THE BROOKINGS INSTITUTION

SAUL ROOM

# 5G IS SMART. NOW LET'S MAKE IT SECURE

WASHINGTON, D.C.

Thursday, December 15, 2022

PARTICIPANTS:

TOM WHEELER
Visiting Fellow, Governance Studies, Center for Technology Innovation

JOYCE CORELL
Senior Technology Advisor to the National Cyber Director, Office of the National Cyber Director

DAVID SIMPSON
Professor, Virginia Tech, Pamplin College of Business
Former Chief of Public Safety and Homeland Security Bureau, FCC

* * * * *

**Tom Wheeler** [00:00:31] Good morning and welcome to all of the hardy souls who have braved the weather to be with us physically today, as well as to the online audience and those of you who decided you could stay at home and not have to worry about the Washington weather. But I understand literally, I've had emails, I understand from, from Europe to Taiwan, we have people who are online today. So thank you very much for joining us. I'm Tom Wheeler. I'm a visiting fellow here at the Brookings Institution. And it was my privilege to be able to work with admirable Dave Simpson in developing this report, which we released earlier this week and are here to discuss. And we're honored to have the ability to discuss that with Joyce Corell, who is the deputy cyber director at the National Security Council at the White House. I'm going to invite Joyce and Dave up here in a second to fill these chairs, but thought that here at the outset, it might make some sense just to walk through a basic overview of what we said in the report and set the stage for today's activities.

We think that 5G is the greatest telecommunications innovation since Graham Bell said, Watson, come here. I need you. That was 1876. We're living through a period where we have two parallel activities going on. One is how microchips are in everything, and the second is the capability to connect those microchips so that you can get the added capabilities of data talking to data and creating new data. By one estimate that we quote in, in the report, by 2025 is it, it is expected that nearly 50% of all of the data traffic in the world will be without human intervention. It'll be machine talking to machine. And in order to do that, you need robust, reliable, secure communications. And that's the great opportunity that 5G represents.

But particularly for us Americans, 5G is largely misunderstood because what we know of it is what we see in the commercials on television and what we know about 4G and how we extrapolate to that kind of an experience. But one of the things that, what we were talking about in the report is that while 4G was about smart apps, principally for our phone, 5G is about smart everything else. And as these two forces of computing power and connectivity come together and connect, it creates the opportunities for smart cities, smart factories, smart cars, smart everything else. And that economic growth and international competitiveness depend upon our ability as a nation to exploit that technological capability.

But it's a situation where the stakes are high. It is different than the stakes in the 4G world, because what we're dealing with is the infrastructure that will define the 21st century, the infrastructure that will drive economic growth, and infrastructure that will give us international competitiveness. But in order for those good things to happen, that infrastructure needs to be secure. And that's why Dave and I wrote this paper. But we know 5G is smart. Now let's make it secure. Because the smart era requires high speed, low latency transmission. That's what the 5G breakthrough is about. But that transmission, those communications have to be secure. If you are the mayor of a city and you're looking at smart city applications of technology, you will be encouraged to do so if the network that connects them is secure. If you're the CIO of a company and you're looking at a smart factory or a smart warehouse or whatever the case may be, the security of the connections will encourage your adoption. And the inverse of those equations is true as well.

So let me make one stipulation here. Dave and I are 5G evangelists. But we were evangelists without illusions. That the promise of 5G, the technological breakthrough that 5G represents, the opportunities that it will create domestically and internationally are huge, important and not without challenge, especially in the security space. And that's why we wrote this paper. And what we pointed out in the paper was what we call the 5G paradox. That 5G, the thing that makes 5G special and different from previous telecommunications networks is that it is software-based and virtualizes in software the kinds of activities that used to be performed in hardware and as a result, it can do more things and do more things less expensively. So virtualizing in software is great and essential and a breakthrough, but we all know that software is hackable. So a great opportunity that we know brings with it new challenges.

The other thing that software enables is supplier diversity, that in the days when your telecommunication networks were hardware-based or hardware and software combined-based, you had Ericsson, Nokia, Huawei and a handful of suppliers who had a chokehold on that equipment. You know, when Google goes to buy a new server for its cloud server farm, it has a standard and it can buy from multiple sources, not be, not be wedded to just one supplier, which is like how telecommunications networks have been tied to one supplier. The fact that 5G is software has enabled that kind of concept to come into the telecommunications network so that, so that there are more suppliers, more innovation, more competition in the network infrastructure space, but that more brings other more, which is more risk. More suppliers, more potential attack vectors. More software, more potential of attack vectors. Using open source in that software, more attack vectors. And the people who need to make the decisions to embrace 5G and bring it into the domestic economy as well as those who might wish ill for domestic activities and international activities understand these realities well.

So we have to address these if we want 5G to step up to its potential. This is a headline from last week's Axios talking about the wireless infrastructure fund that the Congress created, a billion and a half dollars for the purpose of encouraging American innovation and corporate participation in the development of this virtualized new network. And as you can see in the headline, the supplier diversity that this creates, the Congress felt created an alternative to Huawei. But as we've discussed just a minute ago, supplier diversity and cybersecurity are not synonymous. And so we need to think beyond supplier diversity as we deal with the security of the most important networks of the 21st century. And so in that regard, Dave and I have made four specific recommendations for dealing with this issue.

The first is to understand that, to understand the nature of networks, you know, telecom networks are a bunch of independent networks that connect with each other. And because they connect, it means that the cyber hygiene in one can affect the security of another. So what we have to have is a baseline at the network level of cyber expectations, of knowing this is what everybody is doing, not to have a weakest link kind of a situation that creates an access point.

Secondly, that once we say, okay, this is everybody, this is at the network level, this is everybody, we know what to do. The solutions are already known. We don't have to go out and invent new things. That the National Institutes of Standards and Technology at the Department of Commerce, at SISA, at DHS, all have cybersecurity frameworks. The problem is that they're all voluntary. And that leads us back to the first issue, that if you have one part that's a weakest link, it's going to have a hard, you're going to have a hard time having cybersecurity across the entire interconnected network. We know what to do. We know it has to apply to everybody. Therefore, we have to have some kind of government oversight saying these are what the expectations are. These are what the solutions are. We're not going to micromanage like the old telephone utility regulation where you work about every, every detail. But we do want to have the ability to say, are you fulfilling these expectations? And to have reviews of that so we can, so that the agency, whoever is doing this, can learn and spread the learnings across everybody else. But we need to have some kind of light touch expectation that there will be common cybersecurity expectations across the 5G network.

And finally, because of the fact that it is a network that goes across the entire country, we are now spending tens of billions of dollars making sure that everybody in America has an Internet, a high-speed Internet connection. Because it is national security, there is also a very serious rationale for why the additional expenses associated with meeting these framework expectations ought to be a public expense. Let's establish what needs to be done, make sure it applies to everybody, use existing frameworks and make sure that it gets paid for. That's the summation of what our 53-page paper said. And now let me invite Joyce Corell and Dave Simpson up, and let's have a discussion about this and then we'll come back to you and folks online. Joyce, thank you for joining up. We could shake hands, too. Yes, the as I said, Joyce is the deputy director of cyber for the National Security Council.

**Joyce Corell** [00:35:26] I hate to start by correcting you, but I will.

**Tom Wheeler** [00:35:29] I would expect nothing less.

**Joyce Corell** [00:35:31] I'm, I'm in the office of the National Cyber Director, which is a new organization at the White House. It was created through legislation that's a little over a year old. I'm the Senior Technology Advisor to the National Cyber Director.

**Tom Wheeler** [00:35:44] Got it. Back to you. Thank you. I'm going to now really go out on a limb and guess that I know Dave Simpson's description as well, since I was fortunate enough to be able to work with him for almost four years. Dave Simpson is a retired Navy rear admiral, and I was fortunate to be able to call Dave a colleague when I was at the FCC, and he was the head of the Public Safety and Homeland Security Bureau, where he tried to introduce the concept of responsibility and security in, in networks in a, in a new and expanded way. He's currently at Virginia Tech. Did I get anything wrong?

**David Simpson** [00:36:29] No. Other than that, we've worked with Joyce extensively while we were at the FCC.

**Tom Wheeler** [00:36:34] Even before she was the, you know.

**David Simpson** [00:36:38] Joyce had a significant counterintelligence responsibility. And early on, we saw the challenge of supply chain and recognized that, oh, my goodness, in a significant part of the country, we've got hardware being implemented from a country that we weren't exactly sure about its intentions. So we early on set forth in motion what today is a very significant national effort to address supply chain risk. I'd like to pick up on where, where Tom left off. You know, Tom talked about the frameworks. It's important to recognize what the frameworks aren't. The frameworks are not prescriptive regulation on exactly how companies should do cybersecurity. They reference internal controls, but the frameworks are really a language, a common language to talk about cyber risk and what you're doing to address that cyber risk. And every company, every government agency defines their objective risk threshold, and it's never zero risk. You can't afford zero risk. That's unobtainium. And so it's that ability to talk about risk setting and where you are in achieving where you think your appropriate risk threshold should be, which is what we think is missing now from the 5G landscape.

There isn't that dialogue between companies, there isn't that dialogue with the responsible government agencies that are looking end to end across a fabric that has multiple layers to it and new market entrants that, that weren't there before. The cyber threat still exists. Right. We have malicious actors all around the world that still would do harm to our networks. We today have school districts that are wrestling with ransomware and can't access student records or have student records released. We have hospitals that have had operations significantly degraded because they've been taken over. We've had police departments that have actually paid the ransom to get their, their data back, but exposed personal information about citizens in the very worst of days for given citizens. So this is still a contemporary issue that 5G now brings a new set of risk factors.

As recently as last month Log4Shell occurred, and it is very similar to the SolarWinds attack before it. And it was an attack not on foreign code but on US code that was central to the operation of networks. It's how we log our transactions in the networks. Jen Easterly, who's doing great work, it's just a, oh my God, could we have I mean, I didn't think we could improve upon Brian Krebs, and we did. I mean, Jen is just doing a superb job, but she characterized Log4Shell as the most serious vulnerability she's seen in her career, and she's had a storied cybersecurity career, and that was just last month. Right. So vulnerabilities and the attacks, the exploitation of the vulnerabilities continues to increase. But Log4Shell is just an example, it's representative of what is a supply chain for software. Who wrote Log4Shell? I don't know. It's part of the, the construct of many, many modules that today make up the end-to-end capability in an environment where truly we have infrastructure that is code. That network functional virtualization that Tom talked about is infrastructure as code. And that software supply chain has a number of touch points from when the code is written.

Sometimes it's proprietary and you can very easily fix, oh, it's Microsoft. They're responsible for reviewing the vulnerabilities, issuing patches and helping to mitigate. Sometimes it's, it's open source. And there's a community of developers like Linux that contribute to the spotting vulnerabilities that weren't appreciated before and the rapid mitigation. Both of those two approaches can be made to work, but they both require that proprietary running of the software, prioritizing and then investing in this activity. And on the open-source side, a body of open-source participants that are regularly engaged. And as there becomes more and more open-source layers, you know who participates in what open-source review for code that goes all the way from a device operating system up into the now the, the operation of a software-defined network. So that increased number of layers that that 5G brings is is really important to understand because 5G ushers in not just a better smartphone experience— you can only watch a video so fast— but it brings in a machine to machine communication that really underpins what we think about when we contemplate the Internet of Things and its role in smart cities, in smart bases, in smart logistics, in smart vehicle, self-autonomous vehicles. And if we're to attain that, we really need to recognize the attendant risk of the introduction of multiple layers and multiple providers in that system.

It essentially brings the cloud, of which Tom mentioned, Google Azure, AWS, Oracle out to the edge. But that edge cloud could be one of the hyper-scalers, but it could be an enterprise that wants to operate a cloud at the edge. It could be a traditional mobile network operator. So that adds the complication of all this machine-to-machine traffic and protection of cloud. And we all know that the cloud, parts of the security could be great, but you can go to the cloud badly and people regularly do, the DOD, we went to the cloud badly and continue to have risk exposure there so that bringing alive machine to machine at the edge is a volumetric increase in the number of nodes and the traffic going back and forth between those nodes. And not all of that traffic comes back to a nice center where you can scrub it, clean it, make sure that it's cyber secure. Much of that is intended to take advantage of machine learning and AI that is then stored at that edge cloud, that 5G-enabled multi axis edge computing that is intended to sense, make sense and act. That's DOD parlance for for AI but it's really appropriate, right? It's having a sensor that says, oh, the temperatures too hot. I'm going to do something with it, increase the refrigerant. Or, you know, you imagine the automated function. But that low latency, tactile kind of response is now new attack surface and who's responsible for addressing the cyber risk in that?

We really have a national paradox today because we recognize that we're behind in 5G. We don't have the providers of much of the equipment and the software in many of the layers of that technology stack, we're catching up with other nations. At the same time, we're dealing with this increased cyber risk. And when Log4Shell happened, SISA's recommendation to companies, to communities was to reduce their exposed attack surface and translated what that means is that fewer nodes and reduced functionality at the edge right. At the very time we're wanting to catch up with 5G enabled IOT and smart cities. So we really from the executive branch and at the federal and state and local level but also company leadership have this discordant message where we want to be first to get to smart cities and to invent and utilize AI. But at the same time, we perceive still that we need to reduce our attack surface. And so that gap between those two messages is really what we're trying to address. It is saying, okay, that underappreciated cyber risk that an assigned cyber risk needs an owner, maybe it's multiple owners. And we don't think that the regulatory layer across the nation should be telling the industries exactly how to configure their intrusion detection systems or their zero-trust implementation.

But we do think they should be having regular discussions with the industry that they're responsible for, and from that, trying to motivate a self-identification of risk responsibility in the scenes. And where after a number of convenings, it's clear that nobody's stepping up to take that unaddressed risk in a particular scene, only at that point then go forward with increased regulatory activities to get to the point where we affirmatively address that cyber risk. And sometimes it's just a clear delineation of, okay, that part of the industry has, has cyber risk up until that demarcation, and beyond that demarcation, a different part of the industry has it. It's as simple as that.

Bring in O-Ran now and O-Ran has so many exciting pieces to it. Open source, radio-access network, right? It goes from the core to the distributed units to the radio units with a smart orchestration done through the radio intelligence controller. Right. How do you get all those different software piece parts to, to send radio frequency out to close communication, to bring that edge cloud alive. In O-Ran, it was perceived in the United States that this is an opportunity for us. We're behind in the appliances that Ericsson and Nokia and Huawei and ZTE and Samsung have done so well at, we don't have a U.S. provider of that. But we're really good at software. We've got Silicon Valley. Of course, we can use this to leapfrog into software defined networks. There is a lot to like about that, but we need to not look at O-Ran with rose colored glasses. O-Ran is not just a US thing. There are countries all around the world, including the incumbents, that are participating in the movement of the software that wasn't a fixed appliance out into open-source code.

In addition, there are entrants around the world that weren't passed, 4G, 3G, 2G providers that are very ready and, and delivering capabilities now in open-source code. And there are Chinese companies that are part of the O-Ran alliance. So we shouldn't look at O-Ran as yeah that's made in the USA right O-Ran has, has many authors and it's open source. The great news about O-Ran is you can change the instructions that go to the radios in a much more agile manner. It will underpin what I call the velocity of innovation, right? Because we're going to be able to introduce things called X Apps and Mac at the Edge and regularly improve the code base in a way that 5G really 4G in the LTE definition evolution imagine. But at the same time, we need to not fool ourselves. Right. We're breaking up the technology stack. There is potentially a different owner operator of the code at the core, at the distributed unit, at the radio unit for the rick who's operating the cloud at the edge. And all of those elements include risk scenes that need to be addressed.

So we think it's critical to identify those scenes and just regularly in a, think Agile and DevOps, right, you have sprints and that kind of a sprint tempo regularly be reevaluating, okay, where's our unaddressed risk? We think that this is a whole of nation effort, right. We know that 5G will underpin our smart cities, our joint, all domain command and control network. We'll use 5G technologies. We know that we want clean networks around the world, and we know that we want US leadership in the information economies around the world. So it should have a whole of nation response to address that. Current regulatory activities are very static in this case. Rulemaking is ponderous and, and too often when it comes, it's a bit of a sledgehammer when you really should have had a tweak early on.

So we're advocating an early and continuous engagement with 5G providers to identify those consumer and community risk factors. Who's speaking up for the schools that are compromised today? Who's speaking up for the, the hospitals and the police departments to then ensure that in the discussion addressing risk up and down that 5G stack, there is an advocate for that part of risk that is unaddressed. And finally, that, that agile, innovative DevOps kind of cycle for capabilities in the objective 5G architecture is buried up then with an agile oversight an agile regulatory engagement that seeks first and foremost to have this succeed and be a differentiated advantage for 5G capabilities from the United States.

**Tom Wheeler** [00:52:38] Okay, now. Dave, you and I have the great advantage that we're kibitzers, right.

**David Simpson** [00:52:47] At this point.

**Tom Wheeler** [00:52:49] At this at this point, at one point—.

**David Simpson** [00:52:52] We had responsibility throughout our careers.

**Tom Wheeler** [00:52:53] But that's, that's history. And today we get to kibitz about the people who are and make observations relative to the decisions that people in government have to make. Well, look at this. We have somebody sitting right here who is in that kind of the rubber meets the road, we've got to make decisions position. So, Joyce, you know, Dave just did a fulsome discussion of the kinds of issues involved. How do you deal with that in a, in a, in a in a policy environment?

**Joyce Corell** [00:53:33] Thank you for asking. So when you sort of opened up talking about 5G, the, the transition from 4G to 5G has been happening for quite some time now. And I think the average person often just hears a lot of marketing hype and doesn't really follow how the technology is evolving. So, you know, from a government perspective and you know how policy happens, under the previous administration, the government published a strategy for 5G for the nation. And that was very, very high level, but was intended to address security issues. And so over the years, you know, things have been, you know, thought about and launched. So more recently, things that are bringing attention to this space are actually being addressed right now in this particular administration. One of the things that our organization is responsible for is producing a national cybersecurity strategy. So this is, this is underway. And no surprise to anyone, it's a strategy for the nation. So it will include not just things for the federal government, for critical infrastructure and even address things such as cyber workforce development. So that is an activity that is underway.

So when you say, you know, who's going to be looking at security, you know, we will be convening the stakeholders in this particular space. You know, there are already government agencies that have very specific responsibilities. So you have the regulator, the FCC, and you have in the executive branch, the Department of Commerce, that has, you know, substantial responsibilities. In in this era, you maybe talk about risk and, you know, think it's this is about risk management, not risk elimination. And the threat landscape evolves over time. So we're never going to be in a, a perfectly secure state of being. So how do we then look at, there's no one solution, how do we look at the suite of solutions that can be brought to bear here? So I'm going to actually talk about a couple of those. After the SolarWinds event, the, the government got together and issued an executive order on cybersecurity that had a number of things, fairly comprehensive, and included in that were things that the government can do to shape industry behavior. You know, so when you talk about regulation, you know, that's only one tool.

So, you know, government in whatever and many different ways can shape industry performance through contract language, so the power of the purse. You know, so mandatory contract requirements that that require a supplier doing business with the government to demonstrate a level of security. But from my perspective, I thought it was interesting in this, at this stage of the game that these requirements are now fairly substantial and companies selling to the US, selling to the Federal Government now have to not only self-attest that what they have done, that what they have produced has been developed in a secure environment, but they also have to provide artifacts to demonstrate that, that the government will not take at face value, but you know, you know, test or, you know, examine it in some way. So this has also led to a lot of attention, you know, looking at the software supply chain and now requiring organizations to produce a software bill of materials. And in some cases, you know, just so that you can see in the items that had been procured, and then the telecom sector, as you described, when you have networks of networks and systems of systems, the cyber hygiene in one, if it's poor cyber hygiene can affect, you know, another, another system.

So with your software building materials, you then have insight into what is in a product or a system that's being procured. That doesn't fix, that doesn't fix any security problems, but gives you the insight to, in a faster way, identify when a vulnerability has been publicly disclosed more quickly, you know, how to, how to get there. And that speed, speed of action is an important element in in when you have software as infrastructure. That's one of the advantages of having software as infrastructure is that you can do things quickly. So software bill of materials, contract language. There's also a group that was created, was the Cyber Safety Review Board. So this group has convened once, and they looked at the Log4j vulnerability came up with a number of recommendations. So the Cyber Safety Review Board, it was modeled on the Transportation Safety Review Board where, you know, something bad would happen, there would be an examination and lessons learned that would then drive future actions, whether they, those actions take the form of, you know, improvements to technology or, you know, regulatory action. So, so we have now some, some entities in place.

Now, you had mentioned in your slides you pointed to the $1.5 billion from Congress. These moneys came in the Chips and Science Act, and the Department of Commerce, NTIA has the lead to look at this as a ten year, it's a large sum of money to be executed over a ten year time period, which is intended to accelerate innovation, you know with a priority for, you know, cybersecurity in this space, as well as stimulate competition, because having more, more competition helps drive improvements in a technology sector. So, you know, that's, our colleagues at NTIA are leading in that space. And parallel to that activity, Commerce, NIST, you know, has also been doing a good bit of work at the National Cybersecurity Center of Excellence, that's up in the Gaithersburg area. So this is a, at the NCCOE, they have a 5G— I'm going to call it a program or project— and this was an effort to look at security issues in 5G. They focused on a 5G standalone network just for the purposes of being able to manage this as a pilot project. And it's done in partnership with private sector companies who have come to the table with equipment and subject matter experts and then government experts from Commerce, the Department of Defense and other places.

So, so through that and through the testing, you know, establishing interoperability of among these different stakeholders, the objective in that pilot effort as this moves forward is to get lessons learned from a security perspective and then to begin publishing those things. So NIST has already begun, has already begun publishing security guidance for, you know, the breadth of the infrastructure, not, not just for the radio access portion, but for the core and other, other functions within, within the infrastructure. So, so they're doing that fairly quickly. And what, what the lessons that are learned will then be brought back into the international standards environment, to shape, shape that and improve international standards. So I kind of wanted to do sort of wave tops on some of those types of things that, touching on some of the things that you would mention.

As I said earlier, our organization is barely a year old and we were created, we were created by statute, so we have some statutory responsibilities and, and outcomes that were identified and, and we have some specific focuses. So one of those focuses on public private partnerships and another one is on resilience from a critical infrastructure perspective. So my director has come to, come to this, this role with a, a perspective and a vision about public private partnerships, having learned through, through a long and distinguished career, that collaboration isn't really about people sitting side by side and saying, you know, you work on this project, I'll work on this project, and you can do something else. That's not real collaboration. That's a division of effort. So real collaboration is when parties come together, and only by coming together can they derive unique insights.

So. So we will be looking at the different public private sector partnerships to say, all right, how does this play out? And how do we, how do we make that a model for all public private partnerships? And then from a resilience perspective, when the sort of the vision that's been espoused by Director Inglis is that when we look at the cyber, the field of cybersecurity and we think about, you know, where we want to go, we don't do cybersecurity for the sake of cybersecurity. We do it for a particular end. So with that in mind, let's think about what, what are the things that we as citizens or consumers want to do and how does technology enable that? So what is the society that we want to live in? And then let's have the technology get us there.

So in this context where you have mentioned, you know, schools suffering from ransomware or hospitals, the, the technology environment we are in right now is one where those who have to manage risk, you know, like the schools, those who have to manage— or consumers— who have to manage risk are those who generally don't have the skills or the resources to be able to do that. So how do we think down the road— and 5G is the great platform for thinking about this— how do we think down the road that to shift the risk burden to those who are more capable and better resourced to be able to manage that? So those are sort of the framing for actions that we will be taking going forward.

**Tom Wheeler** [01:03:25] So let's pick up on that last point that you just made. I mean, first of all, the other advantage that Dave and I have is that we get to look at a slice. You're looking at the whole pie and and we appreciate that and understand that. But let's go to the point that you were just talking about schools as an example. The fact of the matter is that 100% of cyber-attacks at some point cross over a commercial network. Right. Right. And increasingly, 5G will be essential to, to that, that network. The kind of public private partnership that you were talking about, I think, is very much where our heads are. Dave was, was talking in his presentation about the, the need not to micromanage, to do risk management together rather than the old excuse me, I'm the regulator, you are going to do this or there's going to be hell to pay kind of a kind of a situation.

Getting from here to there in terms of existing statutes, existing regulatory structures, etc, is no small task. So I would in fact invite both of you to comment on how do we get from here to there in the kind of non-adversarial, public-private, working together, but having expectations in this process? How do we get there?

**David Simpson** [01:05:15] Yeah, so the executive branch is, executive branch agencies have appreciated cybersecurity more and more and more over the last decade. Right. And we became so concerned about it in the various agencies that we said we've got to make sure it's being done. And we tried to incent this in a nice partnership way in contract language that said, oh, use the NIST framework and that didn't work. And we then went to obligations in a contract that said, okay, use the framework and these are the controls that you need to apply, and these are the certifications that you need to get. And so we've increased the barrier to entry appropriately, right, that you have to achieve this level of cybersecurity with these controls, and in that time frame, the defense industrial base has decreased. We've got companies, many innovative companies that are just opting out of being a part of that innovation ecosystem that creates that barrier to entry.

So I'm, I'm very concerned in that kind of trickle-down approach. Will this just let our good example of what we put into contract language at the federal level, it, it just hasn't trickled down to the states. I spent the whole summer with different well, most of the states, almost 50 of them, and their public safety communicators and they've got fixed budgets that, you know, aren't able to do the kind of contract obligations and oversight. So I think I love what you said, and it's such a shift, a positive shift in thinking about who should the risk burden fall on. We don't want this unaddressed risk to just devolve down to the consumer or to the community or to the public safety communicators. We should be intentionally looking at the markets that are bringing in these new broadband enabled capabilities and ensuring that as we bring in those new functionalities, that there's an expectation of addressing risk affirmatively.

**David Simpson** [01:07:39] Let me jump in for one second before, before Joyce responds to that, to do a warning to the audience that I'm going to be coming and see if there are any audience questions that you want to ask of this group. And so and there's a microphone will be walking around, but I'll be coming to you in a couple of minutes after Joyce.

**Joyce Corell** [01:08:00] So you're talking about, talking about shaping markets. So certainly we're looking at the cyber insurance industry, you know, to see what, what requirements the cyber insurance industry will levy on companies to get insurance. And when we talk about market differentiators, poor cybersecurity is a market differentiator, not in a positive way. So, so there are things that that we can look at to shape, shape behavior or, you know, beyond, you know, regulations. But this, this particular, and telecommunications underpins all different types of critical infrastructure. So as you, as you well know, there is a cyber regulators forum where all of the independent regulators kind of come together on a, on a somewhat regular basis.

**David Simpson** [01:08:47] Which was developed in the Obama administration. And Tom, weren't you the first chair of that forum?

**Tom Wheeler** [01:08:52] Guilty.

**David Simpson** [01:08:53] Yeah.

**Joyce Corell** [01:08:54] So, so, so this brings together sort of the energy sector, you know, and looking at the, this administration has placed a high priority on, on clean, clean energy. So there's a lot of investment going into that, that sector, as well as into other infrastructure sectors to—.

**David Simpson** [01:09:12] Harmonize risk approaches across that landscape of —.

**Joyce Corell** [01:09:16] Right. So, so what with the monies that this administration is investing domestically, we are looking to ensure that as those grant monies are issued, that there are cyber cybersecurity requirements that go with those, those funds.

**David Simpson** [01:09:30] And DHS has a state and local grant. Right. So state local governments today can seek monies from DHS to help jumpstart their cyber programs.

**Joyce Corell** [01:09:39] So, so those are those are ways to, you know, prioritize cybersecurity, that, that does have a trickle-down effect, ideally down to the schools. But we're also working at the state level. This is probably an organization, where you work at the National Association of State CIOs or State CISOs and just push across those states, you know, some baseline, baseline requirements. We will be looking at, you know, this, you know, we loosely say regulatory harmonization, but there will be things that we look at to see how are industries being regulated from a cybersecurity perspective to ensure that, that we have if there's a lack of, you know, a lack of cyber requirements in the regulatory regime, that, that they are introduced and this is at the, at the federal and the state and local level.

**Tom Wheeler** [01:10:29] So let's go to the audience here. Andy.

**Audience Member** [01:10:37] Andy Schwarzman, Benton Institute for Broadband and Society. I'm not asking you to get on the legislative Santa's lap and ask for a pony. But what is the bare minimum legislative response that's necessary, the absolute floor of what's necessary for 5G security?

**Tom Wheeler** [01:11:03] Well, what we suggested in our paper is that we need to have an agreement on the old, applying the old common law duty of care, which says that we'd have Congress say thou shalt apply the concepts of the common law, duty of care, which says that you must identify, you must take steps to identify and mitigate the issues that are created by the service that you are providing.

**David Simpson** [01:11:32] And in an anticipatory manner, right.

**Tom Wheeler** [01:11:34] Thank you. Yes. And, and, and that there needs to be that kind of you will have this responsibility, we are not going to specifically say thou shall then do A, B, C, D and E, but we are going to say that you need to take this new approach that Dave outlined of, of, of common expectations against proven standards and inspect what you expect as a great mentor of mine once taught me. And, and that's a new approach for legislators and regulators both and is probably in and of itself a Santa's life experience.

**David Simpson** [01:12:25] So I would just add to that floor that there should be an expectation of regulators, that cyber is a responsibility for them. And we have seen just in the agency we came from; the FCC commissioners say Congress didn't tell us that we have a cyber responsibility. Therefore, we won't address some cyber issues. And that shouldn't change from administration, administration from, you know, the party in power, Congress should make clear that in managing a market, in an information-based economy, of course, cybersecurity is an included responsibility for that agency.

**Tom Wheeler** [01:13:11] And it's in section one, Title one of the Communications Act. Any other questions you have got? Yes, sir.

**Audience Member** [01:13:23] Thank you for the great conversation. Andreas Kuhn Observer Research Foundation, America. And we talked a lot about and heard a lot about, about what should be state of the art kind of like, you know, where we want to go with this. But my question isn't I'm asking because it's, it's hard to get information on this. What's actually the state of practice in industry operators, manufacturers and so forth? Did you have insights into where we currently actually are today with that, as opposed to where we should go, which might help us maybe to focus some of those conversation on where we should start first.

**Tom Wheeler** [01:13:58] Are you focusing specifically on state of the art in the telecommunications industry.

**Audience Member** [01:14:06] I mean, or let's say practice. I'm curious what the telecommunication industry is doing at this point compared to where we are. Because I think the conversation we're having right now is where they should go. And I'm trying to get a better sense of where we are today.

**David Simpson** [01:14:19] Yeah, I'd offer that it's a range of cyber maturity across that landscape, and the large national operators are really good at cybersecurity, and they put a lot of effort into ensuring that your use of their networks is thinking about where would the next attack come from. But then there's a range across the mobile ecosystem of smaller operators that maybe don't have SISAs among the 1100 wireless providers across the nation to then the vendors and the downstream utilization of those network capabilities. And we're changing that landscape. We're bringing new players in that are smaller, that don't necessarily have that resource base that the larger companies have.

**Tom Wheeler** [01:15:22] Well, let's just add to that one other thing, too, which is new players. So AWS, Amazon Web Services announced this week that they're going to have a nationwide 5G enterprise offering.

**David Simpson** [01:15:37] Well, and AT&T has announced that their core will be will no longer be operated by AT&T but will be Microsoft Azure. So what are the responsibilities of these new players? Right. Does Azure then become responsible for a 911 call being made or a text to 911? When it doesn't go through, what's the responsibility of the cloud operator? You know, AWS is a great example. And I know many times where people using AWS have had their, their load in the cloud compromised. AWS is very clear, read the fine print, that AWS wasn't compromised, your use of the cloud was compromised. So that's an example where the risk responsibility goes gray. So an increased number of players, some with less cyber maturity and much gray space in that. Who's responsible for what aspect of risk?

**Tom Wheeler** [01:16:35] Joyce. You want to jump in there on anything. Should we go back to. Yeah, anybody else there back in the corner. Brett.

**Audience Member** [01:16:47] Thank you so much. Brett Hahn. A question for all three of you. Could you speak to the international dimension and could your role, your model and public private partnership in your outreach to other regulators be an effort that the U.S. should also lead and dialogue with other countries?

**Tom Wheeler** [01:17:06] Yes.

**David Simpson** [01:17:06] I'll take first hack at it. And I was fortunate actually, Andreas, it was with a, a number of us, including Palo Alto and high-end folks that were in the last administration, asked to do track two diplomacy with, with our Chinese counterparts. And in 2017, in their RSA, their major cyber conference, 5G everywhere. China has been thinking about this problem for, for many years and they've been thinking about it in an end-to-end way. So that 5G wasn't just there, they had the 5G ecosystem at the edge and they had municipalities and their regional version of a county that were all together planning what does that end-to-end cybersecurity for the use of 5G look like. Now I'm not suggesting at all that we have that kind of top-down directed government enforced, we're going to address cyber risk end to end. But that's kind of where the competition is.

Move over to Europe, GSMA and the EU have been very focused on affirmatively addressing cyber risk at the regulatory level. And the German cyber ambassador recently basically alluded— I hope I don't smash her words too much— but that addressing cyber as part of the regulatory process will be a part of their strength, the secret sauce in the EUs the implementation of 5G getting out to smart cities and use of AI there. So we have regulatory competition here and if we're going to have the US approach to 5G cybersecurity not only apply in the domestic market but be attractive in the global economy, I think we've got a lot of catch up to do to have a regulatory and oversight mechanism that is as agile as the innovative technology that we want to accelerate.

**Tom Wheeler** [01:19:33] Okay, we're down to our last minute. You get the last word, Joyce.

**Joyce Corell** [01:19:35] On the international, international front, you know, different countries come from different points in their history of, you know, where they're at to, you know, regulate a particular sector. So under the previous administration, there was a lot of engagement internationally. And the, the topic, the primary topic at that time was looking at the vendor lock-in that Chinese companies had with telcos all around the world and trying to find a different way to approach that. And starting with a vendor, a policy of vendor diversity or supplier, supplier diversity and working with allied nations and the IT sectors in those countries to make statements to say this, we, we agree with these principles of supplier diversity and cybersecurity. That has, that level of effort has in, in this administration now doubled where we have at the State Department recently this year was created a cyber bureau. So there's an entire line of business at the State Department that now focus solely on cybersecurity.

And we also have the financing instruments that the government has with USAID, Ex-Im Bank and others. They are prioritizing some of their financial aid, you know, for cybersecurity in the telecom sector. So, so we are playing a leadership role in this space, and we are actually, you know, bringing some financial horsepower to it. So, you know, can we do more? Yes, we can certainly do more. And I think from the engagements that we have had in my organization and with our counterparts in other, other countries, you know, there is, there is an interest in cybersecurity around the world. And we're learning from one another, what are our best practices in dealing with, with a regulator. I'm not sure that there will ever be, you know, harmonization internationally, and that would be something we just leave to markets to sort out.

**Tom Wheeler** [01:21:41] And with that, you get the last word. Thank you, Joyce Corell, for joining us today. Admiral Simpson, always great to work with you. Thank you. Thank you to everybody in the house here who braved the weather and to all of you online. And thank you to Brookings for the ability to do this kind of research and stimulate this kind of dialogue. Thank you very much, everybody.