The Potomac Institute for Policy Studies
VITAL Center Presents

5G Promises and Risks for US National Security

Potomac Institute for Policy Studies

Cover: Alex Taliesen

July 2019

NOTICE: This report is a product of the Potomac Institute for Policy Studies.

The Potomac Institute for Policy Studies is an independent 501(c)(3), not-for-profit public policy research institute. The Institute identifies and aggressively shepherds discussion on key science and technology issues facing our society. From these discussions and forums, we develop meaningful science and technology policy options and ensure their implementation at the intersection of business and government.

POTOMAC INSTITUTE FOR POLICY STUDIES
901 N. STUART STREET, SUITE 1200
ARLINGTON, VA 22203
703-525-0770
www.potomacinstitute.org

Contents

Image: Shutterstock.com

Executive Summary

The continued development of 5G wireless technology will be a disruptive game changer for the communications industry and the worldwide economy. The quantum leap in performance afforded by 5G will spawn new industries and novel applications within existing industries like autonomous driving, healthcare, industrial automation, and remote sensing. Countries that dominate 5G technology development will enjoy major economic benefits resulting from these advancements. On July 22, 2019, the Potomac Institute for Policy Studies and Venable, LLP cohosted a seminar titled: "5G Promises and Risks for U.S. National Security" to explore issues around U.S. employment of 5G for national security. The event provided a platform for insightful conversation around the approaching reality of a 5G-connected world and the security risks that must be addressed.

Issues surrounding the U.S. employment of 5G for national security applications include leveraging 5G for ubiquitous surveillance, mobile communications, secure networking, and more. Possible domination of emerging 5G technology by foreign national adversaries raises serious questions about national security. The subject matter experts at the"5G Promises and Risks for U.S. National Security" event emphasized the important new security aspects of 5G, the current state of the rollout for the U.S., and highlighted key items that need addressing going forward.

The event was moderated by Dr. Michael Fritze, Director of the Potomac Institute's Vital Infrastructure, Technology, and Logistics (VITAL) Center, which focuses on supply chain security and critical infrastructure resilience. The seminar began with an introduction from Ari Schwartz, Managing Director of Cybersecurity Services for Venable, LLP, followed by a keynote address from Robert Kolasky, Director of the National Risk Management Center (NRMC) of the Cybersecurity and Infra- structure Security Agency (CISA). The event discussion featured both Brain Hendricks, Vice President of Policy and Government Relations for Nokia Americas Region; and former federal government personnel to speak to critical infrastructure and risk management. The discussion compared the fundamental security differences between 5G and 4G technology.

Both government and industry must address such issues if the U.S. is to lead 5G technology. Supply chain security is an important area that requires more developed standards and policies, trusted suppliers, and technological understanding. It was pointed out that simply limiting a supplier to outside the network core misunderstands the technology, as 5G relies much more on processing at the network edge to deliver the faster speeds and lower latency. It has been reported that the average Internet of Things (IOT) network-deployed device is corrupted within two and a half minutes of the initial discovery of that device on a network. For national security, focusing on the "worst possible day" – rather than an "average day" – is needed to properly mitigate risks. The "5G Promises and Risks for U.S. National Security" implementation and security discussion revealed the need for more government investment in the 5G infrastructure to realize the timely rollout of a robust and protected 5G network.

Ari Schwartz – Introduction

Hello everyone, thanks so much for coming to our 5G national security event here at Venable. We're so proud to be co-hosting this event with the Potomac Institute. It's my pleasure to introduce the keynote speaker here today, Bob Kolasky. I had the pleasure of working with Bob in government. He is the lead for the National Risk Management Center of the Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security (DHS). He oversees the center's efforts to facilitate a strategic cross-sector risk management approach to cyber and physical threats to critical infrastructure. The center provides a central venue for government and industry to combine their knowledge and capabilities in a unique collaborative and forward-looking environment. The center's activities support both operational and strategic unified risk management efforts.

Mr. Kolasky's current position is a culmination of years of risk and resilience expertise. He most recently served as Deputy Assistant Secretary and Acting Assistant Secretary for the National Protection and Programs Directorate (NPPD) Office of Infrastructure Protection before it became the CISA Infrastructure Security Division, on November 16, 2018. While there, he led the coordinated national effort to reduce the risk posed by acts of terrorism and other cyber or physical threats to the nation's critical infrastructure including soft targets and crowded spaces.

Bob is a great partner to work with for everyone in government and industry, and he's shown that over the years. We're lucky to have him as a public servant, and now I'll pass it on to Bob.

Image: Shutterstock.com

Robert Kolasky – Keynote

Thanks for having me here today and the opportunity to talk to you all. We appreciate having any opportunity to talk about the imperative around security and resilience as the 5G network continues to evolve – and "evolution" is the word that AT&T uses in their commercial, so I'll use that.

Earlier today, Brian Hendricks, who's going to join us on the panel, was over at the Cyber Security Infrastructure Security Agency at the National Response Center. We host a "Defend Today, Secure Tomorrow" series meeting where we pull in experts to help us think through future security risks, evolution of trends, technology in geopolitics, and some of the traditional scenario planning activities. One can imagine the world going in different directions – certain things happening and certain things not happening. We consider the implications from a security perspective. How can we make sure that we shape the security environment as much as possible, to the extent it's possible, so that as we can take advantage of new technologies – as new things roll out and as the competition among nation-states continues to evolve? How can we do this in such a way that it leaves America in a better place than it was before, in terms of both increased economic opportunity and avoidance of too much additional security risk.

We invited a bunch of experts into the National Risk Management Center to go through a scenario planning exercise and work through some aspects. Michael Fritze also joined us this morning. I can think of no issue in a policy context right now that crystallizes the reason to do that kind of thinking more than the 5G network. This is technology that's going to hit us between now and the next seven or eight years; it's going to hit us relatively quickly, and it's going to create all kinds of opportunity. But it's also going to create new lines of security concerns.

Within CISA, through some of our work at the National Risk Management Center, we are trying to make sure that we can be a positive force for ensuring that the evolution and roll out of the 5G network happens as securely as possible, while ensuring system resilience.

My remarks today will describe our perspective on that issue and where we think there's opportunity for positive interventions so that the 5G network is as secure as possible. That's the way I'd like to frame my remarks, but before I go a little deeper into conversation about 5G, let me tell you a little bit about the National Risk Management Center.

The National Risk Management Center, as part of the Cybersecurity Infrastructure Security Agency (CISA), is a hub for planning, analysis, and collaboration for the biggest strategic risks facing the nation. We strive to conjoin analytic and planning capabilities and the ability to bring together representatives from across the interagency, federal government, state and local governments, nonprofits, and industry to work pressing strategic risk issues – again 5G being one example. We want to do this in an organized way by building from a concerted effort to analyze areas of critical infrastructure risk, consider how those might change, and determine where there are opportunities to buy down risk and create more security and resilience, ultimately for the purpose of national and economic security.

One of our first efforts was to define a set of national critical functions. These are functions of government in the private sector so vital to the United States that their disruption or destruction would have a debilitating effect on security. These critical functions include national economic security and national public health or safety. Reducing risk related to these functions is a national security imperative. We're trying to understand the truly critical functions, key dependencies and interdependencies, and the potential cascading impacts of threats. This will help us better locate pockets of risk that, from a national security perspective, are ones where we want to focus our attention.

The national critical functions construct takes the traditional critical infrastructure sector construct and turns it a little bit on its head and says, "It's not just about the sectors, it's about what it is that those sectors produce," whether it's generating electricity, the transport of key commodities, or the ability to run a financial system. What it is that they do, what are the contributing factors, and where are the opportunities? Where is the risk in that system? Where are opportunities to reduce risk so that we can be sure that those functions are going to continue to operate?

Some of the examples of specific national critical functions we've identified are things like position navigation and timing services, identity management services, radio broadcast and access services, and core communications networks operations. These examples are all publicly available on our website, as the 55 "National Critical Functions" we've identified. I use those as examples because those are certainly functions that have the greatest potential delivery enhancement through the fifth generation of wireless technology. When you look at the confluence of functions that are already crucial to our national security or national economic security, and the evolution and development of the 5G network, you see that those functions are probably going to be delivered in a slightly different way. They're going to have perhaps new sources of risk and delivery methods through the deployment of 5G. We want to make that connection when we talk about ensuring that the 5G network is secure. The 5G network is secure ultimately so that network-dependent functions – especially those that are national imperatives – remain secure. That's one of the reasons I think this is so important.

The essence of what we do and what we rely on is going to be changed in some ways through 5G technology. You all know better than I some of the statistics in terms of what 5G technology means. But it does mean that we're going to do things a couple orders of magnitude faster. There's the ability to execute a couple orders of magnitude faster with very low latency. Because of this, you're going to expand the devices that are connected to our communications networks devices, many of which are captured through IOT phraseology that rely on automation through the ability to have trusted communications, data use, etc. All of a sudden you see a whole new system architecture that is operating in a different way. It's our theory that as this architecture happens, there will be a new set of risks. But we want to make sure that those risks don't slow down the network rolling out in such a way that we can't take advantage of the wonder of the whole technology.

It's this mix of economic activity and innovation, and some thinking through of the national security risks that becomes important from a policy perspective. As we see significantly more data flowing and more things operating autonomously – which will allow more efficiency and effectiveness, whether it's transportation or agriculture – and with the ability to exploit data to make better decisions, you see some things that clearly we should be rooting for and that are very much in America's national interest.

We're going to have new innovation, new markets, and economic growth. It's going to be a wonderful thing, as long as we do it in a way that we're not creating too much risk or national security concern. That's why this is an important strategic issue. Within CISA at DHS, we are trying to understand those sources of risk. How do you both understand how the core and the edge networks are going to function? How does that change the elements of how you think about the overall security of the 5G networks? Where do the other components of network management go? More and more are going to go into the cloud. Are there new sources of risk as we become more reliant on cloud computing? What does the proliferation of software defined networking mean for security around software? We also consider questions about things like radio access networks and securing the small and micro cells deployed in communities to enable rapid process of information packets.

That's all changing infrastructure. Some of this is in place already and is helping us execute the 4G in other networks – but it's going to proliferate. It's going to generate more connections and more opportunities. Again, I've heard from industry in terms of understanding 5G risk, and it's going to create more opportunities to isolate and segment, to do things more nimbly, and to create redundancy; but it could also create connectivity risks.

We've been trying to work with industry, and have conducted our own independent assessment of where we think sources of risk originate. We've collected feedback, particularly through the sector coordinating councils in place for the IT – information technology and communications technology – and we published a risk characterization at the Traffic Light Protocol Amber level (TLP:AMBER). A number of you in this room have had an opportunity to comment on it, which is an overarching view of our thoughts on 5G risk and some opportunities to address those risks. TLP:AMBER means that there's a level of information protection on it. It's not a classified document, but it is a document that we ask is held pretty tightly within organizations that have a need to know. We're pushing to get an assessment out at the unclassified, fully TLP white level (TLP:WHITE) where it can be shared as a source of the U.S. Department of Homeland Security's view on 5G risk.

We think starting to understand the sources of risk points us in directions in terms of locating technical areas to better study those things. Specifically, where are there interconnectivity points and where, if you see the connections, are the national critical functions. These focus us to better understand the key components of the elements of risk associated with 5G. Then we can have a conversation about whether there's an opportunity at scale for the purpose of national economic security to make progress against those risks. That's how we're thinking about where we are in the process to get a better understanding of the risks and start to analyze and assess the risk, and to see the connection points between 5G, risk, and other things that we care about to make recommendations and bring industry and government together to take steps to address some of those risks.

I will continue my remarks with how we're thinking strategically about some of the key vulnerabilities as well as some opportunities of things we're already doing to address those vulnerabilities, and where I see some future opportunities. On the vulnerability side, as part of the risk assessment, we talked about vulnerabilities in terms of three things: logistical vulnerabilities, physical vulnerabilities, and technical vulnerabilities.

The risk characterization we released pulls out more in those areas, but what I'm talking about in terms of logistical vulnerabilities are those vulnerabilities delivered via manufacturing supply chains introduced by component parts of the 5G network that are either poorly manufactured or intentionally compromised or exploited via design flaws. This is where 5G risk management interacts particularly with some of the broader supply chain risk management efforts that we've taken across DHS, but we are increasingly looking for solutions to bring better information to bear, to put more trust into supply chains, and to enhance and incentivize better supply chain risk management across hardware and software components. For the broader Information and Communication Technology (ICT) supply chain, the President issued an Executive order asking the Secretary of Commerce to use special authorities to do that in some places, but there are areas where the Secretary of Commerce authorities are not the right way to approach supply chain risk management. At DHS, we're working with the IT and communications sectors to not only support assessment of where perhaps you want to use the emergency authorities that the Secretary of Commerce has in terms of rulemaking, but also in other ways that we can improve information sharing, information aggregation, risk understanding, and incentives for putting more trust into supply chains. That again is important across the ICT supply chain ecosystem. However, it becomes especially important if you think, as we do, that 5G is an important component of the evolving of ICT supply chains. How do we make sure that there aren't new logistical vulnerabilities introduced through supply chains?

Another area of vulnerabilities is physical vulnerabilities. That really concerns the idea that the 5G network greatly increases the core infrastructure of communication systems and particularly the proliferation of small cells that need to remain functioning in a trustworthy manner. So, again, physical vulnerability of the 5G network has many more access points with the cells and many more physical components that are going to demand a specific level of security.

Then finally, there are technical vulnerabilities. A lot of these are carried over from the 3G and 4G networks, where cyber security and cyber hygiene isn't at the level that you would hope and the nation-states interested in exploiting technical flaws will keep going until they find these technical flaws. Some of the flaws in the system existed through different generations or are potential flaws that existed through generations of communication networks. Clearly, the new system will introduce some level of new technical vulnerabilities. If you think about risk, those characterizations, and understanding vulnerabilities – there is opportunity to intercede in those three areas.

So, that's how we're thinking about it. We do recognize that components of those vulnerabilities could be escalated or elevated based on who the suppliers are within the system, who the manufacturers are of component pieces of the 5G network, and whether there are products that perhaps are less trustworthy. Even regarding physical vulnerabilities, consider maintenance by a trusted group of folks responsible for maintenance – are there intentional technical vulnerabilities or technical flaws in design introduced to the system? From a logistical perspective, where are the supplies produced?

That leads us to have some concern with suppliers who do business in China. It leads us to have some concern with companies that are beholden to government interest of China. That's always in a meeting like this, when we're talking from Washington in a policy setting – there's the question of where we fit and how we think about companies that are subject to influence by the Chinese government. Perhaps there are other governments that we don't trust as much as others, and we don't want to shy away from that. We want to be fair to those companies, but if they are being unduly influenced by a government who is trying to undermine American national interests, then we want to continue to look at that threat and understand whether there are system vulnerabilities that shouldn't exist, and are there ways to manage the associated risks.

I will end with a frame of some of the activities that that we're taking to help do what I said at the beginning is what we hope to do with the National Risk Management Center – catalyze, inspire, and organize activity to address those risks.

I will ease the organizing framework that was presented in the Prague proposals. I think most of you know that this spring, a number of a number of governments including the EU and NATO held a meeting hosted by the Czech Republic, in Prague, to talk through 5G security and recognizing that this is a global evolution – the businesses and companies that will be relying on 5G, that will help build out the network, and that will do business globally. It's important that there's some level of international consensus, particularly around like-minded countries and big influential drivers of economic activity toward the concerns around 5G and how to address it.

The Prague proposals, which the U.S. government signed on to, were a series of proposals around policy technology, economic levers and security, privacy, and resilience. I think that's as good a way as any to organize a set of activities that we need to take on, as the U.S. government, to advance the vision that I'm talking about.

One of the things that we're trying to do and organize, as the U.S. government, is involve the departments and agencies who have something to do to promote a secure and resilient 5G network. We want to ensure that we're working together and, as we hit the world internationally with our partners, to be certain that there's a level of U.S. government consensus, and that it's something we can drive as much as possible toward consensus with like-minded countries.

Most of our work right now regarding policy has been advancing policies on reducing risks to supply chains that will contribute to the 5G network. On the technology level, as we start to better characterize and understand risk and see sources where risk might be introduced into the networks, one of the things we're doing in CISA is to help better understand the technical vulnerabilities through establishment of some testing of technical vulnerabilities to get deeper and understand component parts. We're working with some of the vendors of some of the component parts of 5G networks to better understand their testing, sources, and understanding to validate some of that for our own risk understanding.

In terms of economic levers, one of the things I think the U.S. government can do is to use incentives to ensure that companies – that are based within like-minded countries, that want to do business in the space, and that have trustworthy security practices – are meeting a level playing field. For companies where we might have higher trust concerns – why are they succeeding in the marketplace? And are there incentives that can help balance that? And then, what can we do to encourage and incentivize different components pieces of a 5G network to allow for avoiding things like vendor lock and dominance of the system because you are the only player in there? I think there are some economic policy and trade policy components of this.

Then finally, on security, privacy, and resilience – I do want to continue to push, and hope that you hear my remarks for pushing a risk management perspective to this. Any decision that's made out of security, privacy, or resilience concerns is one that takes into account a proper understanding of risk and that appreciates that we must not engage in so much risk management that it stifles the rollout of the network and the associated innovation.

Continuing to have this conversation in both values, an economic construct, as well as a security construct as you determine the security decisions within it – I think it's an important element.

So, I will wrap up there and I think we're going to take questions after the panel. I've said this before publicly – I'm encouraged that we're doing this, that we're having this this level of conversation around town and places – such as the Potomac Institute and Venable. Getting people in the room now, where we still have some opportunities at the front end of the system to make real security progress, so that we're not just sitting here five years from now after we've created a whole set of national security risk that we didn't think through. It could be a couple years more ahead than we are now, but we're not playing total catch-up. I think that's a good thing, and I think that should be a model as we continue to go forward. Anticipate tomorrow. Anticipate what's going to happen, and get people in the room and start working the issues so that we're not just layering security on things, but we're thinking about designing security as we get it. Thank you.

Image: Shutterstock.com

Ari Schwartz – Introduction of Panelists

Let's call up the other panelists first. First is Brian Hendricks who's head of policy and public affairs in the Americas region to Nokia. Mr. Hendricks has nearly two decades of regulatory and legislative experience dealing with technology and policy issues in the private sector as a senior congressional staffer and as a law enforcement lawyer with the Federal Communications Commission.

Our other panelist is Tom, who retired from the CIA recently after 32 years of experience of service there. He served as the chief editor of the President's Daily Brief and other CIA daily production during the second term of the Clinton Administration and he spent the last 18 years of his career focused on cyber threats as a manager and senior analyst in what is now known as the Center for Cyber Intelligence. He served four years at the White House during the Bush and Obama Administrations, most recently as a senior director for cyber operations and for the National Security Council staff. During his last two years, he was a research director at the DNI Cyber Threat Intelligence Integration Center.

Lastly, I'm going to bring out Dr. Michael Fritze, who is the vice president at the Potomac Institute, and he's going to moderate the session and will tell us a little bit about of Potomac's work here. Thank you.

Image: Shutterstock.com

Dr. Michael Fritze Introduction

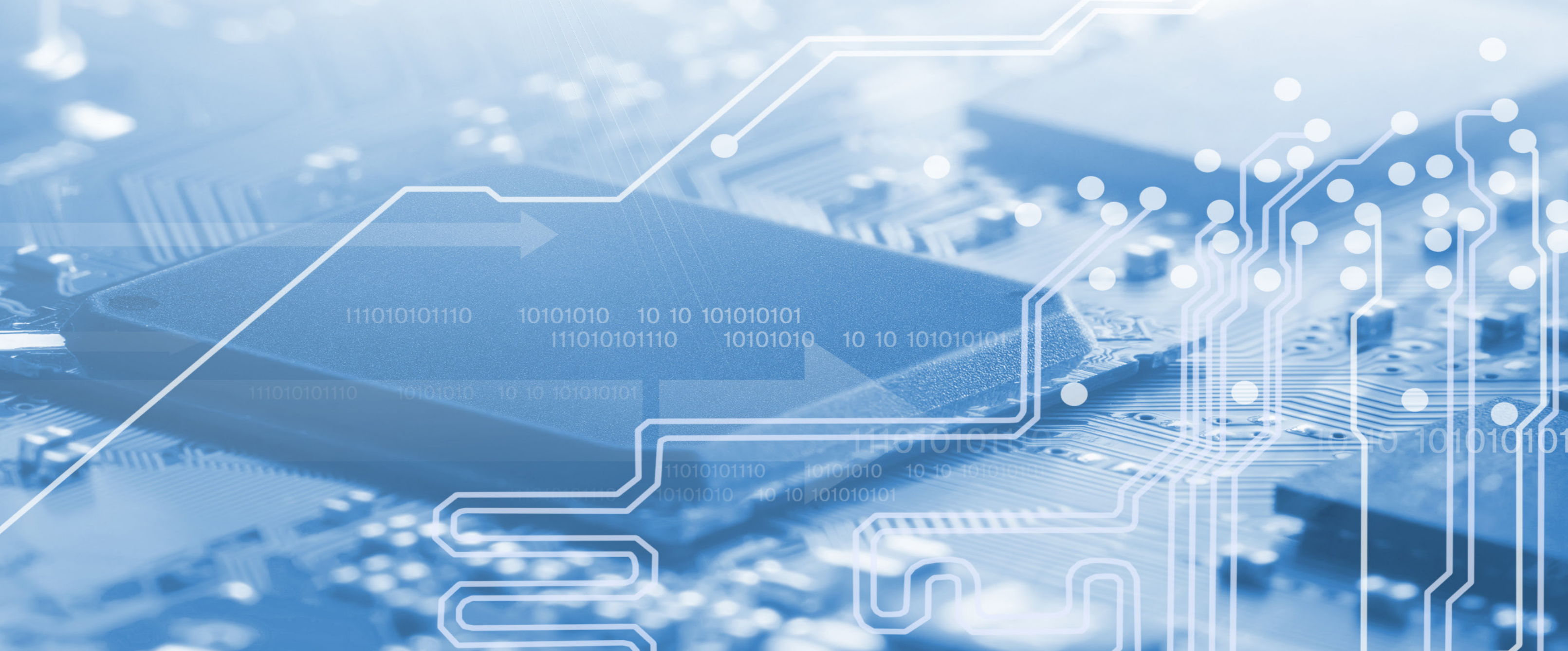
Thank you very much Ari. I want to thank both Ari Schwartz and Bri Law for the long-term, really very productive collaboration that the Potomac Institute and Venable have had over the years on policy issues that are relevant in both the legal perspective and to think tanks, so thanks, Ari and Bri. I hope we have many years to work together on these things – we are much more powerful working together.

Quickly, Potomac Institute is a non-profit, nonpartisan, independent, science and technology think-tank. Each word means something – I won't bore you with all the details but basically, we do strategic policy advice for government, often senior government officials, heavily the Defense Department, but we do a number of other departments, as well. We put policy ideas or alternatives in front of decision makers. That's kind of the one sentence summary of what think tanks do – in case people don't know.

I personally am a tech geek, so I've done technology and microelectronics for many decades. I've now been in the policy world for the last couple of years, so this is actually exciting and new for me and I get a much more diverse group of people, which is a lot of fun.

One quick word about why the Potomac Institute is involved with Venable on this. We have a number of academic centers – we have a Space Center, which recent held an event – we have some military centers, and we also have a Vital Infrastructure, Technology, and Logistics (VITAL) infrastructure security center that uses some of our security expertise in sort of a general critical infrastructure protection role. I manage the VITAL Center, among other responsibilities, and our job and what we've been doing in having events – and by the way this is one of a series of events that we're going to put on in this topic – is to do deep dives in critical infrastructure security and supply chain and extract useful policy relevant items that come out of those. So, don't think this event will cover everything – it won't. However, it will cover some really interesting perspectives.

It is nowhere near sufficient to have just one event so we're going to have a couple of these and distill the results that we have from them. With that, I will get out of the way. I'd like to let the speakers come in and make some initial remarks. We've already heard from Bob Kolasky at Homeland Security, I think Brian is next for the opening remarks, before we proceed to hopefully a very vigorous panel discussion.



Brian Hendricks – Opening Statement

Thank you to both Venable and Potomac Institute for the invitation to come here and speak with you today. I was fortunate to come and speak at an event between the two entities last year and had a very good time, so I'm very eager to be back recognizing that we are just one panel among a series of events.

What I thought would be most useful for me from the vendor perspective is to make sure that we have a grounding for the ways in which 5G is different. Part of the reason for that is that as we travel around town, and indeed internationally, some of ideas that have been cast about fundamentally misunderstand the ways in which 5G will be different regarding appropriate security approaches and assumptions about security approaches. We think that some of these ideas are based on a backward-looking understanding of LTE and 3G, and are not accurate.

So, you have heard that 5G is different, but it really truly is. It's different in a number of ways. It's different in its architecture. You already heard Mr. Kolasky talk a little bit about the use of both macro cells and a huge amount of small cell infrastructure for densification. Software defined networking, which has some implications for how you can mitigate risk – particularly when, as I'll talk about in a few minutes, you look at issues like post development testing and certification, which have been suggested, and how that can be a logistical challenge.

Different capabilities, for sure, and also a different and exponentially larger potential attack surface – what cyber folks talk about as the attack surface, which is kind of a cool phrase – but I'll talk a little bit about why the attack surfaces are much greater.

A third way in which 5G is different is that because of what it will enable, and I'll talk a little bit about this in a couple of minutes, and that for previous generations of wireless, the primary driver was the consumer use case with voice, text, and data as the objective. Although, with advanced LTE, we did start looking at enterprise applications.

The truth is that for a variety of technical reasons, what we were able to do, the use cases that we were able to support based on spectrum, and equipment that was available meant that it was primarily a consumer demand-driven focus. We will now, in 5G, have far more capability, which will invite entire sectors to utilize the wireless infrastructure – everything from connected healthcare, connected car, autonomous driving vehicles, etc. – so what you get there, with the introduction of significant utilization by new sectors, is a different target environment than what we had in previous generations of wireless.

The good news is that we have been aware of these challenges for some time and we have spent considerable time addressing previous weaknesses. It's not like we started a year ago in the standardization bodies, for example, talking about security. We've been having these conversations for four or five years. Conversations about where we left holes in LTE, as an example, and things that needed to be done differently to address that framework.

We have identified ways to use prior approaches and prior tools, that I'll talk about in a couple of minutes, but we also recognize the need for additional approaches and tools given the different threat environment.

I already mentioned that we were looking backward, primarily building for a consumer use case, but you know compelling use cases, like networked hospitals – think about sensor-based technologies to attract employees and equipment, connected infrastructure, and even connected cars were supported technically. But, as I mentioned, we couldn't scale those up, given the limitations, capacity, and latency in LTE networks. So, a lot of the demand for that has been spinning up and queuing up waiting for advancements in technology – mostly in the radio layer and changes in spectrum allocation, frankly to give us much larger channel blocks so that we're going to be able to have really high throughput through the radio interfaces. The radio is no longer going to be a bottleneck.

We're going to move quickly from speeds that can top out at 100 megabits per second, which is pretty high for LTE, to initial speeds of 1-2 gigabits per second and scaling up to 10-20 gigabits per second. So, you're going to see initially a 10-fold, and then eventually many times that, increase in the amount of throughput. But, also, latency – which is an important driver – will move from 40-100 milliseconds per network. It's even higher in cable plant down to one second or less.

So now you have high reliability, high throughput, very limited latency, and a whole bunch of new use cases that that are possible at scale. But, a lot of those will make use of IOT devices that Robert Kolansky identified. One thing to keep in mind is that another key difference between 5G and previous generations of wireless technology is that we had a limited number of device makers in that space. Not all of them were of the highest quality, but many of them – those that are the most widely used by consumers – have heritage and experience with developing secure devices.

We will have many new players with very limited experience in device security introducing often very inexpensive IOT devices. Our threat detection and mitigation Center for Nokia – this is a public report that people can look at – among other things, identifies that today the average IOT device that is deployed on a network is corrupted within two and a half minutes of being discovered for the first time on a network. When you consider that you're going to have many billions of less-secure devices on a network, presenting both attractiveness for the data purposes but also for recruitment into huge

image: Shutterstock

bots with a capability set that will dwarf what we have seen to date. The new sectors that I mentioned including transportation, utility management, health care, and infrastructure maintenance will be making heavy use of the networks and creating higher value targets. The bottom line is that lots of new capabilities are coming at us, but also some significant risks that we need to be prepared to address.

So, "What can policymakers do?" is one of the things that we are asked, and I will talk a little bit about some things that we're not particularly supportive of – that we hear being talked about – that we think yield a pretty minimal security dividend. But there are some things that we think are good approaches, some of which are already underway. We think that the conversation needs to be grounded in the actual vulnerabilities and knowledge of what 5G is and how it's different – which is kind of why I started where I started.

Now policymakers must insist upon trustworthiness and security from all sectors. Equipment and software suppliers and device makers with the heritage and reputation for security are going to continue to play a big role in 5G, and that's the good news. The bad news is there's going to be an influx of new component makers; device makers; software suppliers; and even in some limited niches, network equipment suppliers.

In pursuit of security, one of the hallmarks we believe needs to be fairness and consistency in government policy and enforcement. Companies like Nokia, with our 154-year heritage of ethical conduct and compliance, are often at a disadvantage when we face competitors who show less fidelity to domestic rules and laws. As one example, I will point to the recent headlines about the Commerce Department's decision to enforce its export control regulations against a couple of companies in the last two years. I'm sure you can guess which two companies I'm talking about – but these are predicated on systemic long-term violations of U.S. export controls and sanction rules. Rules that the rest of us comply with at great cost, at great expense, and often at great disadvantage because while they do a wonderful job, it can take many months to get those licenses depending on the complexity of the licenses that we are seeking. So, it confers a time to market advantage upon those who compete with us. So, when you have identified entities that have serially violated these rules, it's important that you actually follow through on your sanctions. If you ameliorate penalties without first insisting upon changed conduct and behavior – it, in effect, rewards the behavior. But it also provides absolutely no incentive for a change in behavior prospectively, and it restores those competitive imbalances. Asymmetric expectations and rules that impact the competitiveness of lawful companies that don't cut corners is going to compromise security.

So, let's be consistent and let's be fair. Simply put, a threshold element of establishing trustworthiness in your supply chain is insisting that the entities that supply your critical equipment and services behave in a lawful manner every day, and that they're punished when they don't.

Following the law is just one element of establishing trustworthiness, and the other is transparency. It is fair and it is reasonable for policymakers to ask all suppliers of critical equipment and services about ownership and governance, including the manner of decision making that includes supply chain management, and methods to mitigate against risk. They're tough questions to answer at times, but they're important questions. We think that those are important conversations to have. Unfortunately, a lot of times – and it's not necessarily the U.S. – there will be a critique of our supply chain, and we will be told, "…and here's what we plan to do about it," as opposed to asking, "So if we have concerns about where you source components, here are the components we're concerned about and here's why we're concerned about them, and what programs do you have in place so that there can be an exchange?" Because where I source mounting harnesses and screws is not a matter of national security.

We need to have a more precise definition of what we're concerned about – is it intelligent components? What are those? Is it software development? What programs do companies have in place to ensure the integrity of software development? This may mean that where you develop it is less important than how you develop it, but those are fair conversations, and vendors and service suppliers need to be prepared to answer. Then we can have a comparison and an effective dialogue on how to address those concerns.

Simply asking us to move the supply chains is not a reasonable approach at this point, particularly not when you want the deployments to continue. But, I am encouraged recently, particularly with the U.S. government approach to understanding supply chain risk. There are a lot of things, in addition to insisting on transparency and security, that we think governments can do. One is to increase and improve, particularly U.S. government, participation and standardization.

We've heard a lot of discussion about the Chinese increased participation level in standardization – which we don't think is necessarily by itself cause for alarm or concern. When you consider that four or five years ago the conversation was, "Geez they're not participating in standardization," and we looked like we might have regional approaches to defining standards, which defeated scale and created a whole bunch of other problems. If the concern is the sheer volume of participation, then the answer isn't to expel them from standardization – it's to find ways to increase the participation rate among U.S. entities, which has sagged considerably.

We have very limited participation from auto OEMs and other vertical industries that are going to be

image: Shutterstock

heavily dependent on 5G technology, often because they haven't seen the need. In some cases, we also see very limited participation from small and mid-sized companies. One reason for that is obviously the cost of obtaining the voting rights for places like 3GPP.

So, one of the suggestions that we've made to the administration repeatedly is to find ways to reduce the cost of participation and standardization, whether that's through favorable tax treatment or direct engagement with the accrediting bodies to get them to tier their membership so that smaller entities have an opportunity to participate. But also using NIST and other government participants to convene dialogues post- and pre-plenary sessions to compare notes and make sure that what we get at the end of the day are still the best engineering-based outcomes from standards bodies.

We also think that there needs to be an implementation of a framework for recognizing companies with superior security records. As Mr. Kolasky said at the beginning, to incentivize others – particularly those who are new to the space and don't have heritage here to adopt and follow those best practices. Part of that may mean providing funding for training, particularly for smaller network operators and IOT companies; to improve the security departments and practices; and to expand the tools that they have, because they can be very expensive. Particularly since we often see a situation where a standards body will produce strong recommendations and build to comply with the standard. But, not all operators will implement the full toolkit of security provisions that have been developed. The large ones can speak for themselves regarding why they don't do that in some cases. The smaller operator simply might not be able to afford all of the features, so there's an opportunity to look there.

But at the same time, we have seen some suggestions that we don't believe are appropriate. We don't think that they necessarily yield a security dividend, but they may yield a political dividend given the nature of the current international conversation. One suggestion is building expensive security centers for post development testing and certification, as we have seen done in Canada and the UK. What we would tell you, based on our examination of the reports coming out, is that their utility is fairly limited. They've been quite effective at finding quality deficiencies, but even their own reports indicate the difficulty in keeping up with the volume of updates or producing remediation.

5G will be different in the amount of software that will be driving a network. Gone are the days where you'll get a once a quarter or once a half release updating the technology – these will be weekly and, in some cases, they might even be nightly.

The idea that we can build a pre-deployment testing regime without causing significant issues and deployment of needed software upgrades is very difficult for us to imagine. We have no trouble with the concept of sharing source code and taking a look at those things after a deployment. But, it has to be taken into account that 5G is going to be different, and that type of regime has significant limitations.

Network segregation is another concept that we have heard kicked around a lot. While realizing that this may sound completely self-interested, we've had some difficulty understanding some of the suggestions – that if you don't trust a particular supplier or multiple suppliers, you can let them in one part of a network but not another. We think that fundamentally misunderstands the way that 5G is architected and will ultimately operate. For example, it is our belief that a lot of traffic is never going to pass through a core in a wireless network in 5G. It's all going to stay at the radio layer in a particular region. As you have more and more infrastructure and services communicating with one another – and even if that weren't true – the idea that having a trusted supplier in the core could be a miracle cure for vulnerabilities deliberately introduced into the radio layer seems, to us, unsupportable from a technical perspective. The key servers for encryption are hosted in the core, but anyone who is in the radio layer – who has interest in intercepting those keys by virtue of being there – would be in a position to do that and potentially cause problems with the integrity of the radio layer security.

It's also important to recognize that as a standard practice in telecommunications networks, we don't encrypt all the way through a network. We encrypt between the user and the radio plane, but often not throughout the network.

So, what happens at the radio layer is pretty important, which brings us back to the question: If you have reason not to trust someone as a supplier, not because they're just having poor quality, but because you actually fundamentally don't trust that supplier has the best interests of the ecosystem in mind, then it's probably best not to allow that supplier to be deployed at all. That would include Nokia if you don't trust our abilities to do things.

Lastly, I would just like to say that having spoken about the ways that 5G will be different, we think that there are nevertheless a lot of very constructive things that can be done. I've talked about insisting on transparency and recognizing and facilitating best practices; providing resources for training; and the increased role in standardization, particularly to make sure that standardization continues to address security concerns in a very timely way. I will say this about standardization – in previous generations, security was handled, but often not as the highest-level priority compared to dealing with other aspects. In 5G, it has been prioritized to a much higher degree. However, continuing to insist on identifying issues and pushing them through development and release is extremely important. And with that I'm happy to address any of the questions that folks have.

image: Shutterstock

Tom – Opening Statement

I'd like to play along a little bit on Brian's comments before I launch into what I prepared, which is on the inspection regime. I think that's a failed concept, just from the point of view that not only can you not find the problem in the thing that you're looking at, but in fact you actually have to look at every single piece of equipment that's going to be deployed. Who's to say that the thing you're looking at has anything to do with what's going to be deployed? In fact, that's one of the problems the Brits have had – version control – everything keeps changing.

Another issue here is this notion that we're fundamentally talking about a lot of software, but we're also talking fundamentally about hardware, which brings us back to the trust issue. We're really talking about the actual root of trust. If you look back at industry experience through the trusted computing group and whatnot, I think industry has consistently found that if you don't trust the hardware, you're doomed. Then, when you consider who's going to be in the best position to cause you a problem, you need to look at the individual components. It's not the most productive place to be evil. The best place to be evil is to be the integrator.

So, you really need to trust the person who's pulling it all together because a lot of what is going to be the capability that somebody might use against you is in fact going to be the features that are built into the system. It's just a question of steering the features to a particular purpose on a particular time period that you may not have anticipated in your initial deployment.

Then, of course, there's the issue of updates and whether or not an inspection regime would actually keep up with every single update – never mind, God help me, nightly. But anyway, the notion that you could have a bunch of features pre-position and then there's just one final update – which by itself looks just fine if you don't understand how it will interact with all the features – isn't a problem. That keeps bringing us back to this notion of trust.

One question I have that I don't have an answer to is, to the people who are asking, "Can I have a little bit over here that may be touching the network?" What is it from a security question? That's one thing people need to understand. What does even a small footprint within your infrastructure give you in terms of being able to reach across and impact across the entire network?

Is it enough to be able to touch what you might think of as a signaling or control plane? In other words, into the trusted communications that are occurring across the management of the entire network – is that, in and of itself, already a problem? And now you're just using other people's features to do whatever you want to do.

One last technical comment, which is to reinforce what Brian was saying about the edge versus the core issue, which is latency. How do you think they're going to get one millisecond of latency? It isn't going to be by going all the way back to the core; it's going to be about having all the intelligence distributed everywhere across the edge. That's why the edge is going to matter and the notion of keeping somebody out of the core is just nonsense.

I'm a former government person and I'm primarily, in some sense, speaking to my former colleagues who remain in the government – this is not a new issue. I'm thrilled that we're having the conversation now, and not five years from now. But you know, we should have had this conversation five years ago, actually ten years ago, in my view. In fact, there were conversations, but it was just too hard to for government to look too far ahead of a problem. We just don't do it – it's like, "No, what's today's crisis," "What's happening next week," – never mind five or ten years from now, but here we are.

A lot of people say that it's too late. 5G – it's all set. The market is set. The standards are kind of set, and "It's just a question of rolling it out now." Well, I disagree with that, too. I think this is something that's going to take time to roll out, particularly in terms of how it's going to manifest itself across our entire infrastructure. We have time to make some decisions, but at the same time, in fact we are on the edge of the cliff and there are people who are making it very hard to revoke decisions about the baseline pieces of the infrastructure. So, if we're going to do anything, we bloody well better do it now. I sure don't want to be coming back ten years from now and having this conversation about 6G or 7G or whatever we're going to be talking about then. Let's get our minds wrapped around this now.

Originally when this conference panel was set up, there was supposed to be somebody from DoD here. So, I'm going to channel the DoD person a little bit today. I'm representing only my view – I'm not representing DoD's view in any way or any other part of the government. I'm just a former old guy lamenting the failures of his career, now. So, here's the thing – a lot of the conversation that we're having around 5G right now has a very domestic, U.S.-centered focus to it. In my mind, that's already the wrong conversation. This is a global conversation. The reason it's a global conversation is because we, the United States, are a global power. We, the United States government, have a responsibility to the American people to be able to project power to protect U.S. national interests everywhere around the planet.

So, to have a policy that successfully keeps Huawei or anybody else out of the U.S. marketplace is insufficient. I need to have resilient command and control all the way from here to anywhere. And, if I have to go through somebody else's equipment that I don't trust on the way, I've got a problem because it's probably not going to be there for me. Which leads me to the second point, which is a lot of this conversation – espionage. Okay, I get it. Lots of opportunities, I think Brian articulated those, yes. Brian will not give you end-to-end encryption, but you can give yourself end-to-end encryption. You should be doing that anyway so just get on with it.

I recognize that, again, there will be all sorts of other interesting things that can be done in terms of watching traffic – even if you can't read it, and you can think about who's talking to whom, and all that kind of stuff. It's great to worry about all that. But from my point of view, the thing I'm worried about is not every day. I'm not worried about the routine day. I'm worried about the "worst day." This is what the taxpayers pay the American government to think about because nobody else will. Nobody else can. Nobody else can afford to – and that is the worst possible day.

When we are in a strategic conflict with a pure adversary our communications need to work across our nation through our critical infrastructure as we mobilize, and we need to be able to talk reliably to all our forces anywhere in the world. So, this is not even just a 5G issue, this is really about what is our strategy for having resilient communications, end-to-end, edge, core 5G, 6G, 4G – I don't care whatever it is. It's all got to work.

So, we have satellites, maybe. Not on the worst possible day. We need to think about that. Do we have the right mixture of stuff to do what we need to do? If you step back and say, "Well what are we doing here in the U.S. government about this?" I think there are some areas we could improve, primarily in the government. We like to talk a lot about innovation. To put it relatively lightly, we somehow don't feel like we're meddling with the market. We don't feel like the government is being seen as meddling in the private sector in an inappropriate manner.

It's like, "Yep, ok. I'm great on the innovation thing." But if you consider how the U.S. government, is supporting innovation, I would argue it is very unfocused. It has no particular purpose to it, and it tends to be way over the horizon somewhere. It has absolutely no focus on helping what's going on in terms of our current day problems – in terms of what makes up our infrastructure.

Consider what's going on in the private sector in innovation. Nokia and Ericsson are dumping lots of money into their research and development (R&D) at a very healthy percentage by any standard. But guess what, their budgets combined don't equal the amount of money that Huawei is putting in today, and Huawei has already said they're going to put in more.

I think there's an opportunity here for the U.S. government to think harder about what we're doing in terms of innovation for critical infrastructure such that it will be reliable, secure, and serve our purposes – maybe to help mitigate in an untrusted environment. But better yet, to help us and help industry get to the point where they in fact have an advantage and can compete in the marketplace using the best possible technology.

I would also note that if you look in Europe, there is money. I believe Nokia is getting a big grant from the EU. It's like a type of loan. They put $500 million down, and that's still chump change. Huawei is putting in numbers on the order of $15 to 20 billion a year into R&D. So, $500 million over five years is chump change.

What the U.S. government needs fundamentally is a comprehensive, systemic approach with a roadmap to thinking about this industry. We're very reactive. We keep hoping for certain things to happen, like emergency preparedness that will have priority when we need it, and so on and so forth. But it always comes down to, "Hey industry, by the way, that thing that you've built – is there anything you can give us for free? I'd surely like to have some." Okay, I'm exaggerating a little bit here, but I'm trying to make a point.

I would say, "No," We need to be looking ahead. We need to be thinking about how the architecture is going to support our national needs domestically and globally, and we need to have a plan for how that's going to work. To do that, in part, we're going to require a much more sophisticated understanding of the market and what drives us than I tend to see at least during my career within the government.

Here in the United States, we have to ask the question, "How did we get to where we are today?" We had industry, that was so-called U.S. industry, and there's an interesting question. What does that mean for U.S. industry, nowadays? But we had things and we had policies that, I would argue, interacted with the marketplace, business decision-making, and economic cycles – we're talking non-domestic companies. A fundamental policy question is, "Is that where we want to be?" I think there are multiple answers to this question, but I think we're taking a very passive approach and just kind of hoping that things will turn out in a way that's not too bad for us.

So, what we, the U.S. government, fundamentally need to do is pick champions. The easiest thing to do would be to say, “We love Nokia. We love Ericsson. We’ve already got a lot of their stuff, let’s really get behind them.” That could mean investment in R&D, it could mean other forms, much more aggressive kinds, of investment provided in ways similar to other sectors of the U.S. economy. It could involve, for example, doing things that we’ve done with the aviation industry and showing up with these companies when they go around the world to sell their products and say, “Hey, by the way, you buy that stuff and we’re going to throw in some special U.S. government magic – no extra charge,” or “We’re going to throw in some financing.” We have the EXIM Bank. The amount of money the EXIM Bank spends nowadays is pretty small in the context of this conversation, but that’s an avenue that we could approach. If these are the people we trust, then let’s get behind them.

When you consider that these companies are multinational companies with big footprints in the United States, and in some cases with big historical footprints dating back to U.S. industry, we could say that we’re going to get behind this. If that’s not good enough for you in terms of, “No, it’s got to be an American – they all got to be waiving little American flags.” Well, fine – then let’s figure out how to fix what we broke 20 years ago.

The other thing to think about with current policy is what are we doing to the high-tech industry, at large. I believe there’s a meeting today at the White House, at which various high-tech industry CEOs are meeting with the Secretary of the Treasury, the head of the Economic Council, and maybe the President’s also dropping in. They’re basically going to say, “Oh my gosh, the amount of uncertainty that you’ve thrown into our lives – The amount of potential denial of marketplace that your policy is going to create is just going to destroy our bottom line.” This brings us back to the issue of U.S. government investing in innovation. Again, we have taken a very passive view about this.

We have to remember where Silicon Valley actually came from. Silicon Valley is the result of the defense industrial base working like gangbusters with Stanford on air defense. Then, there were these useful things – these widgets used in air defense, that we eventually called computers – and then eventually, the semiconductor people showed up, and then the magic began.

But there’s been a tremendous amount of government involvement in innovation that we essentially walked away from about 20-25 years ago. When the internet was created, we basically took our hands off the steering wheel. When I say internet was created, what I mean is that we turned the ARPANET over to business and commercialized it. This thing that government created, we took our hands off the steering wheel said, “Oh, over to you. It’s all about markets.” Well I’m sorry, no it isn’t. That’s just not been the history. That’s not the reality.

We need to face up to the reality, and the United States needs to step up and put some serious money on the table somewhere if they want to have any influence on this. Whining and policy is not going to get you to a favorable outcome, I’m sorry. That’s enough.

image: Shutterstock

Question and Answer

Dr. Michael Fritze – Opening Question:

I want to understand how we got to the situation that we are in today with a lot of foreign domination, and we may not actually control 5G and things like this. Because I know in my own career – I did a tour at DARPA – a lot of the early technologies of doing really low-cost high-performance silicon, which I would argue enabled 5G in the first place, the U.S. Government owned that space. And they certainly owned that space for defense and for the military – our military radars and electronic warfare systems and stuff like that are powerful. So, we owned that space compared to the rest of the world. I know you've addressed elements of it, Tom, but how did we get to a situation where we started by doing robust government investment in research, owning the military implementation, but now as it becomes commercial, we're at the cusp of possibly losing it? And Tom, you've already addressed elements of this, but how did this state of affairs occur?

Tom:

If I could just throw in one more piece on top of what I just said – there was a memo somewhere in DoD which basically said, "Buy commercial."

Dr. Michael Fritze:

When I started my professional career, the buzzword was COTS. So, rebuild your radar box or rebuild your analysis tool and everything, build it in Commercial-off-the-Shelf (COTS) and it'll be cheaper and better.

Tom:

Because there was a point where commercial technology frankly was better, and got better. They invested. It got better. I'm not saying COTS is bad, I'm just saying if we are going to go down that road then we need to get on the train and go down with it, not just sit back passively and then complain about the answer at the end.

Dr. Michael Fritze:

Yeah to me it's personally frustrating because this is an area that we started, and we owned in the military space. I want to turn it over to our audience – but before that, are there any comments from Brian or Bob on how we got to today's state of affairs?

Brian Hendricks:

Well, one comment on maybe how we got to this state of affairs, but maybe two comments on how we get out of the situation that we are in, as well.

One thing to consider is that at least with respect to the hardware side of things, it's a very tough business. Standardization is critical, and developing scale, but it also commoditizes the products to a major degree. That was okay for a while, but now we are dealing with competitors who have some advantages that exploit that fact, which makes it very difficult.

With regard to getting out of it from a hardware perspective, it's probably unrealistic to expect that the United States is going to develop a hardware champion from the ground-up. In fact, we saw lots of consolidation happen with Nortel and Lucent and other prior champions being absorbed into companies like frankly Nokia – Alcatel-Lucent, who Nokia bought – and that's a factor. It's driven in large measure by the limitations in what you can do from the commodity perspective.

But, two things are interesting. First, we have some conversations going on with DoD and others that we didn't have a short time ago. There is a framework for discussion with the National Spectrum Consortium and others if we put real money into it. There is the opportunity to talk about ways that move away from just, "I want to sell you the same base station that I'm selling T-Mobile," and developing technologies – for example, unique technologies to help on the front line, that quite honestly can produce breakthroughs and innovations that will become part of 6G.

Also, something that people should be very concerned about right now is this use case concept where we keep talking hypothetically about use cases, but we haven't necessarily seen a lot of them arriving in the marketplace, yet. For example, iCreate, which is Indian policy of creating small network cities that will become incubators for those use cases by inviting investment from lots of sources, like Nokia, operators, IOT, cloud, edge, web analytics. It takes considerable government work to create these kinds of environments – the living labs that create huge innovation for the future and may mean use cases arrive in Asia before they come here.

There's a real opportunity for the U.S. to do this, here. I know you have some cities who are willing to look at doing that, and who are eager to create streamlining of citing and infrastructure policy. If the government was willing to act as a convener and an investor to bring these together, then we could have living labs in the U.S. that drive the next generation of innovation. This doesn't appear to be a prescription that's being thought about right now.

Tom:

Whereas in China, they are. China's got smart cities initiatives. They're also kind to the road and belt initiatives to spread this to other countries.

Dr. Michael Fritze:

So, Bob, any comments about how we got to this stage?

Robert Kolasky:

You know, it's a good question and one that I would prefer to be asking than answering. It's worth learning the lessons for future policy making, but one thing that occurs to me that we talk about often is one of the contributing factors to getting to where we are today is that security wasn't valued in this process. It wasn't valued as part of the evolutionary process of communications networks. When you have something that's not valued – it doesn't get priced in. You don't think about ways to use policy interventions to get to that, and – as I sort of ended my remarks – too often we cheerlead the innovation, the technology in the development. Then we figure out, "Okay, what's the security consideration that's been created?" If you simultaneously reverse that equation a little bit, you can try to include it to determine the right intervention.

Dr. Michael Fritze:

Well thanks. So, I don't want to hog the mic here – so let's go to the audience.

Audience Question #1:

How would the technology industry react to Tom's lament that, "Hey, we gave you everything. Now you owe us something in return." I'm sorry to tell you that the normal industry reaction services do not tell me what you did for me yesterday, and much less do I want to hear what you did for me 25 years ago, before I was even born.

So no, there is no sympathy for that. We're out for ourselves and that's the way the industry works. But I think that if I try to combine Brian's comment that the tax surface increase by orders of magnitude in the technology with Tom's comment that the connectivity issues are going to increase globally in order for us to defend our position also by orders of magnitude, and then add that by the middle of the next decade, we're going to get quantum computing, which will make virtually any encryption technology we have today worthless. So, the future simply looks impossible and I don't know why we don't just conclude – I guess as the British Admiralty did at some point – that we simply can't protect the high seas. We can't be the global protector of the high seas. That's not going to happen. We don't have enough people in England, or ships in England to do it so we're just going to pull back to what we can do instead of pretending that we're going to spend tens or hundreds of trillions of dollars and beating up all of our allies and every other country in the world to do what we can't do. It's not that it's not theoretically possible to provide the global comprehensive security structure for 5G that we're talking about. Theoretically it is possible, I think we all have to just go bankrupt to do it.

The future does not look bright and nothing that the panel has said makes it look any brighter. The problem is just so enormous that I don't see how it can be tackled, thank you.

Brian Hendricks:

Sobering. I would add two things to what you said. I would agree on the post quantum networking is something that very little – actually next to none – attention is being focused on. That organically is something that the government probably will need to be a little shoving on because we'll look at it, too. But, there's not an immediate commercial application for it, so industry is going to be slow to get to that point. However, imagine a scenario in which the encryption ciphers aren't as valuable anymore and your adversary has already adopted quantum communication systems of their own, limiting your ability to surveil what they're doing. There's a major threat coming there.

I don't know the answer to the question about, "Let's just resign ourselves to what we can't." There are too many things we can do that we aren't doing. That is the place I'd like to start. I think we should take an inventory of the tools that we have to protect 5G now, as opposed to doing what we have done in the past, at least this is my view. A lot of times industry will design things and use standardization mode ubiquity and speed of deployment. The internet comes to mind. We were all about making sure that we had inter-connection protocol – common protocols because we wanted it to be widely distributed.

Security wasn't a total afterthought, but it didn't go into the mix on the front end, and we've seen the limitations of trying to overlay security on top of that, after the fact. We shouldn't extrapolate that same problem to the way that we're designing the next generation of communications networks, and instead think a little bit more about how security can be designed in. We think we're comparatively good at it. We think we've been thinking about 5G a lot, and about how you can do things like with network slicing design – different security for different slices that have different purposes. We'll have the ability to differentiate how we approach security. We'll have adaptive and automated security response and self-healing networks. These are huge advancements over what we had in the past, but they're not sufficient to address the full nature of the problem that you're describing.

There probably does need to be a more active government role in stimulating industry to look at different questions that don't today have an immediate commercial opportunity for us.

Dr. Michael Fritze:

And just like that, in terms of actual research and innovation, we're still pretty strong. There's a lot known on gigahertz and terahertz Radio Frequency (RF) systems. Maybe not in U.S., like telecom companies, but we as a country have a lot of expertise there. So, I'm somewhat hopeful as we – if we – get our act together if we're scared straight.

Tom:

I don't think we're talking about trillions and trillions of dollars here. I'll settle for like $200 billion. You know, something like that. I've heard people say, "Yeah we could do that one of those work/fun things – like raising money on the internet." Maybe. I would also be careful about leaping completely – slicing your wrists over quantum computing. I think the application of quantum computing toward evil is not going to be trivial. It's not going to be magic. There is work being done on quantum-resistant cryptography. There's going to be a pucker factor someday, when somebody finally actually pops a useful machine out the door. But it's going to take time for that to become something useful, and there's going to be time for infrastructure to respond.

To the notion that we should just repeat the British experiment, and failed empire – the British led telecommunications and has since around the 1900s with help from American entrepreneurs, I might add. But, it was the fact that they were drained by two world wars that they eventually gave up. Are we going to go down in history, saying, "Wow we were kind of tired after Iraq and Afghanistan and we gave up our position as the leading democracy on the planet." I don't think so. We shouldn't, in any case.

Robert Kolasky:

I spoke earlier about what we're thinking about in terms of "Secure Tomorrow" in scenario thinking. There are both pluses and minuses to using historical analogy, and looking back to learn from history. Clearly, there are plenty of times when somebody could have asked the same type of question you just asked that would cause us to throw up our arms and just assume we'll never be able to solve it. So far so good in terms of combinations of analysis and innovation and some policy interventions, and then strategic thinking gets us to periods of stability. As long as the U.S. government's paying me, I'm not going to throw up my arms and give up. I think you're right to try to push us toward – one of the parts of your questions – to push us toward strategic thinking and understanding, accepting, and trying to operate within the things that maybe we can't control, as opposed to trying to solve things when we can't put the genie back in the bottle.

Audience Question #2:

Could you all take a step back and talk a little bit about spectrum and spectrum allocation challenges or issues? Is it true that the area that's most favorable for a 5G development is really not available for commercial use in this country, when outside this U.S. most others are focusing on this sub-6 gigahertz portion of the spectrum? That the area that is available in this country is really more the millimeter wave part of the spectrum, which has some technical challenges? Fundamentally, where does that leave us if this is all true? Where does that leave us if our companies and our government and all of our commercial activity is focused on a completely different part of the spectrum from non-US companies and governments? Is there a fundamental incompatibility there? Mr. Kolasky, is it fair to say that we are assuming that scenario, and that the U.S. is how you described regarding risk mitigation? Is it fair to say that we are just assuming a defensive posture, that we are looking at risks and vulnerabilities and trying to mitigate those, but assuming that the U.S. is not going to lead in 5G? Or did I overread your remarks?

Robert Kolasky:

Yes, you overread my remarks. I am a security professional, so I start with the risks. But, I hope what we're hearing is – what I try to say is – there are opportunities here and certainly we're trying to be a global leader. Not just in security applications – in setting up a security regime – but a global leader and other things. It's just not where I spend my time thinking.

Brian Hendricks:

So, you asked a fantastic question on spectrum and I'm delighted because not a lot of people in the U.S. have been asking and talking about this. The short answer is yes, we have a major spectrum allocation problem in the United States. It has not been focused on, and that leaves us behind. What we're thinking about is the evolution to full 5G. You heard me talk at the top about ubiquitous coverage 10 to 20 gigabit per second speeds limited latency. To achieve that, you need the full spectrum stack. You're going to need lower band spectrum for coverage, which we have allocated 6 and 700 megahertz spectrum to all the operators in the United States. That is in the process of being built. We have allocated a lot of millimeter wave spectrum, and there is more slated to come in 37 and 39 gigahertz – we need it all because each of those pieces of spectrum do something different in 5G.

Now the question about whether we should be launching in millimeter wave – probably not. If we had it to do over again, would we start with allocating mid-band spectrum? I think so. Millimeter wave is useful, but in most of the other countries where Nokia does business, the launch is going to be anchored in mid band below 4 gigahertz primarily, and 3.4 to 3.8 gigahertz.

Most countries have already allocated it or will be allocating it soon, and they will be allocating it in huge block sizes – 80 hundred megahertz blocks – to each of their operators. Those are huge channels through which you can do a lot and mid band is kind of the beachfront property because it has both coverage and capacity capability in it. Then, millimeter wave would come later to scale up as use cases drive the need for more capacity – you can densify deployments using small cells and millimeter wave. That doesn't mean that all of the significant investment that's being made right now in millimeter wave deployments in the United States is a wasted effort. It's important, but it will be squandered to some degree if we do not very quickly make mid band spectrum available to all of the operators so that we can capitalize on those deployments. Part of the reason for this is that millimeter wave is very difficult to work with – we're finding that it has very limited propagation characteristics. It has very limited building penetration. Humidity and leaf size can determine whether you're getting 600 meters out of a radio interface or 300, and so those deployments are important – early deployments. But what we're finding is an even smaller part of the urban core can be covered than we thought.

So, if you want to scale out, if you want to cover more of the United States, you're not going to be covering the bulk of the United States with millimeter wave. It doesn't matter how much of it we make available, it's just not going to be economical. You'll need 10 to 50 times as many radio sites to do it. You're going to have to have low-band, mid-band, and millimeter wave spectrum available, and right now we don't. Sadly, we've told the Federal Communications Commission (FCC) many, many times it has one band it has not been making a decision on for the better part of a year. It needs to move on the c-band. There are also some shared bands with the U.S. government – 3.1 to 3.55, in particular – that have resulted in some governmental opposition. We believe spectrum sharing is a reality. We can figure out how to share and mitigate those concerns. Those are bands that need to be pushed aggressively because we're behind – there's just no way around it.

Dr. Michael Fritze:

So, if I can paraphrase, sub six is really where all the commercial action is.

Brian Hendricks:

No, I mean what I would say is it's all important and valuable, and you can't build an evolved 5G network for the future in the United States with only one portion of the spectrum that's needed. We will get there eventually, with all of it, and important work is happening, but we see a lot of discussion about, "Oh the United States is leading; the United States is winning." You can make a case that a number of nations are winning based on what you choose to count. If you're just counting the number of radio nodes on a pole at this point – the U.S. is probably leading. We don't think that's the right metric to determine long-term leadership. It's "Do you have the ingredients necessary to lay the foundation for ubiquitous coverage?" because if you look at Asia right now – China, Japan, Korea, Malaysia, the Philippines, Vietnam – all of these countries have very large populations and very high population densities that make different land use policy. They build these networks out very quickly and scale them out to billions of people. That has all sorts of implications for U.S. economic security if our companies leading in web-scale and other places aren't going to similarly be able to reach the bulk of the U.S. population for some years to come. It's time to move mid-band into the market. It has been for a while, but it is not fair to say that we can't do anything, because maybe we have to have it all.

Tom:

So from a Department of Defense perspective, the extent that DoD plans depend on 5G for anything outside the United States – the low frequencies are going to be more critical because we're not going to be having antennas nicely deployed every 10 feet or whatever it takes for millimeter wave – the longer range that goes with the lower frequencies. It's going to be critical, and maybe DoD is part of the problem with the spectrum. They need to contribute to it if they care about it.

Audience Question #3:

Bob, you mentioned that you are starting to examine ways to incentivize trusted suppliers. What are you trying to incentivize them to do? Is it to release these "vendor locks" that you mentioned? Can you talk a little bit about what you're doing to encourage what I think is open Radio Access Network (RAN)? Is that what you were talking about? And then if you could just clarify it, because I thought I heard you say that the Secretary of Commerce might not be the best way to address all supply chain risks. Maybe there were some you can explain a little bit.

Robert Kolasky:

Sure – that's not a hit on the Secretary of Commerce. I'm simply saying that – and I was particularly talking about the authorities around the International Emergency Economic Powers Act (IEEPA) and the emergency authorities that were called for in the President's Executive order – that is a tool to deal with some critical issues around supply chain risks. But whatever the word is to describe the tool – it's only one tool of things you can do to manage supply chain risk. The last thing I think anyone within the policy committee would like to say is just set restrictions. You can't buy from anyone in your information and communications technology (ICT) supply chain – that's not an effective way to do risk management. So that's what I said on that one. Your question on examining and thinking about incentives – I'm really talking about the interagency discussion about where there are opportunities as we continue to better understand evolution. What's going to happen? Where are the markets going? Where might there be risks? Where there are opportunities to incentivize gaps in places where we don't have trusted suppliers or manufacturers – where we don't have trusted manufacturers at scale. That's how we're framing thinking about some of the policy questions. Again, thinking about what's going to happen absent policy making, and policy making should only intercede when necessary.

Audience Question #4:

What are the gaps? Mr. Hendricks might take opposition to the idea that Nokia is not filling a certain gap right now.

Robert Kolasky:

I don't have an answer to all the gaps here, and that's why I'm framing my remarks in some ways in terms of questioning – the question we're asking, how we're pulling on that, is because we want to be smart as an interagency in better understanding how the markets are evolving and where there are gaps. I don't think we're ready to say that there's a specific gap. I think it's similar to some of the reasons Brian said. Let's continue to learn through this process and not just rush to a solution.

Brian Hendricks:

Yes, I think part of it is understanding the origin of risk. Even in our own conversations with governments around the world, the generation of concerns is unclear. So, for example, if you take a very narrow view that sourcing components in a particular country creates risk, my pushback is not all components can create risk – power supplies, mounting harnesses, screws, whatever. So, let's have a conversation about what causes concern about location of sourcing. Part of that conversation needs to be: What are companies actually doing to mitigate concerns about things that do you do? Do you test? Do you randomly sample when your supplier delivers? What are you recording on software development? Do you have forensic auditing tools that let you watch what someone's doing through the evolution of codes – so that at any point you can go back with signatures for checking in and checking out?

Understanding what people actually do in the sector, comparing that with perceived risk, and then identifying, "Okay some of our concerns have been answered because we just plainly didn't know what companies were doing." But, some of these concerns will remain. What is the best way to address those concerns? To my knowledge, those conversations haven't generally happened globally with policy makers, so we're still left with country of origin and company specific concerns.

While that may be, at the moment, inert to our benefit, it's probably not a practical way to do this on a long-term basis because when you pick a country and say, "I don't like you manufacturing there," at the same time you realize that 95% of the people supplying some kind of ICT infrastructure are sourcing from that country. At least at some level of the supply chain there's a pragmatic element that has not been worked through.

So, I think we have to start with narrowing – defining what the concerns are, where the risk comes from, what's being done already – then, which part of that will we highlight as best practices. Maybe some of our practices will be best practices. Maybe there are things we learn from others. But, there will be a set of risks left unaddressed – and that can be the basis for discussion. I just don't think we're at that point globally right now.

Audience Question #5:

Much of the discussion so far has been about industry and the industry-government collaboration and policy issues. I was hoping you could talk a little bit about how you would leverage existing R&D centers and test beds that the government is already funding. Such as the National Science Foundation (NSF)'s Wireless test beds power, or the Department of Homeland Security's Science and Technology Center for Critical Infrastructure and Resilience, or even DoD's manufacturing institute – there's one in Chicago that focuses on cyber security and supply chain security for the manufacturing sector.

So, as you develop those scenarios and look at the risk assessment, how do those research assets funded by the federal government play into that? And how can you accelerate experimentation and post development testing?

Robert Kolasky:

Sure, so, you know the R&D component we use most often at DHS is the National Laboratories, and so some of what I'm talking about is federally-funded research development centers through the National Laboratories, which tend to be associated the Department of Energy. You mentioned Critical Infrastructure Resilience Institute (CIRI), the Center of Excellence at the University of Illinois. The kind of money there isn't the kind that's good – you're going to get a ton of physical testing or things that are more hard science. It's earlier in the thinking process.

One of the things we want to do is put out a list of the research questions we're most interested in answering, publicize those to some extent, but also share where there are centers that could do some of this and try to create more of a unified R&D agenda. We try to do that around a lot of critical infrastructure problems. This is one, and we've had some success here. This is one, as the interagency collaboration increases – I think that's an opportunity to take advantage of where there has been funding. Just because I don't have all the lists of places we could take advantage of doesn't mean that that thinking isn't being applied. I think it's a good idea.

Tom:

So, I think that's a valid point to be made, but I think the problem is lack of focus. There's where we're spreading money across a lot of pet rocks and ideas. We staple them together and call it the federal R&D program, but there isn't actually any concrete objective that is being sought in doing so. I'd point to the Apollo program, which is a very different kind of example, but since it is the 50th anniversary fantastic amounts of money were spent to solve and get to a specific coherent objective across many different kinds of technological components and it led to making something real. The problem with a lot of these research things is that they sort of identify a theoretical problem. They treat a hypothetical, and it doesn't actually lead to anything happening. In our infrastructure, in DoD language, this is like 6.1 versus 6.3 stuff and the expertise that we had a lot more of in this country. That was in the past, when we had the industrial labs like Bell Labs, that Nokia now has. That lab is an example of the preeminent place where a lot of R&D was then carried forward. There was a way that the R&D was carried forward from the very basic research. What we've done instead is we essentially bifurcated that where academia has a lot of the basic industries – a lot of 6.3. And the question is do we have any connects? Is it connecting in a way as efficiently as it possibly could? And so that would be my approach to that problem.

Dr. Michael Fritze:

So, you are describing the Valley of Death region, right?

Tom:

You bet, and there's another part of this problem, which is particularly in my background in semiconductor manufacturing. What I've observed over the decades is another separate issue. As the manufacturing moves someplace else, the research follows it in the high-tech world because the ecosystem that's necessary to stay on the cutting edge of research is actually – an academic lab cannot compete with the cutting edge thing that's being done in a big semiconductor FABrication plant (FAB) whether it's at Intel or Taiwan Semiconductor Manufacturing Company (TSMC). So, the ecosystem – the supply chain that makes all of that possible – follows it. We're in danger if we go for this design-only kind of mentality that we have in this country. If we don't actually make the stuff then we eventually lose the ecosystem, and eventually we lose the expertise that goes along with it. That's a bad spiral to begin.

Dr. Michael Fritze:

I have to make a quick comment on that myself, because I'm from a similar background. The whole research enterprise is nonlinear. It doesn't start with 6.1, and progress smoothly through 6.2, and 6.3. There's a lot of feedback that happens, and that's why when you move manufacturing, you move research, because you lose the feedback loop.

Audience Question #6:

So, given all of the different stakeholders and players in the market, but especially the new entrants, based on the new use cases that might come to market, how much of a challenge is information sharing when it comes to the security of 5G network, and then what can be done about it?

Brian Hendricks:

We have some recent examples where we have attempted to have the government act as a convening authority to bring information streams together. I speak of the The National Institute of Standards and Technology (NIST) cyber framework, and there are some lessons learned there – one is that industry can tend to be cautious about sharing vulnerability information unless you provide the right environment in which that information can be shared and utilized without there being negative commercial consequences. Something like that is probably essential here. We have some very good threat detection and mitigation capabilities that I mentioned at the top when I was talking about the threat detection reports that Nokia puts out. Part of that is we have agreements with many of the network operators that we have around the world. We're in 130 or so countries where we've deployed millions upon millions of sensors to collect information on threats, so this gives us a very large data set to take a look at previous threats.

We share that at the moment – to the best of my knowledge – mostly through our public reports.

There are certainly other forums and opportunities for us to share that, and even more detailed information may be obtained, potentially, by bringing in some of these new actors and the use cases – also, for example, enterprise. When we think of enterprise it's not just big business, it's going to be whole new sectors that are using things in new ways that will be empowered in part by the fact that they're not going to have just a relationship with a carrier anymore. There might be opportunities to buy equipment from someone and to go out and manage your own network – private Long-Term Evolution (LTE) networks and so forth – but they don't have any experience or heritage when it comes to identifying risks or responding to risks and vectors that have been identified by others. So, we probably need to think about new groups or organizations that we can have as threat-sharing portals with government participation in information sharing what it sees and learns. So, like I said, I don't think it's perfect for a lot of reasons, but I do think that the cyber framework from NIST is a valuable lesson and maybe we need something like that again but more expansive in terms of participation.

Tom:

So, this brings up the whole subject of public-private partnership and how that works. I would argue that information sharing is step one and it's usually about where we stop and usually not as well or as fast as it needs to be. But the problem is that a lot of the partnerships tend to be government with different categories of victims. The partnership needs to be between the government and the people who could actually solve the problem – and those are the carriers in this case. And so, what we need is a situation where the government and the private sector are working together to solve the problem of the day. To actually solve the problem. Not to notify each other that six months ago you should have done something.

Robert Kolasky:

That's some of what we're trying to obtain – to get past information sharing, understanding that the information sharing is a basis for shared understanding and risk mitigation. But we do have structures, in terms of coordinating councils, where there's good information sharing about evolution of risk. We have structures – information sharing and analysis centers – that particularly the comms Information Technology (IT) sector, where there's more real-time information sharing about any threat activities or vulnerabilities.

I think as we continue to focus on this – this is a new area – we'll understand who isn't part of that information sharing environment and we'll push to make progress into that, while making sure that we continue to make incremental improvements in any of our current information sharing environments. I think the other aspect of information sharing we've talked a little bit about is international collaboration, such as the Five Eyes structure of New Zealand, Australia, Canada, the U.K., and U.S. This is a principal topic that we're talking about at The Five Eyes construct, where we are sharing information about the government approaches in our understanding. Of that, there's a little bit less outside of The Five Eyes construct with some of the other like-minded countries because of some of the protection limitations. So that's an area where we probably can make some progress. But certainly, it's an area of focusto share intelligence and technical details through that structure – that part of the process, and it is important for the reasons I think all of us have talked about – that this is an international issue and it should be treated as such.

Tom:

Since this is a law firm, I have to throw in a comment about the fact that DHS – and through the end kick has the carrier's, for example, sitting on the floor as they say, "The problem is that we don't have protocols in place for this type of event, we need to do this this and this; this is the data we're going to share; this is what you're going to be able to do with it on the day." There's a lot of work that I know DHS is embarking on and it's just going to need a lot of support to get through, which is this process to routinize handling cyber disasters – just the same way we've routinized handling hurricanes and we just were just not mature enough yet in this area.

Audience Question #7:

We've got two kind of questions:

1. With the Apollo program there was a clear, concise goal on where we need to go, what needs to be done, and what all this investment should lead to – do you have recommendations of what that should be with the 5G realm?
2. Secondly you mentioned that the inspection regime is impractical for testing of security on this. So, if we wanted to sort of red team some of these products and services that we're developing from current 6.1/6.2, all the way to 6.3 into roll out, what is a good way to validate and verify that the stuff that we're building is trusted and assured?

Tom:

Let me do the second one first because I think the issue of the red teaming is – I think you need to red team your trust model. Stop trying to be in a situation where you're going to look at every piece of code, every piece of gadget. What you need to understand is you need to invest at the front end of it all. You need to have people that you trust providing you with products that you understand. Then you need some way of quickly checking that it's doing at least a bare minimum of what you expect. Then to get to Bob's issues, then you need to have a plan for when it betrays you. I mean just that's what you do with DoD.

I think my mantra on this is to say that for infrastructure, we need to build it; industry, we need to have it; and innovation, we need to invest in it.

So, the question from DoD's point of view is can you shape industry the way we have done in the past such that you will get an supportive outcome X number of years down the road? Figure out who you want to play with and get on with it. There are people you can play with today or you're going to have to go out and make new ones, which is going to have a lot of issues and drop problems and challenges to it.

But you can also think of it – you need to think of it – both at the system level and you also need to think of it at the component level. Are there critical components, as Brian alluded to, that you really, particularly want to invest in because that's where you think the real issues might be? If you look at The National Aeronautics and Space Administration (NASA) as a model – they had a very peculiar outcome that they were going after that nobody else at time particularly was interested in. They didn't have the Elon Musk then to compete with and so they figured out where they needed to invest and that's why I think we need to get back into that mode of thinking and stop being so passive. Commercial off-the-shelf is great when commercial off-the-shelf can provide what you have. That policy was not meant to be that's all you get, you must live with it, and that's not what the policy is. The policy was look and see if it's available, buy it – if not, then you've got to make it. So, we must start investing in the making. We must invest in the innovating so there is something to make.

Dr. Michael Fritze:

I would add just a quick comment on this issue. Microelectronic supply chain is another area, as an example, that we've been involved in, and it wrestles with the same thing. Can you test your way out of – can you test your way into security? It's insufficient, right? We agree with that, just like in 5G. It's insufficient, so you need more.

Tom:

Right, if you look at microelectronics in particular, and you know the economics that Brian was talking about – to build a fab these days is over 10 billion now right and it just seems like the number of the fabs in the United States just seems to keep declining.

We talked about, "This is a U.S. company and that's U.S. design," but oh, guess what – almost everybody is going to Taiwan or to South Korea to get it made. And so, we must think about the whole chain of wheres. This gets back to Bob's point about risk mitigation. I'm not saying everything needs to be made in the United States. Some things might need to be made in the United States. Some things definitely need to be designed in the United States, but we need to figure out where those risks are, manage those risks, and then invest where we think we actually need to have stuff made right here.

Dr. Michael Fritze:

Let me give the panelists a final chance to make a concluding remark or a strategic remark. Maybe I'll set the stage with saying – try to make it positive, in the sense of what can we do? What can the United States do to put us in a better position for 5G going forward?

Image: Shutterstock.com

Robert Kolasky – Closing Remarks

Thank you all for the good discussion. It's nice to have a panel where I think we all get to say most of everything that was on our mind. I'm sitting here as a U.S. government representative and there's some inclination to just bang on the table and say, "This is what we're going to do about 5G." What I'd like to say from my perspective is that I think the fact we're not banging on the table and saying, "This is what we're going to do about 5G," is a good thing and not a bad thing because we are still in the process of working to better understand the risk, the technology, where the drivers are, and formulate policy that would be smart around these issues. This is a complex question. I think it's in rooms and discussions like this that we're going to get smarter, continued collaboration on that and to make sure that there's a better connection between technology and policy making – so thank you.

Brian Hendricks – Closing Remarks

I guess I've been sitting here thinking that at one point – I probably should have emphasized a little bit more is – a lot of this is very nuanced and we need to recognize that blunt instruments often have unpredictable and binary consequences. I think that from a security standpoint, we continue to need to move the conversation away from companies and countries of origin and more toward the origination of risk. Where does it come from? What are you really worried about? How do we meet those concerns?

From a competitive positioning perspective, we also, domestically, have the question about spectrum – maybe think a little bit more about this. Being first, or at least on the lead lap, really does matter. It's consequential and there's been a lot of marketing puffing going on about, "We're winning, who's winning, they're winning, we're winning." This is less important than recognizing that covering the U.S. population with the technology and the capability is pretty critical to our national economic future. Not just my financial future, but the web-scale in the industries that the U.S. does have a comparative advantage over the rest of the world, and we're lagging at the moment. There are more tools that need to be put in place to assure that the technology isn't limited to Urban Corridor deployments, which I think there is a real risk of happening unless we step up and meet that. People really need to think about the consequences to things like a digital divide if the majority of the country doesn't have access to 5G. You can do a lot with LTE, but there's a lot you can't do, and it's going to have a real limitation as we move to a digitalized economy if large pockets of your population don't have it. But it also puts companies – where the U.S. does currently have a strong advantage – at real risk, and so domestically, we need to step up our game.

Tom - Closing Remarks

We need to invest in this industry. Telecommunications is the nervous system of this nation, of this economy, and of our defensive capabilities. In the past we've used things like a moonshot to drive industry, which then led to broader benefits. There's a similar model to be held here, which is that this industry – the telecommunications industry – is essentially like the anchor of a department store in a big mall. We need to have that anchor in order to be able to allow the rest of it to grow, to have that ecosystem in which high technology innovation can occur such that we will continue to lead and prosper as a global power.

Dr. Michael Fritze – Closing Remarks

What we do as an institute is, we have several deep dive workshops. This is much too broad of a topic to cover in just these two hours today. We worked very hard on microelectronic supply chain security some years ago and had multiple deep dives where we had people represented from different parts of the government. For 5G, we're going to go broad and get the economic, financial angle, the Department of Defense angles, as well as a number of other perspectives. We're going to do a number of these events, so stay tuned, because this is a complex issue rife with policy opportunities.

About the Sponsors

The Potomac Institute for Policy Studies

The Potomac Institute for Policy Studies is an independent, 501(c)(3), not-for-profit public policy research institute. The Institute identifies and aggressively shepherds discussion on key science and technology issues facing our society. From these discussions and forums, we develop meaningful science and technology policy options and ensure their implementation at the intersection of business and government.

The Potomac Institute's Vital Infrastructure, Technology, and Logistics (VITAL) Center is dedicated to fostering and supporting comprehensive supply chain security as an integral part of all major US industries. Secure and resilient critical infrastructures will help the US maintain a strong national defense. As part of this mission, the VITAL Center works to:

- Assess the evolving strengths and weaknesses of our nation's critical infrastructure systems and technologies, and the supply chains they depend on.
- Advance knowledge of critical infrastructure and supply chain security challenges and solutions across the US Government and industry to include policy makers, the Department of Defense, and the manufacturing industrial base.
- Bridge the gap between commercial and defense supply chain security practices.
- Strengthen policy to ensure continued security of our nation's critical infrastructure and supply chains.

The Vital Infrastructure Technology and Logistics Center

The Vital Infrastructure, Technology, and Logistics (VITAL) Center is dedicated to fostering and supporting comprehensive supply chain security as an integral part of all major US industries. Secure and resilient critical infrastructures will help the US maintain a strong national defense. As part of this mission, the VITAL Center works to:

- Assess the evolving strengths and weaknesses of our nation's critical infrastructure systems and technologies, and the supply chains they depend on.

- Advance knowledge of critical infrastructure and supply chain security challenges and solutions across the US Government and industry to include policy makers, the Department of Defense, and the manufacturing industrial base.

- Bridge the gap between commercial and defense supply chain security practices.

- Strengthen policy to ensure continued security of our nation's critical infrastructure and supply chains.

US critical infrastructures encompass highly visible sectors like transportation, water, and agriculture as well as less conspicuous sectors like energy, finance, and information technology (IT). If any of these infrastructures were attacked, whether by hostile nation-states or by non-state actors, it would have major negative impacts on our national security and the economic well-being of our country. Even less nefarious disruptions to the supply chain, caused by inclement weather for example, are increasingly worrisome as the global economy becomes more intertwined and interdependent.

Due to the number, scale, and complexity of these sectors, no one entity can tackle the issue of critical infrastructure vulnerability alone. Both government and industry have a shared interest in the continued stability of domestic infrastructures and their global supply chains and are thus natural allies in the efforts to secure these systems. Through improved communication and strategic planning, industry and government entities can combine and coordinate efforts in comprehensively securing critical infrastructures.

The DCIP defines the following 16 sectors as critical based on their influence on the nation's economic health and security: chemicals, commercial facilities, communications, manufacturing, dams, defense, emergency services, energy, finance, food and agriculture, government facilities, healthcare, information technology (IT), nuclear facilities, transportation, and water. The number of sectors considered vital to the US is simply too great to be managed by one office of the federal government, or even by the federal government alone. Taken together, the 16 critical sectors identified by the DoD account for thousands of companies, millions of jobs, and billions of dollars of revenue changing hands across the country. The only effective way to provide comprehensive critical infrastructure protection is through a coordinated effort, both among government agencies and between government and industry. The VITAL Center aims to bridge the gap between government and industry security efforts by connecting diverse stakeholders from both worlds, creating a community of interest to create more comprehensive mechanisms of action for critical infrastructure protection.

Venable LLP

Venable is an American Lawyer 100 law firm. With nearly 700 attorneys across the country, Venable is strategically positioned to advances its clients' business objectives in the U.S. and abroad. Venable's clients rely on its proven capabilities in all areas of corporate and business law, complex litigation, intellectual property, and regulatory and government affairs.

Venable's communications experience and relationships deliver solutions to communications challenges and goals. The laws, regulations, investigations, and procedures relating to communications, privacy, data breach, and cybersecurity pose a bewildering challenge to the successful execution of communications strategy and business development. Venable retains an experienced, action-oriented team that loves to devise strategies for navigating laws, regulations, and procedures to achieve communications goals in a timely way, executing those strategies in an accountable way. Venable's legal team is comprised of a combination of attorneys who have served in the federal executive branch agencies, as members of Congress, and on congressional staffs. Many if not all have long-term experience shaping policy and rule-making, practicing before federal and state agencies. Venable team members marshal the facts, understand the agency processes, and use their knowledge of the process and relationships with decision-makers to accomplish goals.

Venable has over a century of experience staying on the cutting edge of technology, the lifeblood of the communications industry. Venable is experienced in and understands the technologies that routinely disrupt and revolutionize communications. It understands the communications axiom, New technology defies conventional legal models. Venable's mission has been to find innovative ways for service providers, entrepreneurs, inventors, and communications users to bring new technology on line, a challenge that demands attorneys who have the capacity to synthesize and understand the entire communications playing field.

Venable focuses on legal scholarship, regulatory insight, and advocacy. Venable has inaugurated major rule-makings, leading multifaceted campaigns at the FCC, before other agencies, and on Capitol Hill to have rules and policies adopted or to fend off unwanted regulations.

Venable's work combines advice on broad policy questions and specific solutions to everyday industry problems. It offers both front-edge knowledge of the thinking of legislators and regulators and first-hand experience solving the issues that confront the executives of electronic commerce, financial services and communications companies. Venable's policy work enhances its operational advice, and vice versa.

Venable combines legal theory and practical know-how in an integrated approach to complex privacy and security issues. Venable has had a measurable impact on privacy and information security laws and regimes. You can learn more about Venable's Communications and eCommerce, Privacy, and Cybersecurity areas of practice here.

https://www.venable.com/communications/