for interference at the RF level. And I think we've got some real vulnerabilities potentially there that can affect both the reliability and the security of our systems and our devices as we proliferate and get them in a really dense area.

Clete: Can I add to...

Keith: Sure.

Clete: I would say my nightmare scenario is, if you think about the 2008 financial crisis. When you had a series of sub-prime loans that were in default in different parts of the country and unbeknownst to lots of people they were collateralized and split up and spread all over the place and then they were insured by insurance policies that couldn't back them up. And you had a problem in one place that cascaded and took over the entire economy. My nightmare scenario is that as the speed of innovation increases...or the rate of innovation increases and we deploy billions and billions of devices which, let me be clear, this is a very good thing. It improves business, it improves quality of life, it improves health. That was before I even heard of this what you might call a corporal private network that was described earlier, a CPN, I guess.

These are categorically a good thing. But, at the same time, it increases this conductivity among entities, sectors, companies, people that may not be even aware of the connection or where their data sits or how it could be corrupted, manipulated, the network

disruptions that create these cascading effects. And as Monisha was saying, we need to test these things...these networks and we're not going to know what the bugs are in them until they're out in the real world. We're also not going to know what the opportunities are until they're out in the real world. So the upside is also unknown and big. But the reason I feel some urgency about this interagency collaboration and this public/private collaboration that Rebecca was talking about is because it's crucial.

We're all a part of this increasingly symbiotic relationship and we don't know exactly what the effects of that are going to be when something goes wrong. We also don't know what the effects are going to be when we discover that maybe some of this conductivity cures cancer or creates other things that are unimaginable right now. But that's what we've got to get ready for is how all of these things cascade in ways that are...I think one of our panelists said, unknown unknowns.

Rebecca: Mm-hm.

Clete: I like that.

Monisha: Yeah, one of the things...I mean, not addressing the nightmare scenario so much but in the previous panels there was a discussion about standards and how that process can sometimes be very difficult to manage and if you look at the way...I used to do standardization in a past life. I used to be [inaudible 00:19:10]. The way standardization works today is its basically standards are designed on paper, right. A bunch of very smart people get together, you brainstorm ideas, you go off and do some analysis and simulations and then there are bakeoffs. But it's all on simulation and paper. In the past it was the other way around. One of the first things I did in my career was HGTV and they have a system of respect based on whose hardware performed better, right. I don't think that was a great way of doing things, either.

Because you could only build a standard for the next 50 years based on what you could build then, right. So the way we do things is better in the sense that we are keeping a path forward of evolving something. But it's gone a bit too far where everything gets decided on a basis of some exemptions of how systems behave and how we expect them to behave. And so somehow, we have to get this feeling of system testing, system experimentation and deployment into the standards making process. Or it has to be a quicker turnaround that hey, you know, we tested this, we deployed it, these are the bugs. We need to be able to fix the standard quickly. That process takes too long nowadays. And, as a community, we should probably pay more attention to what's that...as to how we fix...somebody mentioned that they found something and then 3GPP came back and said, sorry, we don't think it's a problem. So ways of making standards much more easily correctible once the effects are found out. It takes too long today to fix problems.

Keith: Okay.

Rebecca: Well, I think the first panel also talked about this idea of the systems of systems in the standards and...

Monisha: Mm-hm.

Rebecca: ...the silos that exist even in the standards organizations and when Keith was over at ITS, he was a big advocate of systems of systems analysis. So I think that that's something that...without that component to it, and that goes to the whole collaboration issue, too. Without looking at the whole ecosystems, we do leave ourselves vulnerable.

Keith: So that makes think about two issues. You talked about the collection of systems that cascade and you talked a bit about the scale. How do we test against systems to systems effects and things at scale? Is that something...I know this is completely out of the blue here, but this is...

Monisha: And I think it is a challenging problem. So one approach is we start building experimental test beds. And there's a lot of efforts within the government agencies to do that. But that takes time to roll out. The other is, we are living in an experiment, so to speak, right. I mean, all of the data that is being transmitted from cellular networks, Wi-Fi networks, [inaudible 00:22:06] networks, it is out there. You can measure it, you can analyze it and you can start understanding how these are behaving in the real world. We don't do any of it today. There is very little analysis of say, just...all of us sitting here are connected to base stations. We're connected to Wi-Fi. All of the signal strengths are going back and forth. Your phone has that information.

If only, could you imagine, if we could grab the signals of every phone just sitting in this room and goes to a central cloud and you can analyze it, right. There are, of course, security and privacy issues around just doing that and those need to be resolved just as we have had to resolve the issues around medical healthcare data. How do you collate healthcare data from different patients across the world and make use of it? But those are some of the, I think, solutions that need to be investigated as to how we go about getting a much better understanding of the spectrum future everywhere.

Clete: I think the challenge...everybody...most people in this room are probably familiar with the anecdote from maybe ten years ago when Senator Ted Stevens from Alaska referred to the internet as a series of tubes.

[Laughter]

Clete: And actually, the funny thing is there are significant parts of the internet that are a series a tubes. That's...just to give the late Senator Stevens some credit. But that anecdote points up a challenge we face in the policy making community. And that is that if you're...for those policy makers who are not deeply, technically...who are not

technical, and this is not a critique, this is the vast majority of policy makers, they see the internet as the device or now the connected device in the tubes, the pipes. So they think almost reflexively that the solution probably lies at the device end or at the ISP. And those are two really important parts of the internet ecosystem but are only two parts and maybe they know about a router or a server but don't really know what that does necessarily.

But we've got to...I think in Julius' presentation in the beginning, he laid out six or seven different elements that need to be part of this solution set. So, yes, it definitely is the spectrum engineers and dynamic sharing and addressing interference and jamming and spoofing and all of these issues that happen at the radio layer. It's also, just to go down a long list, it is the ISPs, it is the end devices. It's the gateway in the home or the enterprise. It's the backbone providers, the content delivery networks, the cloud providers, the web hosts, the software developers, the enterprises. To some degree the end user or the consumer, although I think we don't want to put too much of the burden on them.

And then it's state, local governments, national governments. That's a long list of entities that need to be coordinated. That's hard to do. Humanity is stove-piped and territorial. It's going to be hard to get all of those players together when nobody is in charge of the whole ecosystem. I think we start by recognizing that it's sort of an existential imperative that we do that. It's also a business imperative because if these cascading effects ripple through the internet ecosystem, it means a lot of money lost by a lot of enterprises. So we've got to collectively figure out how do we protect the good guys from the bad guys here.

Keith: So let me jump in on that for a minute. One of the previous panels talked about the interaction of systems. There was the example of, what was it, that airport system that was interfering, knocked the hospital off. And you mentioned incentives. So who's responsible for figuring out these interactions? Is it the company that's going to deploy in a particular domain or how do you incentivize them to figure out who am I going to interact with?

Clete: That is the question of this era, I think. Because the real problem is it's not just...I mean, maybe the airport example is one of the easiest because at least the FAA has the beginning of the authority. But if you start thinking about where the threats come from and how they would interact or how they would affect these systems, it goes well outside the aviation industry. It goes to the software development that goes into the systems in the first place, it goes to various authentication mechanisms and encryption approaches and you multiply that by every sector in the economy and the answer is nobody is in charge of that. And it's not even within the geographical region of the Unites States. It's not even the United States government that can purport to be in charge of the internet ecosystem that effects that network.

So we've got to figure this out. I think it starts with the federal government working with allied governments and then going down into the interagency and we can walk through some of the...Pierre would have to pull out his acronym, that flag, one right after the other. But the good news is all of these agencies are working on this and I know that Dr. Porter's counterparts at DHS, Chris Krebs, he's the head of CISA, Chairman Pai at the FCC, Diane Rinaldo at NTIA, Dr. Copan at NIST, all of the...and Monisha's right, it is also NSF, it is also all of these other agencies that are key to this. We have to think about how are we going to secure this connected ecosystem in the future and, by the way, nobodies in charge of it.

So is it going to be a tragedy of the commons that the whole ecosystem just gets trashed because nobodies in charge of it or are we going to figure out a way to structure these incentives such that everybody's equities are maximized? That's quite a challenge. The good new is there are a lot of interests behind doing just that. A lot of national interest, a lot of public safety interest, a lot of financial interest. My glass half full take is, we're going to figure this out somehow. It's probably going to be pretty bumpy in the next few years though.

Rebecca: And I would assert that if no one is in charge and it's a public good we're talking about, then that is the type of thing that the government should fund and that NSF is funding and the sort of work that ITS is working on. One way, I think, to secure, not in the cyber security level but at the RF level, if I could take us to the RF level for a few minutes.

[Laughter]

Keith: Sure.

Rebecca: Because earlier there was talk about interference. And Julian laid out some interference issues and he pointed out, I believe it was in the tutorial, that the first link is almost always wireless. So in order to secure the RF level, we have to understand it a little bit better. We have to make it more approachable. We have to make it be something that is not just mystery and magic and black box sort of stuff. There's a lot of things that are happening in the government right now to be able to solve those sorts of problems. I'm going to give some plugs here to ITS and the work that we do, also. And that the work that NTIA does. Historically, regulatory, there's been three different areas of interference that people have talked about.

They always talked about it at...earlier folks did, too. One of them is intentional interference. That's our jammers and folks like that. And then we had the unintentional interference and I learned a few other things about unintentional interference in the hospital examples that I wasn't aware of. But unintentional interference can also be things like devices that are malfunctioning or components within devices that are malfunctioning or something that is...there's a small change in the manufacturing aspects that cause a change in how the device is made. Or there's erroneous programming. Or there's

intermod issues that nobody expects. So there's different things like that. Or the spurs that folks were talking about earlier.

Those are all sorts of issues that will proliferate the unintentional interference issues and will proliferate as we get more and more devices out there because that interaction between the different devices. And, of course, Julian and the other folks mentioned on the first panel, the incidental interference issues also. One of the other issues that Dale mentioned in the tutorial was big data as an interference issue. And we maybe we can talk about that a little bit, too. But the other one...there's two other ones that I'm seeing popping up in the work that we're doing and one of them is aggregate interference and that is something that we're working on at ITS.

Aggregate interference is basically if you...it's the...when everything is operating at the same time, everything is operating legally but all that sort of stuff combined in the same space at the same time is potentially causing interference and that's an issue that the more we learn about and are able to analyze will provide assistance in the interference issues. The quality of what comes out of the...interference at the arc level can impact the quality of your experience and the quality of the information you're getting out of your medical devices or the other sorts of things and so all that depends on the bandwidth, the [inaudible 00:32:56] latency and the air rate and tall those sorts of things.

So some of the work that I think is ongoing to be able to deal with some of those issues is...I mean, there's a lot of work going on in a lot of places both in academics and throughout the government at NSF and SSF but I would like to, if I could mention a few, one of them is the...one issue that has been in existence my entire career is receiver standards. And for the first time, the commerce spectrum management advisory committee has...which recently was reconstituted and had it's first meeting earlier this or last week. One of the topics that they are going to be talking about is transceiver identification.

And given my historical background in the enforcement bureau, from my personal perspective, this is not NTIA perspective, but my personal perspective is transceiver identification will just be a game changer when it comes to identifying sources of interference. One of the other things that's maybe less obvious for non-spectrum geeks is the role that propagation plays in interference. And one of the things that ITS is trying to do is trying to improve and enhance the existing propagation models by adding clutter data to them and adding litar information to them and looking at terrain and putting all these components together and making them modular so that they're plug and play.

One of the things that we could do potentially also to make spectrum...understanding spectrum interference more accessible to other people is once we get the models out and make them accessible through web services and through apps where people can plug in their locations and be able to potentially identify where the signal might...how far the signal will go. Will it transmit through a wall or will it transmit through this forest or will it only go a mile, or will it go ten miles or will it, you know. So having some ability to be able to

put this information out in the hands of the public, to be able to have a citizenry that is more skilled and more knowledgeable or at least has the capabilities to be able to gain that information through enhanced understanding and demystifying, as I said earlier, the RF work I think is one area that we can continue to work.

Going to your point about collaboration and sharing of information and working together, another area where ITS does a lot of work is in interference protection criteria. One of the things that I think is absolutely critical in order to reduce interference and increase efficiency to that we can have more devices on top of each other in the same place at the same time, same frequency, is if we understand the interference protection criteria's between the different types of devices and systems that we're operating and working with. The only way that we can really get that information is if everybody is sharing information about the technical components of their systems.

And it's really, really hard to get that done because there's proprietary, there's competitive and there's security reasons why people don't want to share that information. The NTIA OSM is doing a really good job right now with their feasibility studies to be able to try and get some information about some of the new systems on the DOD side. But we need the private sector to also be willing to be able to provide information and put it out there in some sort of fashion where people can understand what the real interference protection criteria are so we can get those devices closer together and allow these systems to be able to continue to operate.

And the same sort of thing with the aggregate. The more we understand about aggregate, the more we're going to be able to deal with interference when we have 5G and IOT devices all in a really close location. I was going to leave it for there but there's one other thing that popped up in the discussions earlier.

Clete: You're on a roll. Go for it.

[Laughter]

Rebecca: And then I'll be quiet.

Clete: No, this is great.

Rebecca: No, but folks were talking a little bit about privacy in some of the earlier panels. Once of the issues that has been lagging in us talking about it. I almost hate to bring it up because we haven't solved it, also. But I think it's important. And it deals with the RF level. Is the issues...and we brought it up in the International Symposium on Advanced Radio Technologies in 2016 when we did spectrum forensics. But that's the issue of what do you do with the information that's on your IQ data that you gather when you're doing spectrum monitoring.

Keith: IQ?

Rebecca: Okay. I may have to ask one of the engineers to help me here.

Monisha: In-phase quadrature.

[Laughter]

Rebecca: So that's just another issue that I think fits into the whole issue, and it goes to the security issues also that we need to be able to crack in order to ensure that folks understand where their privacy is potentially vulnerable. And that's all I have for right now.

[Laugher]

Monisha: So I just want to thank you so much for that. That was...

Clete: Great rundown.

Monisha: ...excellent and I really am glad you brought up the topic of receive standards because that really can be a game changer. Historically, we've always talked about interference as something that comes from the transmitter side. That we regulate how much you're transmitting, what your transmit mask is and we think that that's going to solve interference. Interference happens at the receiver. So if you're building a really sloppy receiver and today there are no regulations about how much out of band rejection you have to build in that receiver, so you can build a really sloppy receiver for the same transmit signal and get a lot more interference from adjacent channels whereas somebody else who has built a better receiver cannot, right.

And we don't regulate that today. So interference has to be thought about as something we regulate both at the transmitter and at the receiver level. Very, very important. Going back, a little bit different topic, going back to the topic about spectrum sharing. Today, one of the biggest topics in spectrum sharing and spectrum coexistence in the commercial world is basically license systems like LTE and cellular moving into non-license bands where you've had Wi-Fi for a long time over. And that's one of my personal research areas that I've been working on. That is another one of these problems that you talk to the Wi-Fi people, they say LTE is going to kill us. You talk to the LTE folks that say, we are much better than Wi-Fi, we'll coexist perfectly with them. We actually made them better when we were in their space.

Truth is somewhere in the middle. And there is very little unbiased testing or experimentation or analysis that's attacking a problem like this. Going back to standards for a minute, I was at an IEEE coexistence workshop that IEEE ran, and they brought 3GPP folks into the room and it's interesting to see the dynamics. They all agreed that if

they could have, for example, a common preamble that both would listen to and respect, both performance would increase. But they could not agree on what this preamble should be. Sometimes there is just this hurdle that people have to overcome. These different groups, different standardization activities. And I guess part of it is human nature and I don't think we are going to change human nature as quickly as we can change technologies.

But I'm hopeful that as people see that if you're sharing a piece of property and if you play nice, everybody benefits. I hope that over time, that lesson will sink in and systems will learn to collaborate better. And I think a great example of that was what we saw...some of you've seen some of the recordings of the DARPA spectrum collaboration where they gave points to teams based not on how a single team performed but how the collaborative of teams performed. They found that they automatically pitched policies that would increase the sum rate of all the systems rather than just increase your sum rate.

Somehow, we have to move towards designing wireless systems that adopt this as the guiding philosophy rather than I'm going to increase my [inaudible 00:41:22] at the expense of everybody else. Aggregate interference is a huge issue and, again, is one of those things that we run into all the time in terms of, how do you model it, how do you measure it, what are the effects. I think the outer wide band whole effort sort of fizzled away because nobody could really figure out how you would model many outer wide band devices that are each transmitting according to what they're allowed to transmit but we don't know the aggregate interference is at the receiver. So all of these sound very negative, but I really don't think so. I think just the fact that there are initiatives underway at various levels in different agencies shows that people are addressing these.

Data is, I think, the hidden...could be a solution, could be more of a problem but we cannot ignore it. We have to be able to explore the amount of data that's out there. Wireless systems are great because we don't have to go and tap into wires to figure out what's going on, where the signal strengths are. We can really, really do a much better job of monitoring the spectrum around us. One last thing, if I may.

Keith: Absolutely.

Monisha: Going back to the awareness and education piece. At the NSF, actually, we think that's a huge problem. The workforce development of people just being aware of how important spectrum is. So one of the proposals that NSF funded was one of the [inaudible 00:43:00] power platforms. Part of that proposal was that they had to have a program called research experience for teachers. And this is high school teachers. Not necessarily high school science teachers. They brought them in for the summer and they made modules with simple dongles with software defined radios on them that allowed them to see spectrum. Most of them were seeing it for the first time in their lives. To actually see just a way, from what it meant, that particular piece of spectrum was

occupied, what interference was, how you could find spectrum holes and just seeing the excitement of these teachers and they were going to take back that course material to the high schools and educate the next generation of kids as to this problem, I think is huge. We need to pay much more attention as a community on getting those kinds of initiatives underway.

Keith: Great. Any...do you want to add more to that or...

Clete: No. I think that's the...just to pick up where Monisha left off, the human element of this is, in some ways, the most important and maybe the most difficult. Although maybe I'm just a 45-year-old guy and my three kids who are digital natives would totally disagree with me on this. Let me flip from the pessimistic to the optimistic. Hopefully, that generation that grows up doing everything from school to some aspects of their playful life on devices, intuitively will understand how all these things fit together in a way that would be foreign to us. So hopefully that's where this will go. In the meantime, I think we've got the multi-disciplinary aspect of these challenges is the hardest thing that we're going to have to address. Because it will take awareness of basic spectrum issues, awareness of basic software development and software development life cycle issues, basic systems of systems understanding. And we're not there yet. We've got a long way to go and it's going to be...with all these acronyms that are out there...

[Laughter]

Clete: Just to throw one out that's maybe my favorite is the worst acronym in DC other than...Rebecca mentioned CSMAC. Pretty bad one.

Rebecca: I did use the whole word.

Clete: Yeah, you spelled it out. I was real impressed with that, yeah. I have an even worse one. I'm going to spell it out. CSRIC, the Communications Sector Security Reliability Interoperability Council, it's the FCC's advisory committee on essentially communications security issues. It's a mostly private sector but also some public sector, both DHS, 911 operators, other experts who come together and try to solve these communication security challenges. And the last CSRIC, the last iteration of it published about 150-page report on 5G security and went through the basics. It was the most...it's a very comprehensive look at network function, virtualization, software defined networking, the edge and how you [sneeze 00:46:41] that didn't get as much into the core spectrum issues as maybe they could but the present CSRIC has two working groups working on two elements of 5G security.

One is legacy vulnerabilities that may or may not transfer from 3G and 4G into 5G and then two is the present 3GPP standards process and are essentially, to put it in laymen's terms, are those standards good enough. And if not, what optional approaches need to be taken. That's just the FCC and it has a...it can be kind of cloistered in the

communications sector and even sometimes DHS might not know what's going on on the CSRIC even though that's a great cloister of expertise. We need to find ways for all of those activities to feed into each other and then to somehow reach out into the...beyond the expert policy community into the just day to day business and consumer world. It's a big task. I guess I'll just close by saying I'm counting on my eight-month-old, six-year-old and nine-year-old to get us there.

Monisha: I would also like to mention that we should not forget the passive uses of spectrum, too. Because, actually, NSF manages radio astronomy activities and that may not have any direct commercial benefit right now, but it gives us an understanding of science. So being able to understand...being able to take measurements in certain parts of the radio spectrum is extremely valuable in deep space exploration and all of the other activities that NASA and all these telescopes are used for. And as these folks explained to me is that when we need to observe the emissions from an oxygen line, we cannot move elsewhere. So we cannot share that spectrum with somebody else who wants to use it. If we need to observe the spectrum at that particular frequency, that's when we want to observe it.

Today, because of this, large [inaudible 00:49:00] of spectrum are blocked off because of this observational capacity. Those guys are willing to share in the sense that, we're not observing all the time, when we observe, we don't want anybody using it. When we're not observing it, you're free to observe it. Today we don't have any systems in place that allow them to do that, that allow the commercial world to do that and so the default category is that nobody uses that spectrum. So there is a lot of ways of maximizing efficient use of spectrum in a way that benefits everybody. The passive users as well as the active users of spectrum.

Rebecca: And that will require trust.

Monisha: That will require trust, yes. And that goes back to the whole idea of community and humans and how much do we believe everybody is watching out for each other, right. Because right now, there isn't. There is always that tension of, I need to hold onto this because if I agree to share it it's going to be taken away from me. We need to change that dynamic.

Keith: Okay. Perfect timing. So we're being asked to move to audience Q&A. So per the ground rules of Silicon Flatirons, first question needs to come from a student. So do we have a student volunteer? We have a hand up over there.

[Unintelligible background noise]

Keith: Hold up. Just one second. We're only getting it in one ear. I just want to make sure that the people on the live stream can hear you, as well.

Alan: Hello? That's better. Okay.

Keith: There we go.

Alan: Hi, I'm Alan. I'm a 3L here at the law school. My question was, I came into this conference, spectrum security, I thought it would be much more focused on avoiding things like hacking, exploitation of the systems, jamming, et cetera. But so much of the focus of the panels has been on just developing systems whether it be 5G or 3.5. Rolling out systems that actually work in the aggregate when the systems are densified without betraying themselves. So my questions is, how much are we prioritizing in securing the RF layer and just getting these systems to work versus how much are we focusing our energies on avoiding the more malicious exploitative types of vulnerabilities and does one solve the other. If we design a system that works to not betray itself in the first place and it's harmonious and it works, does that, as a byproduct, prevent a lot of the exploitation or hacking in the first place?

Keith: Great question.

Rebecca: That's a very good question.

Keith: Do we have a volunteer to tackle that?

Rebecca: Yeah. I'm going to do a confession again here, I guess. So in the 3.5, the conformance testing was done on the components of the system, I think, as I had mentioned that the systems of systems. And so the question becomes is, as you said, once it's out and working, will it work, and can we assume that all these things will work together. But I think the first panel pointed out that there...at all of those interfaces, there's always vulnerabilities. And even in the testing that ITS did on the spectrum access systems, we did do security testing on it and I was recently asked this past week if we had done any sort of red team type testing on the SAS and no, we didn't because of the environment that we were in. We were constrained to the types of security testing that were designed through the standards organizations in the way that we did it. I think it's a fair question and I think it's something that we all...that anybody that's...we all need to think about that a little more, too.

Monisha: I think the systems...all of the systems, and I guess in CBRS it's mostly, again, either LTE or 5G that's going to be deployed.

Rebecca: Well, it's technology neutral, so we don't know.

Monisha: Yeah, right. So whatever system gets designed, does get designed using certain attack models in mind, right. So you design the systems to make sure that they're robust against these. But with security, you always are faced with what happens after you deploy them and there are attack models that you hadn't planned for that bring down

your system. What then, right? That's the really tough part. So to go back to your question, yes, most of these systems are designed...I think the second part of your questions is, how do you deal with attacks that you hadn't thought about bringing down your system and that really is on a case by case basis. There isn't a very well thought out way as to how we solve the problems.

Some of it is maybe you have to go back to the standard and fix a hole in the standard that nobody thought about. And so how do you make that...let's see, the other thing is you can patch up stuff, right. So, for example, the [inaudible 00:54:15]...it's not really...nobody...I don't think anybody really thought that that would end up being a security problem, but it did. And there isn't a solution to it even today. There are some ways of trying to end a file but there isn't and that is a problem. It's not a solved problem unfortunately.

Clete: I would also echo, that's a great question. And the way I would answer it is that in my view, and my perspective has always been in thinking about what the bad guys can do. In some ways, building a system that works and works transparently to itself such that it notices if there's an anomaly is a predicate to addressing the malicious threat. I'll give two examples in the wireless world where we're seeing some progress to that end. One is something called the Open RAN Alliance. This is essentially radio access networks that are open...whose standards are open and interoperable. The idea being that you can get to security by interoperability because interoperability requires standardization and if somebody, and we've gone through this whole day almost, I think without mentioning the word Huawei.

[Laughter]

Clete: I guess I'm that guy. If there's a player in the RAN world that's trying to do things differently or even in a customized bespoke way, that's not interoperable with other systems or not interoperable with other core networks, then that might be...that could be a security problem or it could be a way to get into that network that would not be as easy to get into if everything is standardized.

The second one, and this is at the other end of the network, is something...I don't know if there are any folks from the Cisco world here but Cisco has been...has pushed a standard called the MUD standard and I'll give you the...I'll spell that out. It's the Manufacturer's Usage Description. And this is for an end device. So a widget, a connected widget that is on a network and it's talking to a router or some other gateway function and under the Manufacturer's Usage Description, when that widget first connects to the network, it tells the network, here's what I do. So if the network senses that that device is doing something other than what it's supposed to do, it basically can kill the device on the network. This is a...it's a mix of transparency to the network or to the system and anomaly detection that can only happen if you have the predicate of a system operating the way it's supposed to, transparent to itself.

Rebecca: One other thing if I can just...some of the earlier panelists were talking about the data that they've got about security events or interference events and the hospital issues. And they all have them and their information is in their own little bucket. I've always been an advocate for sharing those types of events and incidents and making that information more accessible to everybody, especially to academics to be able to research it because I think that that is potentially a ripe area for AI also to be able to maybe get ahead of these issues on securities and vulnerabilities if we can do some sort of post processing analysis of events that have been reported and have been identified. But just we haven't shared the data across industry.

Moisha: Yeah, there's a lot of work happening in anomaly detection or receive identification. So, for example, we focus a lot about the actual messages that are going over the air. There's a lot of information, also, in the IQ samples of actual signal itself and those are almost like signatures of the device that's transmitting. And you can use that, people are showing as more and more data comes online that it's becoming possible to identify a receiver just by observing it's transmission over time, by collecting the data and you can figure out what the [inaudible 00:58:45] are, what the unique characteristics are. Just like all of us have unique characteristics that we learn over time, you can do that with receivers. And this is where machine learning and data is beginning to show dividends.

Keith: Great. We had another question down here.

Parker: Hello. Is this on?

Rebecca: Yep.

Parker: I'm Parker. I'm a second-year student here at CU Law. It seems like one of the common threads throughout multiple panels has been that we need to increase the diversity of voices at the outset of standard setting but that it's incredibly difficult at the international level. Is there something that the FCC or another agency in the US at a national level can do to help amplify the voices of those independent security researchers or academia, like we discussed?

Moisha: Yeah. So in the US, we've always taken the stance that standardization is in the domain of industry. They know best how to do it and they've done it very well. So there isn't any government level, federal effort to manage that in any way or form. It is actually the burden of academics but [inaudible 01:00:06] standardization board use is pretty high. These meetings are held every two months all over the world and you got to travel there for a week and there's a...it's a full-time thing. Which is very hard for academics to do given that their full-time job is teaching and research in a university setting. There are successful instances, however, of academics collaborating with industry. So where the industry partner is actually going to the standards, getting a lot of the relevant information and having the academics put in their innovativeness in solving problems,

coming up with solutions that they can then take back to the standards board. So maybe not the most efficient way of doing it but that is how it's done today. And it's one of those things where it's...that's just the way it is being done and I will leave it up to the FCC and other agencies if they want to address whether there is any bigger effort...

[Laughter]

Moisha: ...involving the federal government at a level in standardization.

Keith: Okay. We've run out of time at this point. So thank you very much.

[Applause]

Closing keynote

Pierre: All right. So we're just going to move straight into the second pillar of this event. Something I've been looking forward to, not just today but for quite a while. If we could get the panelists to clear the stage, let me just say a few words about our closing keynote speaker, Dr. Lisa Porter. She's the Deputy Under Secretary of Defense for Research and Engineering at DOD. She's a scientist that was trained at MIT and Stanford. Her job is to oversee R&D and prototyping activities across the whole DOD enterprise. And that includes overseeing this whole alphabet soup of all sorts of different agencies. DARPA is one that most people in the room would probably know. Her brief is very wide. It includes artificial intelligence and biotech and that's just the first two letters of the alphabet. And you can go an read about more of them. The reason why she's here today and whey we're so privileged to have her is that the DOD has named her as the leader of it's 5G strategy and initiatives. I've heard it said...and they say this a lot apparently in the DOD, she didn't duck fast enough in that discussion. So, as a result, she's learned a lot, I'm sure, about spectrum and spectrum management and discovered how complex and interesting it is whether she wanted to or not. We're very, very fortunate to have a scientist and a public servant of her caliber here. I asked around, you know, if there's anything about her that I should mention in addition to the resume that you should read and I was told that she doesn't like long introductions. So I'm just going to shut up now.

[Laughter]

Male 1: Dr. Lisa Porter.

[Applause]

[*set-up material deleted*]

Dr. Porter: It's really odd to be giving you a talk this late in the day. So I apologize if you guys are really itching to get out. I'll try to cover this fairly quickly, but I also will allow time for questions. So for those of you who want to stay and ask questions, we will have time for that. All right. So I thought I would start off and yes, it is a true anecdote that I did not duck fast enough. I am an engineer and physicist by training. How many of you guys consider yourselves scientists or engineers? Okay. So you can relate to this.

So I was in a meeting in early February of this year minding my own business and 5G was the topic and of course it was a very important meeting. The Secretary of Defense was concerned about, what is this 5G, what should we be paying attention to, we need to understand it in terms of our mission and what we need to be executing. And then there was just a bunch of bologna being swirled around. So, for those of you who are not engineers, I apologize. But when you're an engineer in a room and you hear a bunch of non-engineers saying stuff that they're throwing out every acronym they know but

they don't really know what they're saying, depending on your tolerance level, which for most of us is right around 45 minutes, then your head just kind of explodes, right. So that's what happened to me. My head exploded. The bad thing about that is, of course, when you finally raise your hand and you say, you guys are full of it, this doesn't make any sense, it's not even...I don't even know what you're saying. They look at you and go, great, you got it now.

[Laughter]

Dr. Porter: And I never learn, right. It's like, this just keeps happening to me. So, yeah. So that's how I ended up with a...and yes, I'm not an expert in spectrum. I will confess to you that I have been really blessed that the DOD actually has DeepBench in this area. Of course, the FCC and NTIA has DeepBench in this area and I've been very fortunate to get to be a little bit educated on it through all of those great, smart people. And also, come to really appreciate this whole domain and the folks who work in this space. It's really awesome because it's a really techo-nerdy area. Right? It's really cool. And I...one of the things that came up in this panel about workforce development, I think actually we have to make that coolness more apparent to our young folks who are going to universities because it's a really awesome area to become an expert in. I've enjoyed getting to learn about this despite having first been handed to it a little bit with an, oh, no, it's mine. I'm glad now that I was asked to do this.

I'm going to give you a little bit of an overview of how the DOD has come to get our head around this topic and try to figure out what we should be doing that's appropriate to our mission. And I've tried, for my colleagues and myself, we've really tried to engage with as many in industry as we possibly can. We recognize how smart industry is in this domain, how long they've been thinking about this and their perspectives have been very valuable in helping us to shape how we're going to go forward. The first slide here shows some key themes. I think some of you have heard these themes today. Interestingly this graphic comes from Cisco, a paper they published in 2014 and I intentionally used that because I think it's actually not a bad graphic to demonstrate what we mean by where we're going toward in terms of ubiquitous connectivity. But clearly people in this area have been thinking about this for quite a while.

It is really important, I think, for the broader community to understand, those who are coming into what is 5G and what does it mean to me, to really recognize that 5G is not just 4G on steroids. It is not just about the RAM and it is not just about cell phones. And it's not just about cat videos at a faster speed of download. So we've been really trying to message this hard because when you think about what ubiquitous connectivity means and in the context of the prior panels it does present both a lot of opportunities as well as a lot of challenges in terms of the vulnerabilities. So we really have to be mindful of that. When we look at security from the DOD perspective, we recognize there's no such thing as a secure system. This has been true since before 5G. This has been true forever.

And I think we fall into a trap when we think we can design perfection. So this was alluded to in a couple of other panels and I was very glad to hear other people expressing that perspective. We obviously strive to make things more secure. We strive to address vulnerabilities. But we should keep in mind an approach that we like to call a zero trust. And in the cyber domain, and some of you are real cyber experts, you know that the zero trust architecture approach is one that's gaining a lot of speed because people are recognizing, as things become more interconnected, perimeter defense approaches really do not make any sense. They actually never really did. But they really don't now. So we are really pushing and advocating for zero trust architectures as part of the thought process.

Then the third point which is really important, when you talk about vulnerabilities and people brought up Huawei or at least one person brought up Huawei in the prior panel, the DOD has a perspective that's very simple. We have a mission. We have to be able to operate through anywhere at anytime. We don't get to choose where we deploy or when we deploy. We have to be able to operate. And so we are approaching 5G and next generation ICT more generally in terms of how do we ensure that we can operate through regardless of who's there trying to prevent us from operating. The military that masters ubiquitous connectivity, in our opinion, is going to be the one that maintains overmatch. Ubiquitous connectivity was alluded to in the prior panel. I liked how it was characterized.

It offers a lot of opportunities, many of which we cannot fully anticipate today. And it also offers a lot of vulnerabilities many of which we cannot anticipate today. But we have to adopt the mindset of continually being flexible and adaptable in our understanding and our ability to both defend and exploit the 5G opportunity space so that we are, in fact, the masters of our domain. All right. So this next slide talks a little bit about operate through in the context of its relevance to the broader first responder community. For those of you who have an interest in the first responder problem space, you recognize that there's a good amount of overlap between what I just said and what first responders have to deal with. The ability to operate in congested and degraded spectrum environments and the ability to operate over networks that may be compromised.

So we see and a lot of conversation earlier today, we really see an opportunity in moving from the static and manual approach to spectrum allocation to one where we really strive for dynamic spectrum sharing approaches. And that's a big part of our strategy as we go forward. The CBRS example, the 3.5 ghz example that was talked about, I think, is a really great proof that this is a possibility. That we need to get serious about this and that we can get serious about it. It is something that's going to require true collaboration as was talked about prior panel around both industry, DOD and other government agencies saying how do we do this together. But it is doable, and we've got to start working on it now. This will give us a significant national advantage...competitive advantage globally, if we solve this problem.

Because if we figure out how to do this, of course, we will be able to maximally use the spectrum and others may not be as good at it if they don't figure out how to solve it. So we are really excited about what dynamic spectrum sharing can potentially offer. Although we recognize that it is very difficult. Particularly when you look at a lot of frequencies and things moving around a lot of different devices and so on and so forth. I would add to that, again, we expect to look at robust overlays in our networks as well as the zero-trust architectural approach that I mentioned prior. And the Cisco example that was given, the MUD example is one that, I think, is motivated in part by a zero-trust mindset, right. It's don't assume that something can connect to your network based on who they say they are. There's a constant need to be doing end point security and end point verification and validation. So those kinds of thoughts are already out there in industry, but we want to amplify them and coalesce them around a strategy.

Here comes our plan, our overview of our DOD plan in one slide. It's always good to have one slide in the government bureaucracy, right. Because typically that's about the attention span of most people you brief.

[Laughter]

Dr. Porter: And then, second, you always have to have a graphic, some pretty picture and then the third thing is every strategy has three points, right. Always three points.

[Laughter]

Dr. Porter: So A for effort here. We have a graphic and it is DOD parlance, so you'll see war fighter to war fighter, war fighter to machine, machine to machine. If you were in the commercial or private sector, substitute human for war fighter and you'll see that there's a tremendous amount of overlap between the amount...sorry, the use cases we're interested in and those that will have commercial or private sector relevance. So we've circled four and it may be a little hard to see those but one of those areas is the VRAR application space. As you know, this is an area that's greatly interesting to the commercial sector for a lot of gaming applications. But, for the military, there's a lot of opportunity here we see in training, that's kind of obvious, as well as potentially medical types of things. But also, educational. Which for both DOD and the private sector has interesting applications.

In the center you see smart DOD ports, camps, bases and stations. Obvious analogs to smart cities. In fact, the NSF representative on the panel earlier was talking about PAWR or Power and part of what we intend to do with DOD is partner with NSF and do some lessons learned and they've been building up those test beds as we push forward to try to develop test beds that explore how we would really do the set scale. There's also the logistics management supply chain. Obvious commercial and DOD analogs. And depot automation, think warehouses, think depots, again, pretty clear commercial analogs. So

when we talk to industry and we ask them, are these the kinds of use cases that are of interest to where you're looking to push 5G, they said, of course, this is not a secret, we've been talking about hese things.

And we said, well, would it be interesting to you if we had some collaborative experimentation that allowed the DOD to accelerate what you're already doing into our space but at the same time would allow you, industry, to perhaps expand the experimentation base that you are currently conducting and really look at some different interesting use cases. And they said, yeah, that would actually be interesting to us. And so, with confidence, we go forward and we say, okay industry, we're interested in working with in collaborative experimentation. This has obvious DOD benefit, but we believe it also has a benefit to industry, as well. They operate through part of our strategy I've already commented on. We definitely need to make sure that we can operate anywhere and anytime. So part of what we'll be doing as we do these tests at scale and on our DOD test facilities at various bases, is we will be doing red teaming. That was the question that came up earlier. Red teaming will be a part of what we do to explore the vulnerabilities as we explore these different use cases so that we can understand how we can improve the ability to operate with these use cases while reducing our vulnerability profile.

Finally, the innovate part refers to the fact, this is something that I'm personally passionate about, that there is no finish line here. There's been a lot of parlance in the popular press around a race for 5G and who's winning a race. I'm not a fan of that analogy because a race implies a finish line and there is no finish line. 5G is just one stop along the way to a continued progress, hopefully progress forward as we go. So it'll be 6G, 7G and fill in the x G. We need to continue to push ourselves as a country to be at the leading edge of innovation. This is why partnerships with NSF, for example, are very important to us because we want to bring industry and academia along and push things forward in the cutting edge. 5G right now promises a lot of things, some of which will come true, some of which we will fall short. The areas where we fall short and we learn through experimentation where we're not ready, we want to continue to innovate and figure out how we address those things.

That's where you're going to see a three-pronged approach from us where we'll have some investments that are more longer term, higher risk, technology readiness level being lower because we see that we've got to keep pushing. For those of you who are interested in working with us, we will be putting out a solicitation in fairly short timeframe, hopefully. You'll see at the bottom of this chart indicates an initial draft RFP is anticipated in early November. But I mentioned the use cases already. The initial RFP will say, okay, these are their initial use cases we'd like to try, these are the initial DOD bases that we're thinking of trying them at, this is the kind of information we think we can provide, this is how we think this is going to go. The nice thing about having a draft RFP is it allows industry to come back to us and say, you forgot to address this or this

part is confusing or we're not sure how this IP coordination is going to work, how we're going to protect our IP and still address what you're trying to do.

That conversation can occur when you have the draft RFP. And then we put out a final RFP that's hopefully tailored enough that industry says, hey, that's a good request you're asking for. We understand what you're asking, and we can respond to it. We expect to do this in a rolling fashion. Meaning there's no way we can know everything nor should we know everything right now to ask for. Rather than trying to put out every single use case in every single base all at once, we're going to do this in a rolling fashion. We're still working out the details of how many bases and how many use cases will come out in the first solicitation and then how many will come out, let's say, three months after that and then another three months after that. These are estimates. Every number I give you is an estimate. Roughly three months, right. I always have to be careful because people write this stuff in the press and the roughly disappears and so when...in the government nothing is ever precise, right. So just keep in mind that we try to give you as much information as we can but here's always a squiggle next to what we say.

So if you're interested in how to work with us in these large-scale test beds and how to work collaboratively, even if you're in academia, if you say is there a role for us, absolutely. There are many members of the National Spectrum Consortium with whom we are working. Some of you may be members already. They have both academic and industry members. It's really easy to become a member, if you aren't one already. They really make the barrier to entry extremely low to join. And you can participate if you're a member. But you can also participate as a sub to a member if you're not a member. Okay? So you don't have to be part of the National Spectrum Consortium to ultimately participate in this activity, but you will have to be a sub to somebody who is a member. I would note that we're pretty heartened by the response we've gotten over the past few months from our NSC Consortium members who have provided over 260 technical concepts for us in these kinds of use case areas, here's what we think, here's what would make sense, here's the commercial use case and the DOD use case we see working out.

We're culling all that together and figuring out exactly what we asked for in that initial draft RFP. So what I'm trying to message to you here is it's an iterative process to try to get it right so that when we go forward and say these are the test beds we want to set up, and we're looking to industry and the private sector to work with us to do that, it makes sense and it doesn't sound completely crazy and people more or less say, hey, I know how to respond to this and bring something reasonable to the government to go do. What are we going to get out of these test beds? Well, we're hoping that we'll get some fieldable prototypes and we intend for them to remain at the DOD locations and hopefully they will be delivered within about three years of the start. Okay? That doesn't mean we couldn't deliver some things earlier but ultimately; we're expecting a three-year kind of effort.

We're hoping there will be turn-key solutions so that if they work, we can actually scale them to other sites fairly easily. So, in other words, we don't have a lot of additional NRE to invest. And we're hoping that there's an opportunity to learn. Because we know not everything's going to work as advertised. We know we're going to learn some things. A lot of the discussion during the day has come up, all those things we're going to learn. Some of them are going to be some pretty ugly lessons. But that's okay. That's how we advance. And we just...we can't be afraid of that. We've got to try things in new ways and the things that don't work, we've got to make sure we write down our lessons learned and share those and provide those, so we get smarter as a community. That's a key commitment that we have here.

So our deliverables will include things like the infrastructure sufficient to support the prototype products and services but also the lessons learned and the software and formulary development kits that will allow us to do continued development and fielding. That's kind of the big picture of where we're going. NWCLA in a couple weeks, I'll be rolling out a little bit more detail, I'll have a little more...the teams are rapidly working as fast as they can. I should mention that all the services are engaged. This is really a DOD large effort. We're closely collaborating also with our agency partners. We have good participation from the NSF folks thinking about the innovate part of our strategy to other parts of the national security community and how do we test for vulnerabilities. And, of course, as I mentioned, with industry as well as with FCC and NTIA who have been very supportive of what we're trying to do here.

The dynamic spectrum sharing will be also part of what we try to explore. The 37 ghz I think was mentioned this morning by Julian about...as one of the areas that we're collaborating on. I think that provides a good opportunity to say, how might we do dynamic spectrum sharing in the millimeter wave regime. Which I think, by the way, the United States has a real opportunity to get way out in front if we figure that out. So 5G timelines, the top part of this chart is something you're all familiar with. This is kind of the standard timeline that you guys have seen. You see the 3GPP roll outs, you see the FCC auctions on there nicely and then, it looks like we were planning for this all along, doesn't it? Yeah.

It didn't suddenly happen in February. No, we had this all along in play. So it looks beautiful. Yeah, so this is the other key when you're briefing in the DOD, you always have to have one of these charts and everything has to look like it was planned all along just like this.

[Laughter]

Dr. Porter: So, yeah. But, in all seriousness, we actually are pretty pleased with how things have come together. And, again, we couldn't have done this, frankly, without the support of FCC and NTIA who have been, they're working in, first of all, educating me but also

being supportive in saying, hey, we want to work with DOD to figure out how we work with industry to solve some of these really hard problems, particularly with the dynamic spectrum sharing. But this is a hard problem, by the way. It's not going to be something we solve tomorrow. But we have to be committed to do it. And we're just really thrilled with the partnerships. So there was a lot of conversation about partnerships earlier. I thought it was a little too neg...not negative but a little too gloomy. I think that partnerships are actually working very well.

The United States is not a centralized communist country. Thank God. And we shouldn't be. And we shouldn't get overly worried about how Chinese and other communist countries run their stuff. Because we don't want to become China to beat China. We have a lot of our own specialness that allows us to be truly competitive on a global scale. So we don't want over-centralization and really heavy handed, top down government dictatorial processes. And I think that's why the FCC has been so good historically is they recognize that, and they try very hard not to be too heavy handed as they, at the same time, put in the regulatory frameworks that allow us all to be successful.

The DOD is trying to come at that from a hey, we want to be collaborative with industry. We're not trying to be heavy handed. We are going to identify vulnerabilities that we hope that you will want to work with us to solve because we want to be able to use your stuff and therefore everybody is successful. But I'm not overly worried about, frankly, how China does their thing because we're not China and we're not going to be China. We're going to do it our way. And our way is the better way. That's just how I think. All right. So, one final slide. I did read your summary paper that was a summary of your workshop in March. I think it came out in June, but I will admit that I only read it a week ago in prep for this. It was really great, and Julian did a great job summarizing it. But I put this slide together in part to address, I thought, some of the things that were raised in there and some of the perspectives I would point out in response.

So many of the lessons we have learned with our current networks, I think, will translate to 5G. Things that have come up, like stronger encryption and as well as the improved privacy protection. The MC issue came up, you know, things like that. I think we're smarter now then we were when...ten years ago and that's good. And we should actually look at that and say, all right, let's leverage what we've learned and let's take those lessons forward. Now, we also should be recognizing, and this has come up and I was glad to hear this, 5G is really going to lead to our true convergence of all these different modes. The mobile fixed, wireless, and wired line which have historically lived in their little stove piped worlds, including their standard [inaudible 01:26:55], right. And that came up a little bit earlier. We have to move past that. This is going to be a truly converged system. And so our security solutions cannot be stove piped by mode. That's going to lead to a lot of suboptimal solutions.

So that's a hard barrier as was discussed earlier. Human nature being what it is. Everyone carves out their little turf wars...or sorry, I should just say their little turfs. But we have to recognize as a country that if we figure out how to collaboratively think about this as one big problem versus stove piped problems, we're actually going to do, I think, a really good job. Now, there are numerous attack vectors. And you guys talked about some of these all day today. From a true attack as opposed to things don't work right, the question that came up in the prior panel. Things like massive IoT DDoS Attacks, excuse me, against the RAM. This is one that you'll hear talked about a lot. It's kind of obvious. It's not obvious how you solve it, though. You have a lot of problems with end point security challenges, as well. That came up earlier. So there are things like that that we know we have to address. These are not the unknown unknowns. These are the known knowns, whatever.

[Laughter]

Dr. Porter: This is stuff we actually know we have to deal with. NFVSDEN just because I didn't feel like spelling it out. For those of you who don't know what that is that's Network Function Virtualization and Software Defined Networking Exploitation, is often raised as a concern. A lot of it is because NFV in particular is still new and we have to figure that out and how that's going to work and what we're going to do to ensure that we don't introduce too many vulnerabilities into that. And then, of course, a tax...this is something I always want to emphasize, a tax against the edge from third-party apps. We can't forget that software and third-party applications are still a huge source of vulnerability. People are really fixated on components and hardware and software is still going to be a huge problem. In fact, there was an article that just came out and I get these daily updates on all the articles.

And it is Federal something, it was one of these small...Federal Computer Networking Online, it was one of these small trade publications. It was about how the NSA identified that software is really the biggest issue we still face in cyber. So we can't forget that. We can't forget about the applications community. How we bring them in to our standards and bodies discussions, where are they in 3GPP? That's an open question that we need to think about. Then, the other thing I like to point out is that 5G also presents some interesting opportunities from a security perspective. Some of these came up as well and I'm kind of bullish on this, software defined networking, to me, also provides huge opportunities. Because if you do that right and you have containerized approaches along with AI, artificial intelligence machine learning in particular, techniques, you should be able to do real time monitoring and response. Most of the folks in industry are bullish about this too.

Now, it's not easy and there's a lot of work that has to be done here but it's credible to assume that that's a doable do. So there's an opportunity space here around really leveraging what [inaudible 01:30:13] has to offer, particularly when you combine it with machine learning techniques. So we shouldn't just look at the bad side, the scary side.

We should look at what a 5G really might offer as opportunities. With that, I will just close. The military, the message ubiquitous connectivity will maintain our [inaudible 01:30:30], that's one of our key takeaways. 5G is not a race, as I said. We really want to make sure that we're emphasizing 5G to next G, continually pushing ourselves all the way. Then, of course, 5G technologies are both enablers of and sources of vulnerability for our economic security, our homeland security and our national security. So DOD strategy is trying to leverage the strength of US innovation and that's what we're hoping to accomplish. So with that, I'll take questions.

[Applause]

Male 2: Thank you so much Dr. Porter for just a terrific keynote speech. When I hear this, though, I get concerned. We had a student here, very smart student, who put together a paper on the monoculture issue. That we're putting everything in the 5G basket. And if 5G gets sick, it spreads through all these different applications, all these different vertical markets and the Irish potato famine, I think, is a very clear example of what monocultures can produce. And recently Pierre found one in bananas. Apparently, there's one particular strain of bananas that everybody is using now and now that particular is subject to some sort of a root virus or something. And now it's causing major problems. That's the big headline issue that I haven't been around for quite a few years and uncomfortable about. There's people like Keith over here, a lot smarter than I am, he can probably express that more in the right terminology, but I have to confess, it does bother me deeply.

Dr. Porter: So I think, if I'm understanding your point, because I don't think it's really about bananas. I'm kidding you.

[Laughter]

Dr. Porter: Ubiquitous connectivity is a daunting proposition because when everything is connected to everything else then there is a huge problem. Right?

Male 2: But using a common 5G. It's the 5G... everybody using 5G for everything. From mart monitors to controlling valves up here in the dam above...it's the 5G. I'm sorry if I wasn't clear.

Dr. Porter: Uh-huh.

Male 2: It's the 5...total reliance on 5G that disturbs me.

Dr. Porter: Okay.

Male 2: If it gets sick.

Dr. Porter: Okay. Okay. Well, I mean, we have to face that reality, frankly. We're going to have to figure out how to address this realm that we're all marching toward. I'm not sure how else to answer that question or if it's even a question.

Monisha: So I I may just address that concern a little bit. I know that we are focusing on 5G here but in actuality there are actually a lot of modalities that we are using to connect these devices, right?

Dr. Porter: Yes, yes.

Monisha: Wi-Fi 6, we didn't talk about Wi-Fi much. That's the huge other parallel connectivity mold that we're all using. There is these low power long range methods that are out there which are not 5G which are alternative methods. Some of them are proprietary, some of them are standardized. Most of the low power health monitors are using Bluetooth low energy or they're using some other connected modalities. So, yes, 5G, they want to do it all, I don't know whether they will actually do it all. They do want to take over the world but I think all of these parallel methods of connectivity will survive and if a virus were to strike 5G, hopefully one of these other smaller systems can come in and come up with a new way of connected these devices together.

Dr. Porter: But I think it also goes to, and this is why I was struggling to answer your question, if you don't think about it ahead of time from an architecture perspective, how you deal with the reality of the more complex a system is, the more interconnected it is, you're going to open yourself up to a world of hurt. So things like zero trust architectures which are really about, how do I think about segmentation, network overlays, endpoint authentication, techniques. How do I get smarter about assuming, frankly, that that stuffs going to happen? And it's more about resilience. Assume bad stuffs going to happen, assume a part of my network may go down but the whole network isn't going to go down because I have alternative means of connecting. I think that's the mindset we have to bring to this. I don't know if that helps answer your question but I'm trying to pull out...make sure I'm addressing the right point.

Male 3: Funny thing about the Irish potato famine, there's a biotech potato that's resistant to late blight which is the virus that caused the famine. It's been banned in Ireland.

[Laughter]

Male 3: Because they don't like GMO's.

Dr. Porter: I really don't know what to do with that. But, okay.

[Laughter]

Dr. Porter: Go ahead. Thank you.

Male 3: Yeah. I mean, we could easily get caught up in analogies but there are...there's a reason why monoculture is the way farming is always done. Because it's most productive with all these benefits. And there's only one problem you have to solve. As long as our engineering talent is focused around the 5G and related standards then all those eyeballs can be put to work to make the system more resilient.

Dr. Porter: Mm-hm.

Male 3: And there's not a universal virus that can spread through the whole 5G ecosystem and destroy everything. That's not the way networks work.

Dr. Porter: Right, right.

Male 3: But there is an advantage to focusing our talents onto a problem that can become generally well understood. Right?

Dr. Porter: Yes, yes. Agreed. Agree.

Chris: Hi, my name is Chris McGillan and I'm a 2L here at the law school and one of the things I'm interested in is as you push forward new technologies like this, necessarily at the tactical level, the training objectives will focus to becoming very competent at that new technology and how to employ it. But then, by addressing that concern, you also talked about how at the deployed location, you won't actually have the network able to utilize the technology that you just trained to. So how does that DOD address the fact that the majority of your training objectives over the course of this life cycle that you're talking about, are going to be compromised potentially at the deployed location and so you're essentially putting time and effort and, theoretically, from the computer level, it'll be fine but at the person on the ground level actually doing the throttle work, that's going to be a very different thing. And so I just want to generally address that.

Dr. Porter: Sure. And remember, we have these problems today, right. It's not like it's a new thing to say, we go places and people are trying to keep us from operating. And we have network challenges we have today that the DOD has to be able to establish coms in areas where people are trying to keep us from communicating. That's just fundamentally true and will always be true. So the way we address that is we train as we fight. And that's why our training bases are so important. And that's why things like CBRS are actually such a big deal because it was kind of alluded to but the details around that are, the Navy needs that spectrum when it needs it to operate it's radars. And that's whey that was...and I think it was NTIA who brought up, you know, it kept her up at night to make sure that there wasn't any unintended consequences of sharing that spectrum. Because we train as we fight.

So we do think, always, about how we're going to operate in degraded spectrum arenas. So that's why, for us, dynamic spectrum sharing is so interesting because from the DOD side, we want to take that experimentation, look at it how we would do it in times of peace time, if you will, domestically but also how we would take those tools and techniques and use them in times of adversarial conflict. Right? Which you will no longer be sharing because they're not giving it...you know, they're not willingly sharing it. But, you know, we will have to work through that in order to ensure we can communicate in those environments. Does that make sense?

Chris: It does, yes. Thank you.

Dr. Porter: Okay.

Male 1: We've got time for two more questions.

Dr. Porter: Okay.

Joe: Hi, I'm Joe Kerry with Trimble. As I understood your slides, you're looking at 5G predominantly for logistical and that sort of thing not in the combat arena. If I understood correctly. Can you verify that or correct me?

Dr. Porter: So I think in terms of how we're collaboratively experimenting with industry, our first focus is in how do we accelerate our ability to adopt those capabilities for those kinds of examples you cited. Logistics, smart ports, smart bases, all those kinds of things that have obvious commercial analogs that people are talking about now. When we talk about operate through and how we might really want to understand dynamic spectrum sharing and take it further to dynamic spectrum, let's call it utilization, then that is absolutely about how we would operate in more congested and contested environments.

Joe: Yeah. But that won't be relying on the 3GPP 5G standard necessarily.

Dr. Porter: No. We're...yeah.

Joe: Okay.

[Laughter}

Dr. Porter: But, you know, but the dynamic spectrum sharing, right, where obviously we want to drive those...we want to be...and I think this is where the United States has an opportunity globally to be a leader and, of course, Julian, correct me if I'm wrong on this but I think in terms of how we approach that, if we can drive that then there will be standards that we drive. As long as everyone's collaboratively sharing. But the DOD's going to figure out additional techniques and tools, let's put it that way.

Joe: And so, a related question, I'm sorry, if I may.

Dr. Porter: Sure.

Joe: Is...so my understanding is that most 5G systems operate at shorter distances or shorter ranges than most 4G systems, although there may be some exceptions. And I would think that in your concept of operations, that poses a problem.

Dr. Porter: So I would say that 5G offers an ability to also introduce millimeter wave which does, of course, operate over shorter distances. And that's, I think, a feature. I think people are mischaracterizing millimeter wave. Actually, out there they are characterizing that as a bad thing but actually for many use cases both commercially and militarily, that makes a lot of sense. I mean, if I have a factory and I want to have an automated factory then I'm...I think it would be really great if I don't have to worry about anyone interfering outside of my factory. You can imagine how millimeter wave is extremely interesting to the DOD because we don't...you know, that gives an advantage. So I think it's actually a good thing and it's complementary and, again, Julian, you can comment on that, as well.

Julian: [Inaudible 01:42:32].

Dr. Porter: Yeah, it really is.

Julian: [Inaudible 01:42:37].

Dr. Porter: Yep.

[Laughter]

Julian: [Inaudible 01:42:40]

Dr. Porter: Yeah, I think it's worth it.

[Crosstalk 01:42:43]

[Laughter 01:42:47]

Julian: Oh, thank you. No. So a lot of folks because there's been so much focus on millimeter wave, which is a key component, think that's it, it's short range, it's not going to go very far. But it's actually...we've had this strategy of providing spectrum at low-band, mid-band, high-band. And the carriers have...are either deploying or have plans to deploy in each of them. So you're going to see...and what you are seeing is heterogenous networks...

Dr. Porter: Yes.

Julian: ...that combine each of these. So if I want to get out farther, I'm probably going to use the low-band for that. I may not have pound for pound as much bandwidth as I have higher up but...and that's why there's also so much focus on the sweet spot, the mid-band spectrum. Whether you're talking two, three years, so forth. So it's not just short range.

Dr. Porter: Right.

Julian: Because if you were trying to cover the United States all with millimeter wave it really wouldn't be practical. Sorry if I was jumping in but it's really...

Dr. Porter: I appreciate that.

Julian: ...important to understand that...

Dr. Porter: I think it is.

Julian: ...because it's not one band, it's not...it's going to be deployed. And satellite, as well.

Dr. Porter: Right.

Julian: And you're going to see flavors of it. It may not be...because 3GPP is even working on standards for device to device and so forth. So you're going to see lots of variations of this in different frequency bands and so forth.

Dr. Porter: I think that's an important message. That's why I wanted him to comment because there has been a mischaracterization of what 5G is about and it really is about all those bands and using the bands appropriate to the use case that you're driving toward.

Male 1: Do we have time for another one?

Dr. Porter: I can take one more.

Male 1: One more quick question.

Jim: So, Jim Dillon, I'm the IT audit director for the university here and I just wanted to check a little bit on the understanding of zero trust. I certainly applaud the concept. Things are not trustworthy in many cases. My understanding of zero trust includes a lot of data monitoring, AI assisted anomaly detection, behavioral norms, stopping things that are out of norm. So my question is, zero trust is one thing in a closed system, say like a corporate network, and quite another in a ubiquitous and open system. How does DOD pursue zero trust in the face of totalitarian concerns or the loss of personal freedoms

that may be promoted in a zero-trust environment where every action is monitored and possible recorded. Will that impact the ubiquity forecast?

Dr. Porter: Did you write that down ahead of time?

[Laughter]

Jim: I had to. Because I could have taken two hours to try and form the question correctly.

Dr. Porter: Do I think you're asking a really good question. Zero trust is obviously easier to implement for a network over which you have some sense of control. Now, you understand that, of course, zero trust is a response to historical approaches to do perimeter-based defense, essentially. And we're trying to drive people away from that. And a lot of it is also...it's not, you know, you can't just assume something is "trustworthy to be added to your network" because the person says they're trustworthy. Right? Or because, oh, well, you know, I've used this before so it must be okay. So a data driven approach is really fundamental. You touched on that. And that doesn't mean we've figured out how to solve for a completely open diverse system. To your point about imagine different devices and some we haven't even anticipated and they're not all going to have the same capability, blah, blah, blah. But from a mindset perspective, that's what we're trying to advocate for. And it does drive you to a different set of solutions and ways of thinking about it then if you say, I'm going to draw a perimeter defense kind of approaches. Right? That's what we're advocating for.

All right, well, thank you very much for your time and for staying as long as you did.

[Applause]

Pierre: So that was a spectacular end to a fantastic day. Starting with Julie through three panels. Thank you all for being here in the face of a storm. Just a couple of quick notes to close. The presentations are going to be posted on the website. There will be video, there will be transcripts. Two students, Chris McGillan and Greg Callahan are actually going to be writing reports so keep your eye out for that. We're going to move to the reception now so if you're a student and if there are still students, please make sure you talk to your practitioner. If you're a practitioner, please talk to a student. You will be getting e-mail asking for your feedback. Please tell us what we can do better and what you liked. The next Flatirons conference is in two weeks here. It is about entrepreneurship in rural America. 1:00 p.m. Thursday the 24th. Hope to see you here then. Thank you very much for being here.

[Applause]