HEARING ON CHINA, THE UNITED STATES, AND NEXT GENERATION CONNECTIVITY

HEARING

BEFORE THE

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

ONE HUNDRED FIFTEENTH CONGRESS
SECOND SESSION

THURSDAY, MARCH 8, 2018

Printed for use of the
United States-China Economic and Security Review Commission
Available via the World Wide Web: www.uscc.gov

UNITED STATES-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

WASHINGTON: 2018

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

ROBIN CLEVELAND, *CHAIRMAN*
CAROLYN BARTHOLOMEW, *VICE CHAIRMAN*

Commissioners:
HON. CARTE P. GOODWIN
DR. GLENN HUBBARD
HON. JONATHAN N. STIVERS
HON. JAMES TALENT
DR. KATHERINE C. TOBIN
MICHAEL R. WESSEL
DR. LARRY M. WORTZEL

The Commission was created on October 30, 2000 by the Floyd D. Spence National Defense Authorization Act for 2001 § 1238, Public Law No. 106-398, 114 STAT. 1654A-334 (2000) (codified at 22 U.S.C. § 7002 (2001), as amended by the Treasury and General Government Appropriations Act for 2002 § 645 (regarding employment status of staff) & § 648 (regarding changing annual report due date from March to June), Public Law No. 107-67, 115 STAT. 514 (Nov. 12, 2001); as amended by Division P of the "Consolidated Appropriations Resolution, 2003," Pub L. No. 108-7 (Feb. 20, 2003) (regarding Commission name change, terms of Commissioners, and responsibilities of the Commission); as amended by Public Law No. 109-108 (H.R. 2862) (Nov. 22, 2005) (regarding responsibilities of Commission and applicability of FACA); as amended by Division J of the "Consolidated Appropriations Act, 2008," Public Law Nol. 110-161 (December 26, 2007) (regarding responsibilities of the Commission, and changing the Annual Report due date from June to December); as amended by the Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015, P.L. 113-291 (December 19, 2014) (regarding responsibilities of the Commission).

The Commission's full charter is available at www.uscc.gov.

March 20, 2018

The Honorable Orrin Hatch
President Pro Tempore of the Senate, Washington, DC 20510
The Honorable Paul Ryan
Speaker of the House of Representatives, Washington, DC 20515

Dear Senator Hatch and Speaker Ryan:

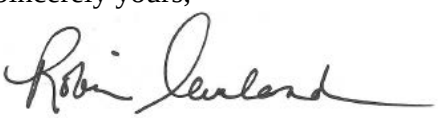
We are pleased to notify you of the Commission's March 8, 2018 public hearing on "China, the United States, and Next Generation Connectivity." The Floyd D. Spence National Defense Authorization Act for 2001 § 1238, Pub. L. No. 106-398 (as amended by the Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015 § 1259b, Pub. L. No. 113-291) provides the basis for this hearing.

At the hearing, the Commissioners received testimony from the following witnesses: Chuck Benson, Assistant Director for IT in Facilities Services, University of Washington; Doug Brake, Director of Telecommunications Policy, ITIF; Jennifer Bisceglie, President and CEO, Interos Solutions; Anthony Ferrante, Senior Managing Director, FTI Consulting; and James Mulvenon, Ph.D., Special Programs Division, SOS International LLC. Dr. Heath Tarbert, Assistant Secretary for International Markets and Investment Policy, U.S. Department of Treasury submitted written testimony for the record. This hearing compared and contrasted U.S. and Chinese pursuit of next generation connected devices and networks and the implications for U.S. economic competitiveness and national security. The hearing focused on U.S. and Chinese 5th generation wireless technology (5G) and Internet of Things standards and technology development, U.S. usage of Chinese Internet of Things technologies and 5G networks, and the ability of Chinese firms to collect and utilize data from U.S. consumers through Internet of Things technologies.

We note that the full transcript of the hearing is posted to the Commission's website. The prepared statements and supporting documents submitted by the participants are now posted on the Commission's website at www.uscc.gov. Members and the staff of the Commission are available to provide more detailed briefings. We hope these materials will be helpful to the Congress as it continues its assessment of U.S.-China relations and their impact on U.S. security.

The Commission will examine in greater depth these issues, and the other issues enumerated in its statutory mandate, in its 2018 Annual Report that will be submitted to Congress in November 2018. Should you have any questions regarding this hearing or any other issue related to China, please do not hesitate to have your staff contact our Congressional Liaison, Leslie Tisdale, at 202-624-1496 or ltisdale@uscc.gov.

Sincerely yours,



Robin Cleveland
Chairman

Carolyn Bartholomew
Vice Chairman

cc: Members of Congress and Congressional Staff

CONTENTS

THURSDAY, MARCH 8, 2018

CHINA, THE UNITED STATES, AND NEXT GENERATION CONNECTIVITY

Panel I: Economic Implications of U.S. and Chinese 5G and IoT Standards and Technology Development

Panel II: U.S. and Chinese Policies to Address 5G, IoT, and Data Privacy and Security Challenges

CHINA, THE UNITED STATES, AND NEXT GENERATION CONNECTIVITY

THURSDAY, MARCH 8, 2018

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

Washington, DC

The Commission met in Room 2255 of Rayburn House Office Building, Washington, DC at 9:30 a.m., Commissioner Michael R. Wessel and Commissioner Larry M. Wortzel, Ph.D. (Hearing Co-Chairs) presiding.

OPENING STATEMENT OF LARRY M. WORTZEL, PH.D HEARING CO-CHAIR

HEARING CO-CHAIR WORTZEL: Good morning. Welcome to our third hearing of the U.S.-China Economic and Security Review Commission's 2018 Annual Report cycle.

Today's hearing examines China's pursuit of next generation connected devices, or the Internet of Things, future networks, and the implications for U.S. competitiveness, national security, and data privacy.

We are on the verge of an interconnected world with near real-time, high capacity networks that will affect industry, economies, society, the military and warfare. The Internet of Things means the connection of computing devices embedded in everyday objects, enabling them to send and receive data as well as responding to commands.

I mean we've all probably seen commercials asking a connected speaker in a home to order food, adjust the temperature, and start the pickup truck. Smartphones are shown as opening our doors and locking them to allow deliveries into the house, monitoring the home security system, controlling lights and the home's temperature.

This capacity to link devices, control them and have them communicate with each other applies to industrial control systems and connected military weapon systems. However, there is some danger involved because the technology of these inter-connected things can be hacked, monitored, manipulated, or otherwise exploited by malicious actors.

At the same time, on the Internet, the United States and China are competing to lead the transition to a 5th generation wireless technology, or a "network of networks," that will deliver higher capacity bandwidth more quickly than ever before to increase the capacity to use or manage this Internet of Things.

Now it exists now--the Internet of Things--smart cities, you know, smart grid systems, things like that--but it's going to be faster and higher capacity with some problems.

The Chinese government has dedicated enormous resources to attaining leadership in these technologies and to penetrating the U.S. market. This hearing will explore the security risks of the increasing integration of Chinese-made or designed devices and 5th Generation cellular network equipment into the United States.

The hearing also will explore how the integration of Chinese technology into U.S. systems could provide means to conduct espionage or sabotage.

The panelists in today's hearing will also explore what role the United States government should play in securing its own networks and to protect the Internet of Things, how to maintain U.S. global competitiveness, and ways to protect U.S. data privacy and security.

We look forward to exploring the issues in more detail with our panelists. We really have a superb lineup.

And before I conclude, I want to thank all the witnesses for the effort they've put into preparing their testimonies and the travel. I think you've probably made the longest trip on this one. Thank you.

[Laughter.]

HEARING CO-CHAIR WORTZEL: Let me turn it over to Commissioner Wessel, my co-chair, for his remarks.

PREPARED STATEMENT OF LARRY M. WORTZEL, PH.D
HEARING CO-CHAIR

Good morning. Welcome to the third hearing of the U.S.-China Economic and Security Review Commission's 2018 Annual Report cycle. Today's hearing examines China's pursuit of next generation connected devices, or the Internet of Things, future networks and the implications for U.S. competitiveness, national security, and data privacy.

We are on the verge of an interconnected world with near real-time, high capacity networks that will affect industry, economies, society, the military and warfare. The Internet of Things means the connection of computing devices embedded in everyday objects, enabling them to send and receive data as well as responding to commands. We all have probably seen commercials asking a connected speaker in a home to order food, adjust the temperature, or start a truck. Smart phones are depicted as opening our doors and locking them to allow deliveries into the house while monitoring the home security system, controlling lights, and the home's temperature. This capacity applies to industrial control systems and connected military weapons systems. However, there is some danger involved in such technology because these inter-connected things can be hacked, monitored, manipulated, or otherwise exploited by malicious actors.

At the same time, on the internet, the United States and China are competing to lead the transition to a 5th generation wireless technology, a "network of networks," that will deliver higher bandwidth more quickly than ever before to increase the capacity to use or manage an Internet of Things.

The Chinese government has dedicated enormous resources to attaining leadership in these technologies and penetrating the U.S. market. This hearing will explore the security risks of the increasing integration of Chinese-made or Chinese-designed Internet of Things devices and 5th Generation cellular network equipment into the U.S. The hearing also will explore how the integration of Chinese technology into U.S. systems could provide means to conduct espionage or sabotage.

Panelists participating in the hearing also will explore what role the U.S. government should play in securing its networks to protect the Internet of Things, how to maintain U.S. global competitiveness, and ways to protect U.S. data privacy and security.

We look forward to exploring these topics in more detail and hearing the insights of our great lineup of witnesses.

Before I conclude, I want to thank our witnesses for the effort they have put into preparing their excellent testimonies.

Let me now turn to my hearing co-chair, Commissioner Wessel, for his opening remarks.

OPENING STATEMENT OF MICHAEL R. WESSEL
HEARING CO-CHAIR

HEARING CO-CHAIR WESSEL: Thank you, Dr. Wortzel. I join him and the other members up here in thanking you for your travel and all the work that went into the testimony today, the expertise you bring to us.

Today's hearing addresses an issue that has enormous repercussions, but here in the U.S., here in Washington, has received limited attention. Indeed, the National Intelligence Council took the unusual step by releasing a report in September indicating that by 2035 the new interconnected economy is expected to enable $12.3 trillion in global economic output and support more than 22 million jobs. From an economic point of view, the technologies and products we're talking about will help shape and be the foundation for the future.

The course of who controls the standards, who develops the products, and who produces them is now being set.

Some believe that the U.S. is at the forefront, but China is well underway on a comprehensive plan to close the technological gap and control the enormous economic benefits these interconnected devices and faster, more powerful networks will enable and create.

In addition to the economics, Dr. Wortzel touched upon the security and intelligence concerns that we'll be looking at today, but, in my view, we are dramatically underestimating the potential threats that are out there. We should be alarmed about China's dominance of these new technologies.

The Chinese government seeks to establish the global standards for these next generation networks and technologies and be the manufacturing center for all the products. According to an article in the South China Morning Post, China has committed already more than $400 billion to their efforts.

America, it seems, still lacks a strategy. Indeed, recently, a draft National Security Council document called for nationalizing the 5G network. That suggestion was quickly shot down by technology companies, many of whom have already placed their bets in China.

Today, I hope, we will have the ability to lay the groundwork for a serious discussion of the issues, their implications, and identify some potential recommendations for action. The need for attention couldn't be more serious.

As we examine these issues, we can't forget that China's leaders are tightening their grip on their economy and their people. Technology is used to advance the Party's and the state's interests. Many of their interests are in direct conflict with our own goals and ideals.

We look forward to our panelists' insights and contributing to our and Congress' understanding of the opportunities and challenges that must be considered.

As a reminder, the testimonies and transcripts from today's hearing will be posted on our website at www.uscc.gov. And our next hearing--please mark your calendars--will be on April 5, "China's Relations with U.S. Allies."

PREPARED STATEMENT OF MICHAEL R. WESSEL
HEARING CO-CHAIR

Thank you, Dr. Wortzel. I join my colleague in welcoming and thanking the experts and guests who have joined us today.

Today's hearing addresses an issue that has enormous repercussions but, here in the U.S., has received limited attention. Indeed, the National Intelligence Council released a report in September indicated that by 2035 the new interconnected economy is expected to enable $12.3 trillion in global economic output and support more than 22 million jobs. From an economic point of view, the technologies and products we're talking about will help shape and be the foundation of the future.

The course of who controls the standards, who develops the products and who produces them is now being set.

Some believe that the United States is at the forefront, but China is well underway on a comprehensive plan to close the technological gap and control the enormous economic benefits these interconnected devices and faster, more powerful networks will enable and create.

In addition to the economics, Dr. Wortzel touched upon the security and intelligence concerns that we'll be looking at today. But, in my view, we are dramatically underestimating the potential threats that are out there. We should be alarmed about China's dominance of these new technologies.

The Chinese government seeks to establish the global standards for these next generation networks and technologies and be the manufacturing center for all the products. According to the South China Morning Post, China has committed more than $400 billion to their efforts.

America, it seems, still lacks a strategy. Indeed, recently, a draft National Security Council document called for nationalizing the 5G network. That suggestion was quickly shot down by technology companies, many of whom have already placed their bets in China. Today, I hope, we will have the ability to lay the groundwork for a serious discussion of the issues and their implications and identify some potential recommendations for action. The need for attention couldn't be more serious.

As we examine these issues, we can't forget that China's leaders are tightening their grip on their economy and their people. Technology is used to advance the Party's and the state's interests. Many of their interests are in direct conflict with our own goals and ideals.

We look forward to our panelists insights and contributing to our and Congress' understanding of the opportunities and challenges that must be considered. As a reminder, the testimonies and transcript from today's hearing will be posted on our website at www.uscc.gov. And please mark your calendars for the Commission's next hearing, "China's Relations with U.S. Allies," which will take place on April 5th.

PANEL I INTRODUCTION BY COMMISSIONER MICHAEL R. WESSEL

HEARING CO-CHAIR WESSEL: I'll now kick off our first panel by introducing our two experts here to discuss the economic implications of Chinese 5G and Internet of Things standards and technology developments for the U.S.

First, we will hear from Chuck Benson, assistant director for IT in facilities services at the University of Washington. He has chaired the University's Protection of Industrial Controls Task Force, the University's central IT Service Management Board, and currently chairs the IoT Systems Risk Management Task Force for Internet2.

He will discuss how U.S. "smart" cities and "smart" campuses are incorporating Internet of Things and the potential economic opportunities and security risks for the U.S.

Next, we will hear from Doug Brake. He is director of telecommunications policy at Information Technology and Innovation Foundation, ITIF, specializing in broadband policy, wireless enforcement, and spectrum-sharing mechanisms. He previously served as a research assistant at the Silicon Flatirons Center at the University of Colorado, where he sought to improve policy surrounding wireless enforcement, interference limits, and gigabyte, gigabit network development.

He will examine U.S. and Chinese firms' efforts to set international 5G standards and the implications for U.S. global competitiveness.

Thank you both very much for your testimony. I'd like to remind you to keep your remarks to roughly seven to ten minutes so we'll have enough time for the question and answer session.

Mr. Benson, we'll begin with you, but in making your comments, please help us. Limit, if you can, deep dives into technologies like software defined radio and other issues, and, if you can, help us through some of the major policy issues that are before us.

Mr. Benson.

OPENING STATEMENT OF CHUCK BENSON, ASSISTANT DIRECTOR FOR IT IN FACILITIES SERVICES, UNIVERSITY OF WASHINGTON

MR. BENSON: I will do that. Thank you for the invitation and thank you for the opportunity to participate in this important work.

The Internet of Things Systems, combined with underlying wired and wireless infrastructure to support them, have the potential to bring substantial value to government, cities and universities, other institutions, and companies. However, without thoughtful application and awareness of the process and components, IoT Systems can also bring substantial risk to these same entities.

Three broad risks of IoT Systems to universities, institutions and cities include: supply chain risks; poor selection, procurement, implementation and management of IOT Systems; and lack of institutional governance and lack of awareness of social-technical issues in IoT Systems deployments.

Any of the above risks or some combination of those risks or other risks can have substantial negative impacts. Examples include, but are not limited to: use of large numbers of compromised IoT devices to build botnets for distributed denial of service attacks. Those are also called DDoS or DDoS attacks.

One example is the October 26 DDoS attacks using the Mirai malware that brought substantial impact to Internet services such as CNN, Netflix, the Wall Street Journal, Twitter, and many others. In the month right before that, a similar IoT-based DDoS attack was used to go after a very prolific security researcher and reporter named Brian Krebs. His site is krebsonsecurity.com. At the time, these were the biggest attacks ever seen--biggest attacks on bandwidth.

Another IoT-based botnet dubbed "Reaper" has been discovered in the past year by security researchers, and it appears to be substantially larger than the Mirai botnet. It hasn't been used yet, but it's been built. So the people are wondering what's it going to be used for?

Another example of a negative impact is IoT devices to facilitate attack on internal systems, to include critical infrastructure. One example is the Turkish pipeline explosion of 2008, and in that one, malicious actors went after the network video surveillance cameras, then used those as a jumping off point to get into the critical infrastructure and from there do malicious things that had a fireball explosion impact.

Another negative impact is use of IoT devices to collect and reroute sensitive information. On the personal level, this manifests itself in privacy issues. On the corporate level, it can be seen in corporate espionage. On the government/military/national security level, this can manifest itself in intelligence collection and critical systems disruption.

Another negative impact is compromising life-safety medical devices. Ever increasing numbers of these devices will be deployed in individuals and across populations. The inability to manage cyber risks in this space will stifle innovation and increase liability to providers.

Some examples include insulin pumps, defibrillators, blood-storing refrigerators. Other examples include medical equipment itself, diagnostic devices such as an MRI machine. Those can be hacked.

Another negative impact is use of IoT devices to cause large-scale disruption in economic systems. For example, in part or in whole, causing a hospital to fail, a manufacturer to fail, other companies to fail.

There can be--IoT devices and systems can be used to cause long-term product quality control problems as well as short-to-long-term disruption in companies of any sort.

This testimony will propose four activities the U.S. government can support and/or enhance that will help to mitigate these risks. These include standardized provenance vetting and reporting for IoT device components; support for increased U.S. labor force training in operational technology, or OT, skill sets; support for development of institutional and city IoT governance frameworks; support for data ethnography and socio-technical research and application in the context of IoT Systems.

These are not all the risks that IoT Systems pose to cities and institutions nor are these all the possible mitigation approaches, but it's a reasonable place to start.

The potential benefits of IoT Systems--there's many. Universities and institutions can benefit from an IOT System such as building automation systems, energy management control systems, safety systems, building and space access, and space being like the space in a building or campus or city, environmental control systems for large research environments, academic learning systems.

Cities can also benefit from IoT Systems supporting public safety. For example, surveillance of high crime areas, air quality monitoring by sector, transportation control and management systems, city accessibility guidance, and many others.

You can see the interest in IoT if you look at some of the major technology manufacturers, and just put in their name, a space, and then IoT in a Google spacebar, and everyone has got a page on it. Everyone has got a whole set on it.

Some of them are actually doing some things; some of it is kind of aspirational. But some of the big players include: Intel; Cisco; Microsoft; Siemens; Johnson Controls; Honeywell; AT&T; Verizon; and many others. And that's a subset of the big players. There's also a lot of medium-sized companies and lots and lots of small companies, and they're also relevant too, I believe.

To go back on some of the risks for a minute, we talk about supply chain risks. As we deploy these end-points on our buildings and our spaces and our institutions and our cities, we're deploying them by the thousands or hundreds of thousands or millions, and each of these, each of these--the thing in the Internet of Things, is a device that is networked, it computes, it interacts with the environment in some way.

Just the first two alone should be eye-opening for us--it computes and it's networked--and they're deployed all around us. Each of those devices have components, hardware and software, that come from many different places, and we really don't have a great way of knowing right now what's in those things, and we're deploying them by the hundreds of thousands or millions.

How IoT Systems are selected, procured, implemented and managed matters, and I will say that we're not very good at it right now. That's a different kind of system, and if we have a chance later on, we can talk a little bit more about that.

Governance and ownership of systems within a city, university or corporation. Right now there's not great governance. Cities and institutions don't ask yet good questions about what, what do I need, what's good for my city, what's good for my institution? And when we don't ask those things, it gets delivered to us. A vendor says, okay, this is what you need. This is not anti-vendor sentiment at all. We need those relationships. But cities and institutions need to be asking those questions themselves. What is a system; what is a good system; what are the criteria for performance?

I'll take about a minute or two to go through six characteristics of IoT Systems that make them different from traditional IT systems, and I think these are important to consider as we evaluate these in the context of institutions and cities.

One is just the large numbers themselves. In 2011, Cisco famously said there would be 50 billion connected devices by 2020. Now over the past couple of years, that number has gone up and down, but it's still--most people generally agree or most resources generally agree it's in the low tens of billions of devices in the next few years. Plus it has this exponential growth.

There's high variability of devices so there's high variability of what these devices do, and there's high variability of the things that are inside the devices. So you could have, you know, Fitbit devices, we can have pacemakers, we can have building automation systems, we have energy control and management systems, we could have military systems, we have research systems. There's all kinds of these different IoT devices, and they don't lend themselves to ready categorization or classification. So we have a hard time talking about these things.

Then there is variability within each device. I mentioned earlier there's multiple hardware and software components within these so that also makes it hard to categorize devices and get them kind of into risk categories so we can mitigate risk.

And that leads to another area which is lack of language. We don't have great language for talking about this stuff yet. It's new to most of us, and when we don't have good language for talking about it, it's hard to mitigate risk and it's hard to make good decisions about it.

Another substantial area is that these systems tend to span many organizations within an institution or within the city. So it's not like they just came into the central IT department and it just gets deployed from there. You have multiple groups that would be involved because these devices and this technology is getting embedded all around us.

You could have a planning and budgeting group involved; minor and major capital development; facilities management; central IT; distributed IT; multiple vendors; the actual end-users themselves. So what happens in an institution or city, the system spans all this, but it's not clear who the owner is. It's not clear who is managing that system to performance. And that leaves us pretty open.

Another aspect of these devices is that they tend to be out of sight and out of mind. You know we think about our work station computers that are sitting in our desktops, our laptops, our phones. We see those. We think about we should mitigate risks around those. Or if we go to a data center and look at racks of hardware, whether it's physical or virtual servers or whatever. We think about, okay, we should mitigate risks there. We tend not to think about all these computing devices that are embedded around us. So they tend to be out of sight and out of mind. This is like a real substantial social shift for us, I believe.

And, finally, there's lack of precedence for implementation. We're not good at it yet. Because it spans so many organizations within an organization or a city, it's new, it's new space. We don't have this deep history of saying, you know, last time we did it this way and I learned a few lessons and so we get this expertise of development now. We don't have that, and our colleagues and peers don't have that either. And even competitors, it's hard to look at a competitor and maybe observe what they're doing.

So this is new space for us, and it adds to the risk of the overall systems. So I think it's helpful to keep, keep these differences in mind as we think about IoT Systems in cities and institutions. That concludes my opening statement.

PREPARED STATEMENT OF CHUCK BENSON, ASSISTANT DIRECTOR FOR IT IN FACILITIES SERVICES, UNIVERSITY OF WASHINGTON

Hearing on China, the United States, and Next Generation Connectivity
Testimony before the US-China Economic and Security Review Commission

Internet of Things (IoT) Systems Risk Mitigation for Universities, Cities, and Institutions
with Observations on 5G and China
March 8, 2018

Chuck Benson
University of Washington

1. Overview

Internet of Things (IoT) Systems, combined with the underlying wired and wireless infrastructure that support them, have the potential to bring substantial value to government, cities, universities, other institutions, and companies. However, without thoughtful application and awareness of process and components, IoT Systems can also bring substantial risk and exposure to those same entities.

Three broad risks of IoT Systems implementations to universities, institutions, and cities include (not in order of priority):

- Supply chain risks
- Poor selection, procurement, implementation, and management of IoT Systems
- Lack of institutional governance and lack of awareness of social-technical issues in IoT Systems deployments

Any of the above risks or, more likely, combination of these and others can have substantial negative impacts. Examples include, but are not limited to:

- Use of large numbers of compromised IoT devices to build 'botnets' for Distributed Denial of Service (DDoS) attacks.
    - One example is the October 2016 DDOS attacks, using Mirai malware, that brought substantial impact to Internet services such as CNN, Netflix, the Wall Street Journal, Twitter, and many others. [i] The previous month, a large scale IoT-based DDoS attack was launched against popular and prolific security researcher Brian Krebs [ii]
    - Another IoT-based botnet dubbed "Reaper" has been discovered by security researchers that appears to be substantially larger than the Mirai-based botnet used in the attacks of fall 2016. It is not known what it's intended target may be. See Wired article, "The Reaper IoT Botnet Has Already Infected A Million Networks." [iii]

- Use of IoT devices to facilitate attack on internal systems, to include critical infrastructure.
    - One example is the Turkish pipeline explosion of 2008 where, "by hacking the video and sensors that closely monitored the … pipeline, the attackers were able to prevent operators from learning of the blast until 40 minutes after it happened, from a security worker who saw the flames."[iv]

- Use of IoT devices to collect and reroute sensitive information
    - On the personal level, this manifests itself in privacy issues
    - On the corporate level, this can manifest itself in corporate espionage
    - On the government/military level, this can manifest itself in intelligence collection and critical systems disruption

- Compromising life-safety medical devices. Ever increasing numbers of these devices will be deployed in individuals and across populations. Inability to manage cyber risks in this space will stifle innovation and increase liability to providers.
    - Some examples include insulin pumps, defibrillators, blood-storing refrigerators
    - Other examples include hacking medical equipment such as MRI machines[v][vi]

- Use of IoT devices and systems to cause large scale disruption in economic systems
    - Hospitals, manufacturers, others to fail
    - Long term product quality control problems
    - Short term to long term service disruption

This testimony will also propose four activities that US government can support/enhance that will help to mitigate these risks. These include:

- Standardized provenance vetting and reporting for IoT device components
- Support for increased US labor force training in Operational Technology (OT) skill sets
- Support for development of institutional and city IoT governance frameworks
- Support for data ethnography and socio-technical research and application in context of IoT Systems

These are not all of the risks that IoT Systems pose and these are not all of the potential mitigation approaches, but these constitute a good place to start.

Potential benefits of IoT Systems for universities, institutions, and cities

Potential benefits of appropriately selected, procured, implemented, and managed IoT Systems are substantial. Universities and institutions can benefit from IoT systems such as traditional building automation systems (e.g., HVAC), energy management and conservation systems, building and space access systems, environmental control systems for large research

environments, academic learning systems, and safety systems for students, faculty, staff, and the public. Cities also benefit from IoT Systems supporting public safety (e.g. surveillance of high crime areas), air quality monitoring by sector, transportation control systems, city accessibility guidance and support, and many others.

The *potential* value-add of IoT Systems for institutions, cities, and government is virtually limitless. Just check the IoT page of any major or minor technology provider. For example, all of these companies [vii] have substantial presence (or at least aspirational web pages) in this space:

- Intel
- Cisco
- Microsoft
- Siemens
- Johnson Controls
- Honeywell (e.g. Tridium Niagara)
- AT&T
- Verizon
- Many others

More on potential risks of IoT Systems for universities, institutions, and cities

The *actual* value-add is less than limitless and needs to consider substantial and often non-obvious costs and risks incurred. As mentioned above, these risks include supply chain risks of components and subcomponents, failure or inability to in systems selection, procurement, implementation and management, and issues around governance and socio-technical relationships.

- Supply chain risks – what is in those thousands, hundreds of thousands or more, devices that we are deploying in our institutions and cities?
- How IoT Systems are selected, procured, implemented, and managed matters (and we're not very good at it)
- Governance and ownership of systems within a city, university, or corporation. What is the criteria for system selection? What is the criteria for performance management of the system? Is it doing what we thought it would? Do we know what we thought it would do? Is it costing what we thought it would cost?

2. Characteristics of IoT Systems, IoT Devices, and the IoT Ecosystem

a. IoT Systems are different from traditional enterprise IT systems

IoT systems are different from traditional IT and information management systems and require new approaches to achieve investment value as well as to maintain or enhance an institution's

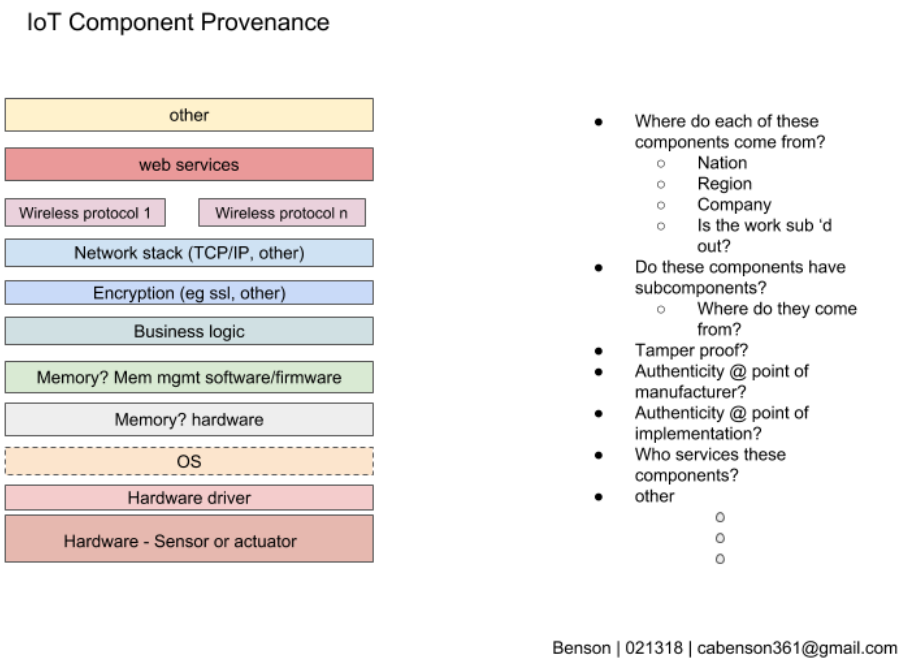
risk profile. Six factors distinguish IoT systems from other technology systems: (1) the large number of devices; (2) the high variability of types of devices and components within those devices; (3) the lack of language and conceptual frameworks to discuss and easily categorize and classify devices; (4) the fact that they span many organizations within an institution; and (5) the fact that the hundreds or thousands of devices embedded in the physical infrastructure around us tend to be out of sight and out of mind; (6) lack of precedence for IoT systems implementation and management.

Large numbers

In 2011, Cisco predicted that 50 billion devices will be connected to the Internet by 2020, and the growth appears to be compounding. It can be difficult to wrap one's head around the magnitude of this growth. To help, we can borrow from the "Rule of 72" used in finance, real estate, and other industries for quick and dirty approximations where the growth rate is divided into the number 72 to get an approximation of the time it takes the count of devices to double. For example, if you buy a house that increases in value at 6% per year, the time it takes to double in value is approximately 72/6 = 12 years. To use an example in the IoT space, an International Data Corporation (IDC) report suggests an 18.6% annual growth rate in the IoT market in manufacturing operations, starting with a $42 billion market in 2013.[viii] Applying the Rule of 72: 72/18.6 = 3.9, meaning the market size would grow from $42 billion to $84 billion by 2017 (an estimated 4 years).

High variability

The variety of types of devices and of the hardware and software components within each device is very high. IoT devices do numerous different tasks, including measuring building energy, video monitoring a space, reading a heart rate, and sensing air quality every few seconds in a research facility. Devices can have many different types of hardware from many different manufacturers as well as many different layers of software, each possibly from a different software company (or person). This huge variability contributes to the challenge of identifying device categories that can be helpful in developing risk management approaches. This variance also makes provenance tracking/management very difficult.



In their paper, "Internet of Things Device Security and Supply Chain Management," [ix] researchers Lee and Beyer contribute:

> "… policies relating to electronic supply chain security at national level are lacking … although companies try their best to follow piecemeal governmental and industry guidelines for supply chain security, this vigilance is only as strong as a company's dedication to security." [Supply chain policy shortcomings] "… arise because cybersecurity issues are highly complex and difficult for policymakers and industry leaders to reach agreement upon."

Lack of language

We do not have commonly accepted language or conceptual frameworks for talking about the IoT and these systems. Without a shared language, planning IoT systems implementations or managing risk around systems is very difficult. It is also challenging to establish standards and vendor contract performance expectations without this language.

Spanning many organizations

IoT systems tend to span multiple organizations within a higher education institution. For example, environmental control systems for large research spaces are rapidly increasing in number. These systems often sense and regulate air temperature, humidity, particulate levels, light, motion, and many other factors. These measurements are used for safety, energy efficiency, regulatory compliance, and other research needs. Implementing an environmental control system will likely involve an institution's central IT organization, the facilities

management group, the researcher/principal investigator, distributed/local IT organizations, and at least one and probably several vendors. Between these organizations are gaps through which systems accountability and ownership can fall. For example, the researcher thinks that the central IT organization is monitoring and managing the system and keeping it secure. At the same time, the central IT organization doesn't know what is being plugged into the network backbone. Each one hopes the other is managing the system well. Because of this spanning nature of IoT systems, there is often no overarching visibility, much less ownership and accountability, for the whole system.

Out of sight, out of mind

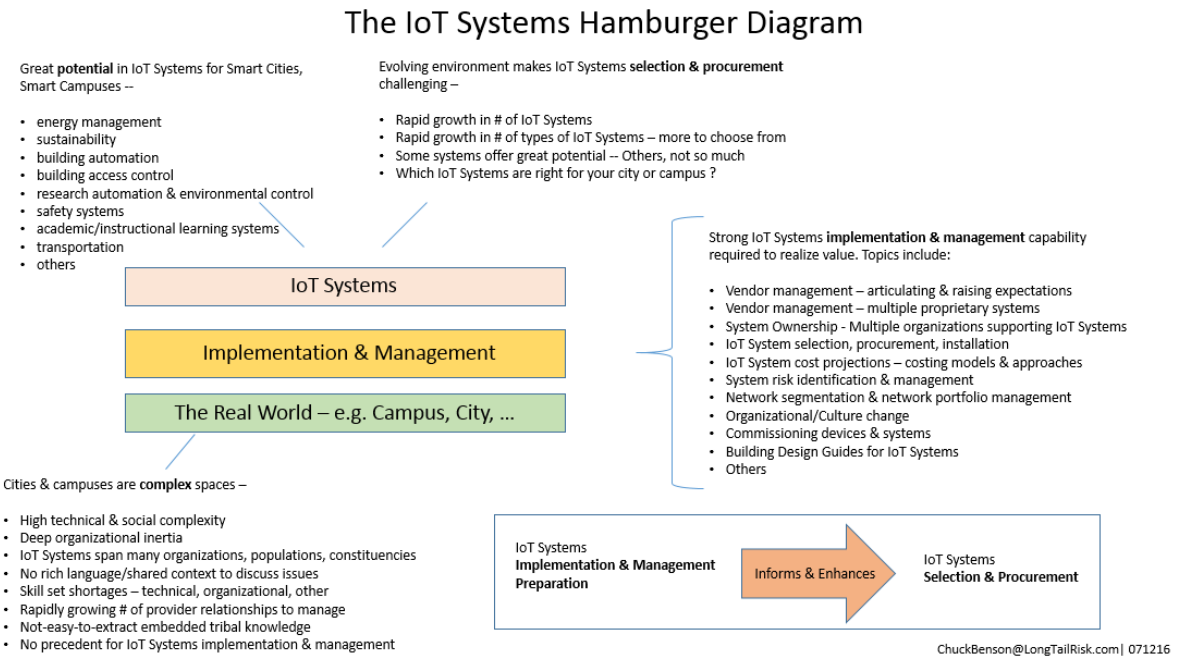
Finally, IoT systems are unique in that many of the technical parts of the IoT system—that is, the computing and networking endpoints—are built into the physical infrastructure, out of sight and out of mind. A smart grid or campus energy management system can easily have thousands of networked, computing, sensing endpoints that are built into campus buildings. We don't think about them because we don't see them.

Lack of precedence for implementation

Institutions, cities, and companies have very limited precedence for IoT Systems selection, procurement, implementation, and management. There is not a depth of history of implementations, colleagues with depth of experience to ask, or even competitors with depth of experience to observe. These technology (IoT) systems are now being thrown into traditional capital development, construction, and facilities operations organizations and implementing complex technology systems is not a part of the history or experience of these disciplines. Similarly, with an IoT System's broad geographical distribution of devices, requirement for trades skill to access these devices, and other factors, implementing IoT Systems is unfamiliar territory for central IT organizations as well.

b. How IoT Systems are implemented is critical

How IoT Systems are implemented is critical to successful implementation. Universities, cities, and other institutions have a substrate of historical complexities, organizational structures, skill set issues, and other factors. Selecting, procuring, implementing, and managing an IoT System to such a substrate is a critical endeavor and one in which we have little experience.



c. Measuring success of an IoT Systems Implementation for a university or city

Two overarching factors that can help measure or determine success for an IoT Systems implementation in a university or city are:

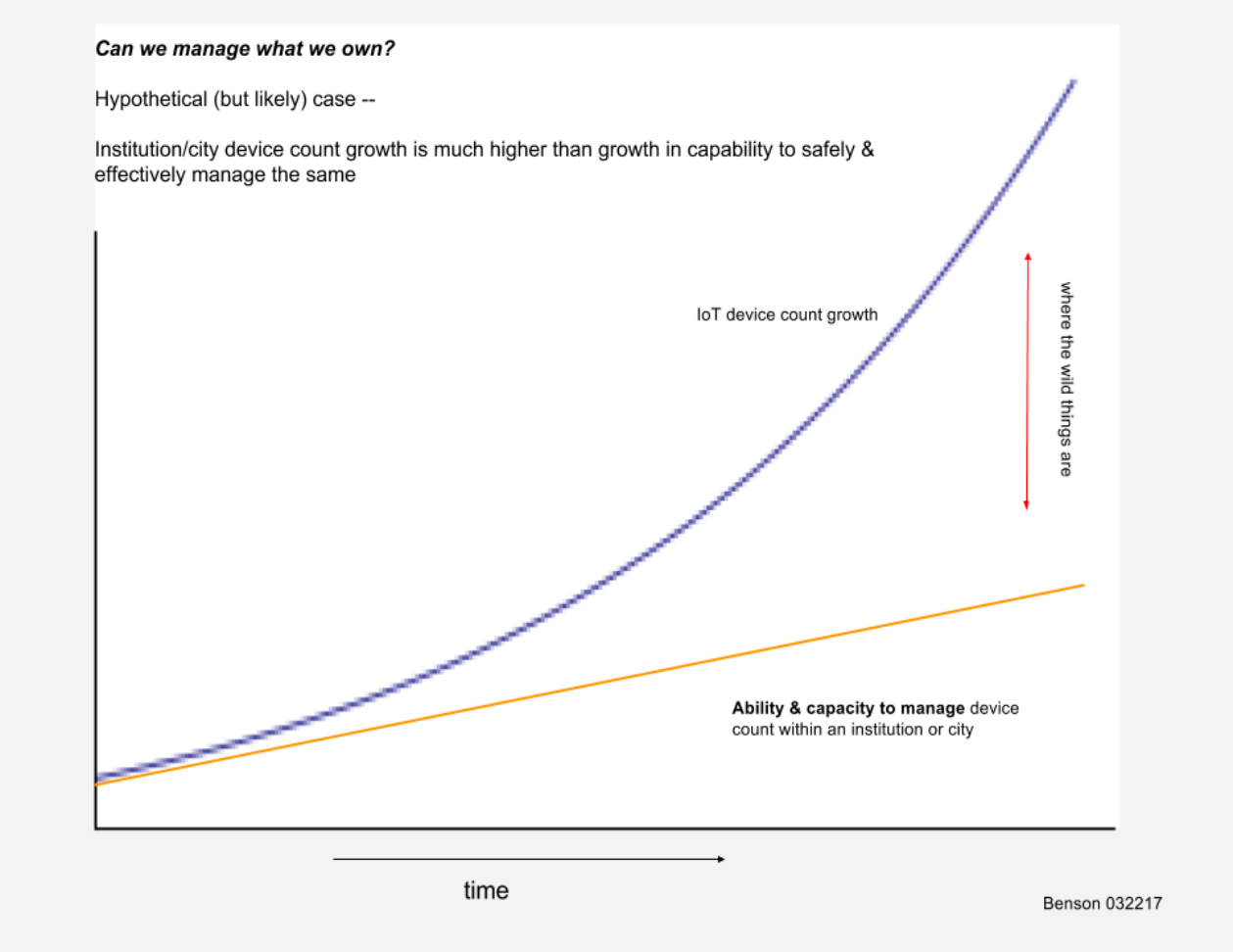
- ROI
  - Does the IoT System do what was expected and *deliver the value that was expected* at the *actual costs incurred* (vs projected costs)?
- Cyber risk
  - Did *implementation* of the IoT System make the cyber risk profile for the university or city worse?

Regarding the first — ROI, does the system do what we thought it would do at the costs/investment that we thought would be incurred? Determining costs of IoT Systems implementation is different from traditional enterprise systems. Most institutions and cities have little experience at it and are generally not very good at it. Further, other subtleties such as expectations of the data [x] created from deployed IoT systems across a spectrum of populations, demographics, and constituencies directly impact perceptions of system (and investment) success.

Regarding the second — cyber risk profile, did the IoT System implementation make things worse for the institution or city? Cyber risk profile degradation for an institution can come from

poorly configured devices, insufficient management resources (skill, capacity) to support IoT devices and data aggregators/controllers, inadequate vendor management, and others.

d. IoT Systems Manageability



A key component to both IoT Systems ROI and changes to cyber risk profile is the *manageability* of the IoT System.

> *IoT Systems — with their* ***multi-organizational boundary spanning*** [xi]*, unclear systems ownership and accountability, lack of precedence for implementation, and high number of networked computing devices ('Things') — are particular candidates for unmanaged/under-managed systems in a city or institution.*

IT systems that tend to be more manageable allow for more predictability in an institution's resource and cash flow planning. Criteria for high systems manageability include:

- having well-defined performance expectations
- thoughtful, thorough, and integrated implementation
- accessible training and documentation
- strong vendor support and strong vendor relationships
- others

Unmanaged or under-managed systems increase the likelihood of a cyber event such as device compromise or whole system compromise as well as facilitate potentially substantial operations disruption and unplanned financial burden.

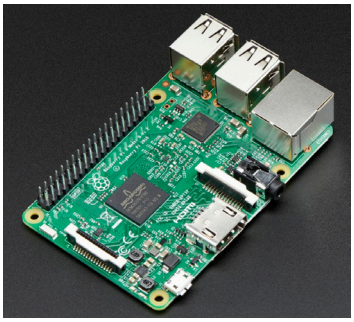
e. Low barriers to entry -- Makerspace, Raspberry Pi's, Arduino's, Adafruit, and …

It is increasingly easy to create the 'Thing' in the Internet of Things. The 'T' in IoT is a device that:

- is networked
- computes
- interacts (senses or changes) the local environment in some way

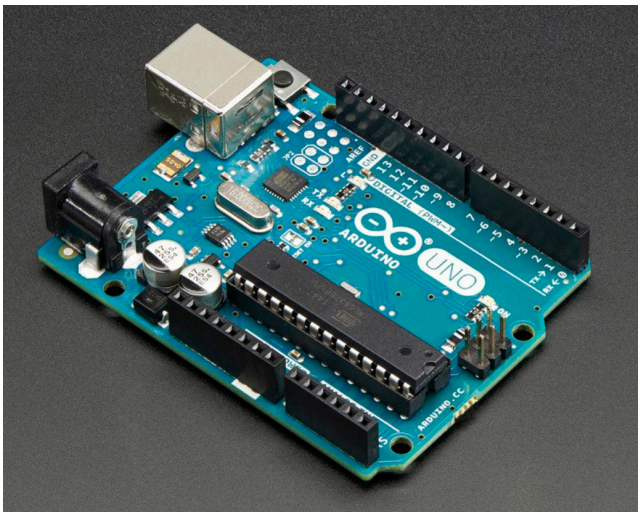
Whether hobbyists, participants in the Maker/Makerspace [xii] movement, commercial developers, or some combination, there are more and more components – simple and sophisticated, accessible development platforms, training, vendor support, and community-based support that facilitate IoT device and systems development. Three examples:

- Raspberry Pi [xiii]. The Raspberry Pi, developed and released in 2012 out of the UK, is a full featured computer the size of a deck of cards originally designed for education that costs approximately $35. It supports multiple Linux-based operating systems and has a very rich set of features to include wireless support, video (HDMI) support, audio support, input/output for attaching sensors, actuators, and other devices. Importantly, it has strong and broad community support.



- Arduino [xiv] . The Arduino, developed and released in 2003 out of Italy, is also a full-featured computer at a cost of ~$30. Though the Arduino operates without the support

of a traditional operating system such as Linux, it has strong development tools, and a huge community support base. It can be argued that this small computer kicked off the Maker/Makerspace revolution.



- Adafruit [xv] was founded in 2005 by MIT engineer, Limor "ladyada" Fried. Adafruit sells electronics components such as Arduino and Raspberry PI. The company also designs, makes, and sells its own products as well in additional to a wide array of support tools and components. Importantly, the company has an increasingly sophisticated training program for device design and production. The founder was also featured on the cover of Wired magazine in March 2011.

f. Cloud services in direct support of IoT System and device deployment

There are rapidly evolving cloud platforms to support IoT device/system development and deployment. IoT devices and systems often go hand in hand with cloud-based services. These are also easy to access and are becoming less and less expensive. These cloud services are designed specifically for IoT devices and systems and there is substantial competition between them to garner IoT space mind and market share. Examples of IoT cloud services include:

- AWS IoT [xvi] -- with web tag line – "A system of ubiquitous devices connecting the physical world to the cloud."
- Google Cloud IoT [xvii] – with web tag line – "Platform for intelligent IoT services"
- Microsoft Azure IoT Suite [xviii] – with web tag line – "Capture and analyze untapped data to improve business results"

These are just a small subset of the cloud services being offered to support IoT devices and IoT systems. Many cloud service solutions will, in fact, incorporate one or more other cloud services.

g. Shodan & Censys: Freely available attack research tools/risk mitigation tools

There's good news and bad news when it comes to getting a quick snapshot of an institution's public-facing IoT systems exposure. The good news is that tools for doing this are publicly available. The bad news is that tools for doing this are publicly available. Anyone—those in institutions and cities as well as those criminal and nation-state actors with malicious intent—can use the same tools. However, since those with malicious intent are most likely using their own, nonpublic approaches, these publicly available tools might well be a net benefit to higher education (if we use them).

Shodan [xix] a private endeavor, is the best-known of these public tools and has been around the longest. Censys [xx], stemming from research at the University of Michigan and the University of Illinois at Urbana-Champaign, is the newer entry into the space. Although their approaches are different, the two tools do similar things: they scan (almost) all publicly available IP addresses, record the responses, and make the IP addresses, responses, and metadata (e.g., location and timestamp data) available to the public. The scans look for devices often associated with IoT and traditional industrial control systems. Both tools have the ability to download data, and they offer APIs that allow direct access for further analysis. So, by using either or both tools and searching the IP address space of a campus, institutional IT leaders can get an idea of current exposure—results that can be surprising.

h. Socio-technical and cultural aspects of successful IoT Systems integration

There are substantial socio-technical aspects to implementation of IoT systems on university campuses, cities, and others. With widespread IoT device sensing, data creation, data aggregation, analytics, and business and social decisions made on the same, we are in a new world. Three aspects of this new world include:

- How IT and built environments technology worlds come together
- How constituents of an IoT System perceive value of the system
- Governance

Blending Information Technology and Operational Technology

To the first point, the technology deployed in built environments (buildings, campuses, cities, etc.) is often called Operational Technology (OT). This is the technology device that senses the environment (e.g. outside air temperature, electrical power consumption, measures heat usage in a building, or other) and/or interacts with the environment (e.g. makes a remote HVAC thermostat or blower setting change, moves a networked video surveillance camera, or other).

These professional skill sets that deploy, configure, manage, and monitor these sensors and actuators *are in short supply*. These skillsets are a cross between traditional trades skill sets (such as electricians) and IT skill sets (with software configuration and testing skills). The skill sets are in short supply and in high demand. Without them, deployment demand for IoT Systems (or 5G) cannot be met and the risk of systemic (e.g. thousands or more of devices) misconfiguration and lack of ongoing IoT systems support is very high. This misconfiguration/poor configuration, in turn, results in lost ROI and a substantially degraded security posture for the campus, city, or institution.

Adding to the challenge is that the skill sets of traditional IT and traditional OT have very different cultural backgrounds. Historically, the professional deploying the OT device has come from a building and maintenance background, for example a facilities management or construction organization. Because these professionals build and/or maintain buildings expected to last decades, they tend to think in terms of decades – long term support of an operational building. Further, these professionals, understandably, tend to be motivated not to change a system (electrical power delivery, heat delivery, as examples) that is working -- something of an, “if it ain’t broke, don’t fix it” approach. IT professionals, on the other hand tend to think in terms of months, weeks, and days and they are frequently changing software configurations, software versions, etc. in an attempt to keep up with newly discovered vulnerabilities and types of attack that are discovered almost daily.

The differences in the cultural mindsets of these two professions become readily apparent as IT and OT professionals and teams come together to implement and manage IoT systems. Successful, risk-mitigated systems implementation requires mature, experience skill sets that

can navigate the blending of these two historically disparate cultures. And again, these skill sets are in short supply.

Understanding data expectations is essential to IoT Systems & smart city success

One of the subtle but powerful factors affecting IoT Systems implementation and management success in complex organizations such as a smart campus or smart city is *the organizational and cultural change required in becoming a data-centric organization.*

In most cases, this is not a small transition. The evolutions of these cities and institutions has been from a place of relatively limited data available across multiple contexts. When an organization begins to shift, or seeks to shift, to an organization where data production, acquisition, consumption/analysis, and management – such as that coming from an IoT System -- are core to its operation and to its perception of self, subtle but powerful cultural and organizational change is required.

Data generation and/or acquisition is a major component in almost all IoT Systems that may be deployed in support of smart campuses and smart cities. *Data creation and data actionability is often where much of the value is derived from an IoT System deployment.* The challenge is that the expectations of data from the many constituencies and consumers can vary in significant ways and these variances in expectation, in turn, influence perceptions of IoT Systems, and in turn smart city system, success. Further, *early IoT System implementations that are viewed as failures not only mean lost investment on those particular systems, but also that these failures will (understandably) make constituents wary of funding or deploying subsequent systems.*

Reflecting on and planning for what expectations of data are in different constituencies and contexts can substantially help identify criteria for perceptions of successful IoT Systems implementations and smart city deployments.

Institutional governance – one example – our approach at the University of Washington

Governance and guidance for IoT Systems implementations in most universities and cities is nascent. At the University of Washington, we have instantiated and operated task forces to profile the problem of growing IoT Systems risk as well as plan for mitigation of the same. For example, we ran the Protection of Industrial Control Systems task force in 2013-2014 and the University of Washington (UW) Compliance IoT Systems Risk Mitigation Task Force (current). This latter task force has reports to University of Washington Regents which reflects the university's growing awareness and intention of the effort. The university also supported my effort of chairing a national IoT Systems Risk Management Task Force for Internet2 [xxi].

Our current effort, the University of Washington Compliance IoT Systems Risk Mitigation Task Force, seeks to:

- Increase awareness of IoT Systems risks and benefits in all facets of the institution
- Provide guidance and oversight for IoT systems selection, procurement, implementation, and management
- Increase inter-organizational coordination for managing IoT Systems across the institution
- Identify clear IoT Systems owners within the university
- Establish robust expectations for IoT Systems vendors and providers
- Identify a workable IoT System and device classification and categorization to assist in managing risk
- Propose an institutional governance structure for providing oversight to IoT Systems deployments

Participating organizations and roles within the university include:

- Major and minor capital development
- Planning and budgeting
- Energy management and conservation
- Central IT
- Facilities management
- Academic research
- UW Office of Chief Information Security Officer (CISO)
- UW Medicine Office of Chief Information Security Officer (CISO)
- Institutional privacy official office
- Enterprise risk management and compliance office

While there is more work to be done, Task Force-led directed discussions and related efforts involving these multiple organizations and departments are already creating benefit in terms of increased awareness and enhanced communication on the topic IoT Systems implementation and risk mitigation.

3. Observations on IoT, 5G, and China

IoT and 5G

I am not an expert on 5G, but I can make observations based on existing IoT deployments with existing wired and wireless approaches and my understanding of potential 5G features and capabilities.

Fully deployed and managed, 5G purports [xxii] to deliver benefits that include:

- Increased bandwidth
- Support of increased device count

- Reduced latency

The effects of a fully-deployed, as advertised 5G system would serve as an effect multiplier for IoT Systems in universities, institutions, and cities. That is, there would be:

- More potential value-add and potential social benefit because of increased capacity and feature sets of part of the network supporting IoT devices and systems
- More cyber risk and potential for lost investment if systems are not thoughtfully implemented

Another aspect that would also act as a multiplier would be that a deep and broad and fully-deployed 5G network could allow IoT Systems providers to 'hop over' constraints of existing city, university, and other institutional legacy network systems.

Importantly, there is still capacity for IoT Systems evolution with existing wired and wireless technologies. A fully-deployed, functional, and well-managed 5G system would add more capacity for IoT Systems development, but there is still room to work with existing wired and wireless deployments.

Also important to note is that a full-featured, deep, and broad 5G deployment will require:

- Increased technical (OT) support for the more numerous and dense small cells and antennae required of 5G technology
- More negotiation and bureaucratic/relationship navigation between vendors, cities and institutions for issues such as utility pole use and other spaces for cell/antenna deployment

From my point of view, it is not clear that these issues can be addressed quickly or easily.

Because of these uncertainties, a systematic approach to 5G deployment in the United States is highly desirable. A rushed approach would only exacerbate the non-trivial risks stemming from IoT Systems implementation.

Two comments on IoT and China

An anecdote on electronic component provenance

While the following anecdote is certainly not indicative of all manufacturing processes, it has always stuck in my mind as a reminder that not everything, i.e. electronic component, may be where I think it's from or coded the way I think it's coded.

Andrew ('bunnie') Huang, MIT electrical engineering PhD, and his business partner Sean ('xobs') Cross [xxiii] gave a talk at the 2013 Chaos Computer Congress [xxiv] on hacking SD cards. SD cards are the removable memory cards that go into digital cameras and other electronics.

In the course of the presentation, Huang describes vast bins of memory cards of ranging quality, size, and performance in the market of Huanqiangbei in Shenzhen, China. He talks about card relabeling as a common practice to adjust for sub-performing cards as well as card factories that have very few access controls regarding what configuration files are written to cards and chips and how they are configured. Transcribing from the presentation video (at approximately 50:45):

> ".. when we've been to the factories where they burn [program] the firmware in, you can basically just walk in and go up to the burner [component programmer] and replace the files on it … literally, there were chickens running through the factory … there's no security, there's no badges … they make these things [components] and ship them all over the world …"

My previous naïve assumption that all electronic parts were created and programmed in carefully controlled and audited environments was appropriately debunked. Many buy from this kind of loosely controlled electronics market because the components are very inexpensive compared to a highly regulated manufacturer. IoT devices have many of these kinds of components.

A view of the Maker culture in China

IoT devices are a core component of many "Maker" activities. The February/March 2018 issue of the popular Make magazine has a section focusing on the Maker culture in China. The Maker culture, in turn, is substantially supported by and enhanced with IoT technology. [xxv]

One author, a 23 year old woman from Shenzhen, speaks of establishing the first Open Source Hardware Association certified project in China. She states that Shenzhen used to be known as the cloned/copycat capital of the world but that that is no longer the case. She also has a YouTube channel [xxvi] dedicated to her Maker work.

Back to Table of Contents

Another writer in the issue is the Director of the International Collaboration of the Shenzhen Open Innovation Lab. She discusses helping to organize the "Maker Workshop in the National Mass Innovation and Entrepreneurship Week – a major national event to promote innovation policy by the Premier Li Keqiang." She also discusses Maker partnerships with other countries to include Britain, Nigeria, Ethiopia, Peru, and Pakistan.

A third contributor is the general secretary of the Shenzhen Industrial Design Association (SIDA) which works to "promote the importance of industrial design to government and business." SIDA has over 700 institutional members and works with "over 100,000 industrial designers in Shenzhen." Further, she says,

> "Today, Shenzhen has one of the best government policies in the world to encourage creativity and innovation in industrial design … and the Shenzhen Industrial Design Faire has become the largest industrial design event in the world."
>
> "…Shenzhen industrial designers … help Shenzhen manufacturers move up the value chain … and building the bridge between global makers and the Shenzhen ecosystem …"

These attestations by the article's authors convey a very active, substantial, and growing IoT and Maker effort at the individual and group level that is being integrated with robust industrial design approaches. This integration and mutual leveraging of efforts will only continue to drive the IoT movement in China.

There is also an increasing amount of IoT curricula in United States schools and programs. [xxvii] It is not clear to me whether China or the US as the advantage in this pipeline.

4. Recommendations

While there are many opportunities for the US Government to help, both in terms of IoT Systems risk mitigation and enhanced value from IoT Systems, four recommendations are below.

1. Develop a standard system for reporting electronic component provenance of firms developing IoT devices and systems
    a. NIST, ISO, SAE and others have done some work here [xxviii]
    b. It is important that this system is implementable in practice
        i. Balance is needed between thoroughness and pragmatism
        ii. Approaches that are overly burdensome will not be adhered to and thus be ineffective
        iii. Burden will vary with firm size

2. Fund and support development of operational technology (OT) skill sets
    a. The current shortage of these critical skill sets contributes to:
        i. poorly implemented systems,
        ii. increased cybersecurity risk to institutions and cities,
        iii. reduced opportunity for value-add and returned investment

3. Fund and support development of governance frameworks for cities and institutions
    a. Universities, cities, and institutions can use these frameworks as templates for their own organizations that they can continue to evolve to meet their needs

4. Fund and support data ethnography and social-technical science research as it relates to IoT Systems.
    a. Interpreting and mediating the unprecedented amounts and types of IoT Systems data is a very new space for universities, institutions, and cities and is critically important.
    b. Data ethnography and other social-technical research can be used to inform institutional and city leadership as they become increasingly immersed in, affected by, and dependent up IoT systems.

References:

[i] "2016 Dyn cyberattack", Wikipedia, https://en.wikipedia.org/wiki/2016_Dyn_cyberattack, accessed March 4 2018

[ii] Brian Krebs, "Krebs on Security Hit With Record DDOS", https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/, September 21 2016

[iii] Andy Greenberg, "The Reaper IoT Botnet Has Already Infected A Million Networks", https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/, October 20, 2017

[iv] Dan Goodin, "Hack said to cause fiery pipeline blast could rewrite history of cyberwar", https://arstechnica.com/information-technology/2014/12/hack-said-to-cause-fiery-pipeline-blast-could-rewrite-history-of-cyberwar/, December 10 2014

[v] Rachel Arndt, "Hacked medical devices could wreak havoc on health systems", http://www.modernhealthcare.com/article/20180120/NEWS/180129999, January 20 2018

[vi] Kim Zetter, "It's insanely easy to hack hospital equipment", https://www.wired.com/2014/04/hospital-equipment-vulnerable/, April 25 2014

[vii] Intel -- https://www.intel.com/content/www/us/en/internet-of-things/overview.html
Cisco – https://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html
Microsoft – https://www.microsoft.com/en-us/internet-of-things
Siemens -- https://www.siemens.com/global/en/home/products/software/mindsphere.html
Johnson Controls -- http://www.johnsoncontrols.com/buildings/specialty-pages/iot
AT&T -- https://iotplatform.att.com/
Verizon -- http://www.verizonenterprise.com/products/internet-of-things/

[viii] "New IDC Forecast Asserts Worldwide Internet of Things Market to Grow 19% in 2015, Led by Digital Signage," press release, May 19, 2015.

[ix] Stacia Lee, Jessica Beyer, "Internet of Things Device Security and Supply Chain Management," https://www.wilsoncenter.org/publication/internet-things-device-security-and-supply-chain-management , November 22 2017

[x] Chuck Benson, "Understanding data expectations is essential to IoT Systems and Smart City/Smart Campus success", http://longtailrisk.com/2016/07/27/understanding-data-expectations-key-iot-systems-smart-city-success/, July 27 2016

[xi] Chuck Benson, "Organizational-spanning characteristics of IoT systems", http://longtailrisk.com/2016/06/07/organizational-spanning-characteristics-iot-systems/, June 7 2016

Back to Table of Contents

[xii] "Maker culture", Wikipedia, https://en.wikipedia.org/wiki/Maker_culture, accessed March 2 2018

[xiii] Raspberry Pi, https://www.raspberrypi.org/, accessed March 2 2018

[xiv] Arduino, https://www.arduino.cc/, accessed March 2 2018

[xv] Adafruit, https://www.adafruit.com/about, accessed March 2 2018

[xvi] AWS IoT, https://aws.amazon.com/iot/, accessed March 2 2018

[xvii] Google Cloud Platform, https://cloud.google.com/solutions/iot/, accessed March 2 2018

[xviii] Microsoft Azure IoT Suite, https://azure.microsoft.com/en-us/suites/iot-suite/, accessed March 2 2018

[xix] Shodan, https://www.shodan.io/, accessed March 2, 2018

[xx] Censys, https://censys.io/, accessed March 2 2018

[xxi] Internet2, https://www.internet2.edu/about-us/, accessed March 4 2018

[xxii] Sascha Segan, "What is 5G?", PC Magazine, https://www.pcmag.com/article/345387/what-is-5g, accessed March 3 2018

[xxiii] Ebony Calloway, "Engineer Spotlight: bunnie and xobs and the Essential Guide to Electronics in Shenzhen", July 27 2016

[xxiv] Andrew 'bunnie' Huang, Sean 'xobs' Cross, "The Exploration and Exploitation of an SD Memory Card," 2013 Chaos Computer Congress, http://www.bunniestudios.com/blog/?p=3554, comments at time 50:45

[xxv] Naomi Wu, Vicky Xie, "Shenzhen Standouts", Make magazine, February/March 2018

[xxvi] Naomi Wu, YouTube Channel, https://www.youtube.com/channel/UCh_ugKacslKhsGGdXP0cRRA, accessed March 2 2018

[xxvii] Jeffrey Voas, Phillip Laplante, "Curriculum Considerations for the Internet of Things", https://www.computer.org/csdl/mags/co/2017/01/mco2017010072.html, January 2017

[xxviii] NISTIR 8200, "Interagency Support on Status of International Cybersecurity Standardization, https://csrc.nist.gov/CSRC/media/Publications/nistir/8200/draft/documents/nistir8200-draft.pdf

Back to Table of Contents

OPENING STATEMENT OF DOUG BRAKE, DIRECTOR OF TELECOMMUNICATIONS POLICY, ITIF

HEARING CO-CHAIR WESSEL: Thank you, Mr. Benson.

Mr. Brake.

MR. BRAKE: Co-chairs Wessel and Wortzel, and members of the Commission, thank you very much for having me here.

It's a pleasure to be here to discuss "China, U.S. and Next Generation Connectivity." I'm Doug Brake. I'm here in my role as Director of Telecommunications Policy at the Information Technology and Innovation Foundation, or ITIF. ITIF was founded in 2006. We are an independent nonprofit, nonpartisan research and educational institute--a think tank.

We consider it our mission to formulate, evaluate and promote public policy solutions that accelerate innovation and boost productivity to spur growth, opportunity and progress.

The subject of the hearing you have convened today is knotty and complex but incredibly important. I hope to cover three main issues related to China, the U.S. and Next Generation Connectivity.

First, why it's important that the United States aggressively deploy 5G networks and the policy levers we can lean on to achieve robust wireless platforms for continued innovation.

Second, I'd like to discuss China's efforts to lead in 5G and compare its strategic orientation with that of the United States.

Last, I'd like to address concerns around national security risks in the telecommunications equipment supply chain.

First, the opportunity of 5G and why the U.S. must adjust policy to ensure next generation platforms flourish here.

One can appreciate the 5G opportunity by looking to the astounding innovation enabled by 4G wireless broadband. It has been a little over a decade since the first introduction of the iPhone and the evidence of mobile broadband's power as a platform for economic growth is all around us. Beyond entertainment, the mobile broadband ecosystem has improved productivity through transportation, payments, navigation, logistics and more.

U.S. companies played a major role in handsets, software, network switches and underlying technology of the LTE platform. Importantly, we also led in the deployment and use of 4G, enabling the new app-based economy and related mobile innovations.

While 4G was focused on the broadband use case--bringing the web to mobile--5G is envisioned as a much more flexible system, able to adapt to a wide variety of different applications that will integrate with more sectors of the economy. It will be able to support dramatically lower latency, allowing for real-time applications.

5G will also allow for massive Internet of Things deployments, with simpler coding parameters for much cheaper devices with dramatically longer battery life where called for.

In the United States, 5G is estimated to require about $275 billion in infrastructure investment and ultimately contribute three million jobs and $500 million--500 billion--excuse me--in GDP growth to the U.S. economy.

5G technology will require a change in architecture, however, eventually seeing deployments of hundreds of thousands of what are called "small cells." This shift from large 200 foot-tall macro towers to much smaller, lower-powered but more numerous small cells requires a retooling of regulations and permitting processes at the local level.

Because of the tremendous cost and difficulty in deploying such infrastructure, standards organization 3GPP has developed two versions of the 5G air interface that connects handsets to wireless base stations. The first version, referred to as "non-standalone," requires an LTE anchor, allowing operators to leverage existing investments in 4G networks.

Rollout in 5G is likely to be an evolutionary process in the United States, with carriers first looking at incorporating aspects of 5G through this non-standalone version, relying on existing LTE networks and gradually deploying 5G hotspots, wireless point-to-point connections to the home, with pure 5G technology coming later.

To accelerate deployment in the United States, we must update regulations and permitting processes to streamline small cell deployments, as well as make additional spectrum available at low-mid and high frequencies with a variety of different licensing models.

China has recognized the tremendous opportunity of 5G and has oriented policy accordingly in several key areas, which brings me to the second set of issues: China's approach to influencing the direction of 5G and its plans for deployment.

China has significantly increased its presence in standard-setting organizations like 3GPP and international institutions like the International Telecommunications Union.

In some ways, China's engagement with standard-setting institutions is an encouraging sign. In the past, China has gone its own way with technology standards, most notably with its favoring time-division duplexing for 3G and 4G standards but also in important areas such as WiFi related protocols.

China would rely on its own standards to foster domestic production, avoid royalties to western companies, and gain leverage over those trying to enter its large market.

While Chinese participation in global standards setting means a more interoperable market with better opportunities for trade, it also signals China's efforts to dominate many technology areas related to 5G.

Indeed, Chinese firms have aggressively invested in research and development in telecommunications equipment, chipsets, coding methodologies, handsets, et cetera. By some measures, China has already secured ten percent of the essential patents for 5G.

Developing the technology matters. IT supply markets are large valuable sectors, but 5G standards and presence at international bodies brings influence, bargaining power and scale.

U.S. operators have set an aggressive timetable to deploy early versions of the Phase 1 standard, looking at commercial launches this year. U.S. operators will explore a more experimental evolutionary path, leveraging our existing LTE networks and transitioning to 5G systems where it makes the most economic sense.

Chinese operators, on the other hand, appear content to wait for a uniform global standard of pure 5G with commercial launches targeting 2020.

China Mobile is explicit in its plans for an aggressive push of the second phase of the 5G standalone specification. This will prove more expensive for the state-directed operator at first but will gain early economies of scale in the particular technology and the vendors they rely on.

The United States should first and foremost adjust policies to ensure we lead in deployment and adoption of 5G relying on our private sector competition and not entertain ideas of government-led deployments.

Lastly, I want to address concerns about security risks in the telecom equipment supply chain. The United States should approach Chinese vendors, such as Huawei and ZTE, within the scope of the broader strategic effort to confront China's innovation mercantilism. Rather than a presumptive blocking of Chinese equipment from entering the U.S. market, we should develop

clear processes and institutions to evaluate any potential security threat, ideally in cooperation with like-minded allies.

Huawei has made clear that the actions to date that have effectively blocked U.S. entry are perceived as unfair, punitive and prejudiced. As a general matter, we should avoid this sort of perception if we are to guide China to a rules- and market-based policies and continued liberalization of the Chinese market.

By working with other large western markets, making clear participation would be barred if an intentional vulnerability was discovered, would change the economic calculus of any potential security threats.

We should also continue to rely on formal processes such as Section 301 investigations and other opportunities within the WTO within a broader strategic coalition. But a heavy-handed tit-for-tat approach would not be effective to return to rules-based trade and ongoing development of a mutually beneficial innovation ecosystem going forward.

Thank you very much, and I look forward to your questions.

PREPARED STATEMENT DOUG BRAKE, DIRECTOR OF TELECOMMUNICATIONS POLICY, ITIF

ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Testimony of

Doug Brake

Director of Telecommunications Policy

Information Technology and Innovation Foundation

Before the

U.S.-China Economic and Security Review Commission

Hearing on

“China, the United States, and Next Generation Connectivity”

March 8, 2018

2255 Rayburn House Office Building

Washington, DC

INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION | 1101 K STREET NW | SUITE 610 | WASHINGTON, DC 20005
ITIF.ORG | MAIL@ITIF. ORG | (202) 449-1351 | FAX: (202) 638-4922

Co-chairs Wessel and Wortzel and members of the Commission, thank you for this opportunity to discuss the views of the Information Technology and Innovation Foundation on China, the United States, and next generation connectivity.[1]

INTRODUCTION AND SUMMARY

Next generation connectivity, 5th Generation (5G) in particular, represent a tremendous economic opportunity. Deploying 5G at scale, and seeing it leveraged for productivity gains throughout the economy, should be a national imperative. There are several technological components to 5G, but the key architectural shift requires far more cell sites, meaning an expensive infrastructure deployment justifying a rethinking of local permitting policies and federal regulations.

The Chinese are extending their influence in standards organizations and international bodies like the International Telecommunications Union (ITU). They are also engaged in intensive research and development, and already making key contributions to essential 5G patents. While they may not be the first to use 5G, many expect they will aggressively deploy a final 5G specification at tremendous scale. The U.S. government should focus on improving the investment conditions for deploying 5G through reforms to siting and permitting policies and make more spectrum available on a flexible licensed, unlicensed, and shared basis.

The United States should continue to rely on its competitive private sector to deploy 5G networks and not consider a government-built network. Furthermore, any policy focused on specific Chinese firms must be considered as a component of a broader, nuanced strategy to return to a rule-of-law, market-driven expectation on trade and protection of intellectual property. Presumptive blocking of specific firms is likely not the best route.

5G REPRESENTS A TREMENDOUS ECONOMIC OPPORTUNITY

Discussions of the evolution of mobile classify the various technologies into different "generations." The first generation of mobile was focused purely on basic voice service, and was an analog (as opposed to digital) service; 2G was still focused on voice, but made the switch to digital standards; 3G introduced data services, expanding the functionality beyond voice and including multimedia, texting and some limited internet access. It was not until 4G that we got a full Internet Protocol (IP)-based specification. The waves of new generations of technology have come in roughly decade-long cycles, 1G mobile voice in the 1980s, 2G in the 1990s, 3G basic data in the 2000s, and 4G LTE data in the 2010s.[2] 5G is expected to not just bring faster downloads, but bring a much more flexible network that can adapt to the needs of different verticals throughout the economy. It will bring a new architecture, with significant changes to the core network and potentially seeing deployments of hundreds of thousands of small cells.

Within the United States, the four main wireless carriers are racing to deploy 5G, but generally different varieties. For example, Verizon, partnering with Ericsson and Samsung, has been focused on a fixed-wireless flavor of 5G that will beam connectivity to a piece of equipment fixed on the side of a building.[3] AT&T is focused on first deploying wireless hotspots, rather than phones. Cable companies are also exploring their role in 5G networks, and may be well positioned considering their extensive existing wireline facilities.

A report by Accenture commissioned by the wireless trade association CTIA estimates 5G will require infrastructure investments by U.S. telecom operators of about $275 billion, and ultimately contribute 3 million jobs and $500 billion in GDP growth to the U.S. economy.[4] Some of the expected benefits are expected to flow from "smart city" applications. For example, 5G connectivity, combined with data analytics, could be applied to the "management of vehicle traffic and electrical grids could produce $160 billion in benefits and savings through reductions in energy usage, traffic congestion and fuel costs."[5]

5G is being designed to meet three general types of use cases: enhanced mobile broadband, massive Internet of Things (IoT) connections, and critical high-reliability and low-latency services. The goal is to have a flexible network that can adapt to a wide variety of use cases throughout a number of different vertical industries. Enhanced mobile broadband should see faster throughput (with multi-gigabit per second speeds possible), latencies as low as 1milisecond, and a consistent user experience. Massive IoT services within 5G are being designed for power efficiency and simplification to keep device cost low, as well as long range and support for far denser IoT connections.

There are certainly technologies other than 5G to perform IoT services. Some are wireless-carrier centric such as LTE-M or Narrow Band IoT (NB-IoT). Others leverage unlicensed spectrum. The Internet of Things is expected to contribute up to $11 trillion in value per year globally by 2025.[6] Forecasters expect global cellular IoT connections will increase from 520 million in 2016, to 2.5 billion in 2025.[7] Companies can use the Internet of Things to become more efficient, for example by reducing downtime in factories as they constantly monitor machine performance to address issues before they become problematic, or as they use real-time data about customer demand to better manage supply chains.

Successfully deploying and utilizing next generation networks is a crucial goal to spur economic growth.

NEXT-GENERATION CONNECTIVITY INCLUDES A VARIETY OF TECHNOLOGICAL COMPONENTS

Understanding how the United States and China are positioning economic and policy forces around next generation connectivity requires an understanding of what we mean by next generation connectivity. This section offers a brief, non-technical background on the technological components of 5G networks and the Internet of Things (IoT) for the purposes of discussing the strategy of different countries and companies.

The New Radio (NR) Standard

The Third Generation Partnership Project (3GPP), a cluster of seven different telecommunications standard development organizations, has been hard at work developing the 5G radio and related standards. The aptly named "New Radio" (NR) standard allows base stations to communicate with mobile devices. There are other important standardization processes for other parts of the network, but the radio interface is a defining characteristic of the transition to the next generation.

The NR standard has been broken into two phases: standalone and non-standalone. Both are components of 3GPP Release 15, but the key difference is the non-standalone version utilizes an

LTE control channel or anchor, and was put on an accelerated timeline and completed last December.[8] The non-standalone version allows carriers to continue to leverage their investments in 4G LTE networks while 5G chipsets are designed and integrated into handsets and equipment specific to 5G is deployed. The standalone version is targeted to be released later this year.

mmWave

The use of extremely high-frequency spectrum is one of the most prominently discussed components of a future 5G system. For discussion purposes, mobile spectrum can be broken down into three different ranges: low-, mid-, and high-band spectrum. Low-band spectrum is below 1 GHz. Mid-band spans from 1 GHz to 6 GHz. The high-band spectrum envisioned for use as part of 5G systems is above 24 GHz.

These are often called the millimeter wave bands (or mmWave), as their wavelengths can be measured in millimeters. These bands were long thought useless for mobile applications, as their propagation is severely limited. Signals in this frequency range are easily blocked by clutter on the ground—like buildings or trees. Rain can significantly impede these transmissions, and electromagnetic energy is even absorbed by oxygen at some portions of high-band spectrum.

The hope is that recent advancements in advanced antenna technologies can overcome these challenges and make these bands more practical for mobile operations than previously thought. NYU Wireless at New York University has been a research leader in exploring the feasibility of using this spectrum for mobile broadband.

Advanced Antenna Technology

High-band spectrum really shines when combined with advanced antenna technologies. Antenna size is inversely proportional to the spectrum frequency the antenna is built for. By turning to the millimeter wave bands, engineers can shrink antennas tremendously compared to what are used for wide-area networks today. In turn, far more of these small antennas can be fit into devices and equipment.

Using multiple antennas to transmit a single stream of information is a technique known as Multiple Input Multiple Output (MIMO). A particular flow of traffic can be broken down into pieces and intelligently transmitted through multiple antennas, with the effect of dramatically increasing throughput and reliability. MIMO can be used with other spectrum bands, but the small antenna size enabled by high-frequencies allows for large arrays of antennas to be used—known as massive MIMO.

Small Cell Architecture

Historically, spectrum reuse has been far and away the source of most gains in increasing the overall use of wireless systems. Techniques like making smaller cell sizes or splitting cells into different sectors allow for greatly increased capacity, but this solution is limited as well. As cells get smaller, costs skyrocket. The expenses of additional equipment, backhaul connections, rights-of-way negotiations, and the engineering to avoid self-interference quickly swamp the benefits and cannot easily be borne by additions to consumers' monthly bills alone. This will

continue to be an important consideration as we move closer to 5G—what the technology can achieve and what is economically feasible to actually deploy may not necessarily coincide.

Network Slicing, Automation, and Programmability

Access network operators are quickly adopting technologies to shift aspects of networking traditionally done by hardware to software environments. Specifically, the last few years have seen a dramatic rise in the use of software-defined networking (SDN) techniques. This is a technology well-proven in data centers; it essentially creates another layer of abstraction that separates the control over where network traffic is sent from underlying systems. This new software-centric control over networks enables network slicing, which will give control over logically separate data flows and allow the network to tailor specific technical requirements for different use cases. Network slicing will give better performance, supplying resources on demand and enable new business models beyond the classic mobile carrier.

These changes to how networking is done may seem obscure and technical, but they are incredibly important to how networks will transition to 5G. These technologies allow for a far more dynamic network that can adapt to the needs of specific applications on a granular basis.

The long-term goal is a combination of 5G connectivity and artificial intelligence, not just within the orchestration and operation of networks, but to enable the coordination of decision-making at the application layer. As researchers with Huawei have put it, "One of the most fundamental features among the revolutionary techniques in the 5G era, i.e., there emerges initial intelligence in nearly every important aspect of cellular networks, including radio resource management, mobility management, service provisioning management, and so on."[9] The integration of advanced machine learning into next generation networks is an area of intense research; for example, Huawei has supported research in artificial intelligence, internally as well as in the United States, including a strategic partnership into basic AI with UC Berkeley.[10]

Summary: Phase 1 vs. Phase 2 in 5G

There will be two phases of deployment of 5G networks. This divergence between the two phases is the clearest in the standardization process, where 3GPP is developing a "standalone" and "non-standalone" version of 5G New Radio. The body accelerated the non-standalone version last December, allowing for chipset development and earlier commercial launch plans.[11]

Rollout of 5G is likely to be an evolutionary process in the United States, with carriers first looking at incorporating aspects of 5G through the non-standalone version of NR standard, relying on existing LTE networks, and gradually deploying 5G hotspots, wireless point-to-point connections to the home, with true mobile coverage with pure 5G technology coming later.

U.S. operators have set an aggressive timetable to deploy early versions of the Phase 1 standard, looking at commercial launches this year. Chinese operators, on the other hand, appear content to wait for a uniform global standalone version of 5G, with commercial launches targeting 2020.[12] In other words, U.S. operators will explore a more experimental, evolutionary path, leveraging our existing LTE networks and transitioning to 5G systems where it makes the most economical sense. They will use the non-standalone standard for years until making a gradual shift to pure 5G technology.

China Mobile is eyeing an aggressive push of the standalone specification.[13] This will prove more expensive for the state-run carrier at first, but will gain early economies of scale in the particular technology and vendors they rely on. Guang Yang, a senior analyst at Strategy Analytics, believes China Mobile is likely trying to leverage its deep financial strength for competitive advantage.[14] Standalone 5G will demand higher up-front capital expenditure, making it difficult for competitors to follow in the early rollout of the standalone version. Yang also notes that China Mobile is risking that interoperability and interworking for the new standard may not be complete by its planned commercial launch in 2020 and "may delay the deployment."[15]

DYNAMICS OF INTERNATIONAL COMPETITION IN NEXT GENERATION NETWORKS

5G is an incredibly complex technology, with a wide variety of arenas for companies and countries to exert influence over the shape of the next generation networks. A recent report from investment analysts at Jeffries examined the geopolitics of 5G and IoT across intellectual property rights ownership, influence within standard-setting bodies like 3GPP, and spectrum coordination efforts both within countries and at the international level at the ITU.[16] The analysts explained their view that "China will roll out 5G fast and big" once international standards (phase 2) are finalized.[17]

It can be difficult to ascertain the level of influence intellectual property rights of any one company has over these technology platforms, but one 2017 estimate by LexInnova put total China ownership at about 10 percent of "5G-essential" intellectual property rights, most of which are owned by Huawei.[18] The leader in overall 5G patents is Qualcomm, with about 15 percent of the total.[19] One important breakthrough for Huawei was the acceptance by 3GPP of its proposed coding methodology for the control channel in the non-standalone "phase 1" 5G version.[20]

As a part of this growing contribution of R&D, China, mostly through Huawei and state-owned China Mobile, but also ZTE and others, is dramatically increasing its participation in standards-setting bodies like 3GPP and the ITU. According to Jeffries, The number of Chinese representatives in 3GPP technical working groups has risen from 8 in 2013 to 10 in the most recent election (out of a total of 57 positions). FCC Commissioner Michael O'Rielly has criticized ITU processes, claiming it "needs an overhaul… [to prevent] authoritarian governments [from] push[ing] their myopic agendas."[21]

Ultimately what makes the biggest difference is how well these technologies are integrated with the broader IT ecosystem and enable innovation and productivity gains throughout a nation's economy.

CHINA IS NOT YET LEADING IN 5G DEPLOYMENT, BUT HAS LONG-TERM ADVANTAGES AND IS EXECUTING A COHERENT STRATEGY

It is likely the U.S. will win the race to be first to deploy 5G. However, China has a long-term strategy to deploy phase 2 standalone 5G at scale.

The Context of China's Innovation Mercantilism

We at ITIF have argued that effectively managing the U.S.-China trade and economic relationship is one of the most significant international challenges facing the United States.[22] The ITIF report, "Stopping China's Mercantilism: A Doctrine of Constructive, Alliance-Backed Confrontation," explored the challenge:

> "There is a growing understanding that China is an outlier when it comes to global norms and rules governing trade, investment, and economic policy, and that the unremitting and even accelerating 'innovation mercantilist' behavior on the part of the Chinese government represents a threat not only to the U.S. economy, particularly its advanced industries, but indeed to the entire global economic and trade system."[23]

However, we also argued that a "new approach to U.S.-China economic and trade policy from the U.S. government will need to be pursued with great care and sophistication," that the goal must be a careful return to rules-based international trade order, and not about punishing China or holding back its economy or its contributions.[24]

China is Working to Gain Influence Over Next Generation Connectivity

The Chinese government is actively supporting both the development of 5G standards as well as the deployment of 5G networks. Beyond government support for research and development, policies find explicit articulation in the "Made in China 2025" plan and the 13th Five Year Plan, which aims for a commercial launch of 5G services by 2020.[25]

China is working collaboratively with a number of industry associations, governments, and research universities to develop a global standard and set of technologies that can be quickly scaled.[26] Chinese companies, such as Huawei, invest heavily in R&D and have continually increased their patent portfolio.

As discussed above, China has increased its presence in both the 3GPP and ITU, and Huawei has already made key contributions to the 5G NR specification. All of these mechanisms lead to greater influence over the direction of ICT development, lowering costs for their technology and increasing their bargaining power in the ICT space. 5G is also anticipated to be a key platform for economic growth—successful deployment of next generation wireless is a matter of national competitiveness.

China has Advantages in Allocating Spectrum and Overcoming Deployment Challenges

The general consensus is that the United States and China are leading in 5G, closely followed by Japan and South Korea. According to Nokia CEO Rajeev Suri, "It's a neck-and-neck race between the U.S. and China to see who will be first to deploy."[27] Europe is generally seen as lagging in 5G deployment, as the market is highly fragmented and the average revenue per user is lower than other countries, making the investment needed to deploy more difficult to justify.

China has the advantage of a large population and relatively concentrated market at the operator level (China Mobile has roughly 70 percent market share). The government is also able to exert much stronger control over existing spectrum users, allowing for more efficient use, potentially driving global economies of scale. Furthermore, China does not share our system of

federalized government, which is important for the physical deployment of wireless infrastructure. Here, local governments often have control over the terms on which wireless companies gain access to poles or rights-of-way, and can hold out for fees in a way that may contravene national interests.[28]

THE UNITED STATES SHOULD NOT DEPLOY ITS OWN NATIONALIZED 5G NETWORK

Earlier this year, *Axios* reported that the Trump administration was considering "nationalizing" a 5G network.[29] The reporting included a memo and a slide deck presentation arguing that a centralized and rapidly deployed 5G network, with a focus on incorporating robust security features and sourced through a trusted supply chain is necessary because "China has achieved a dominant position in the manufacture and operation of network infrastructure," and "China is the dominant malicious actor in the Information Domain."[30]

The memo considered 5G only in narrow terms of national security, and did not appreciate the complexity of dynamic global supply chains adapting to new market challenges and cutting-edge research. It appears the memo and presentation were preliminary efforts of a single employee within the National Security Council, and thankfully do not represent the official views of the administration. The memo's author, an Air Force Brigadier General, left his detail to the White House's National Security Council shortly after its publication.[31]

This proposal would represent an especially bad direction to follow, as it would undermine one of the key advantages of the U.S. model: private sector led innovation and experimentation. As economists and telecommunications experts Thomas Hazlett and Scott Wallsten recently explained, "The idea floated was considerably worse than commonly understood."[32] They explained:

> The means [the memo proposed] were dubious and dangerous. A contemplated pivot away from market competition — the product of a longstanding consensus that dispatched the old, staid Ma Bell monopoly with an array of robust networks, devices and mobile app ecosystems — reached back into the dustbin of history, reprising methods that long stymied progress.[33]

Leading in next generation networks is not a question of shock and awe, 3-year timeframe buildout. It will be an iterative process, especially in the transition from Phase 1 to Phase 2. The U.S. government—at the federal, state, and local level—can do a lot to make spectrum available and streamline the process for accessing rights-of-way, poles, and streetlights. It can do more to support U.S. industry through trade and protection of intellectual property rights. But to actually take over the build-out and development of the network itself is a radical and unhelpful suggestion.

THE UNITED STATES SHOULD NOT PRESUMPTIVELY BLOCK PARTICULAR EQUIPMENT MANUFACTURERS

The most acute area of contention between the United States and China when it comes to next generation connectivity is Huawei and ZTE's access to the U.S. market. This dispute can be resolved through the combination of an open and ongoing review of these companies' equipment and practices and targeted economic incentives without devolving into a trade war or

encouraging further protectionism. Any action should be a part of a broader policy of insisting on reciprocity from China so that the market access conditions facing U.S. firms in China are the same as the ones facing Chinese firms in the United States.

The United States, however, should not be Pollyannaish. Over the years, Verizon's Data Breach Investigations Reports have continually highlighted data breach and cybersecurity violations originating from China. Its government strongly supports an increased international role for its information technology sector, sometimes through means that do not comport with its commitments to enterprise-led, market-driven, and rules-based trade.

Yet virtually every telecommunications network worldwide incorporates foreign technology. These are complicated supply chains with each component often sourcing technology from a variety of different firms—simple answers won't suffice. A nuanced approach should be integrated with a broader strategy on international trade and intellectual property.

Background of Huawei and ZTE Attempts to Enter the U.S. Market

Huawei and ZTE, two telecommunications equipment manufacturers, have long attempted to enter the U.S. market, primarily for network equipment, but also in handsets. These efforts have been rebuffed by the U.S. government through a variety of mechanisms.

In 2012 the House Intelligence Committee released a 60-page report titled "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE."[34] The report highlighted ways in which the companies did not fully cooperate with the body's investigation, and recommended U.S. network providers seek other vendors for equipment and services. The Intelligence Committee noted that "Based on available classified and unclassified information, Huawei and ZTE cannot be trusted to be free of foreign state influence and thus pose a security threat to the United States."[35] The U.S. national-security clearance of SoftBank's acquisition of Sprint in 2013 included restrictions on use of Chinese equipment.[36]

In recent testimony to the Senate Intelligence Committee, FBI Director Chris Wray said the intelligence body is "concerned about the risks of allowing any company or entity that is beholden to foreign governments that don't share our values to gain positions of power inside our telecommunications networks."

Bicameral legislation recently introduced by Senators Marco Rubio (R-FL) and Tom Cotton (R-AR) in the Senate and Representative Michael Conaway (R-TX) in the House that would explicitly prohibit the U.S. government from purchasing or using telecommunications equipment or services from Huawei and ZTE.[37]

Huawei's response has been pointed, with its current CEO Richard Yu calling recent developments "ridiculous" at trade show Mobile World Congress earlier this month.[38] He went on to point to Huawei's competitors, saying "Our competitors are using some political way … to try to kick us out from the U.S. market but we have no issue at all. We are transparent …. But they cannot compete with us on product, on technology, on innovation, so they compete with us [using] politics."[39]

As further discussed in our policy recommendations below, we do not think a heavy-handed approach strikes the right balance for navigating the difficult path of achieving an effective return to rules-based trade and ongoing development of a mutually beneficial innovation ecosystem going forward. We should take care that any actions are aimed to dissuade China from doubling down on the "secure and controllable" route, and avoid their tightening and centralizing state control over information flows and technology equipment.

Here the institutional arrangements in the United Kingdom point to one possible way forward. In 2004, Huawei made a successful bid for a major network upgrade for the incumbent wireline operator British Telecom. In 2010 Huawei opened the "Huawei Cyber Security Evaluation Center" (HCSEC). An oversight board was established in 2014 to audit the group's practices.[40] The evaluation center and the oversight board have found "no high or medium priority findings."[41]

The United States should create a strengthened version of this body to oversee equipment entering the U.S. market. The HCSEC is staffed by Huawei employees (although the oversight board is a third-party)—a similar body made up of technical experts from different organizations could perform a similar function in the United States.

POLICY RECOMMENDATIONS

Below we outline a number of policy recommendations to ensure continued U.S. leadership in the deployment and use of next generation communications networks, and an option to navigate potential security threats in the global equipment supply chain. We must continue to rely on our private-sector driven, light-touch regulation model, while supporting basic R&D and clearing the path to 5G investment.

on Importing Chinese Telecommunications Equipment

It is important to look at the net risk of a system and weigh the costs of any approach. By excluding some equipment from the U.S. market you eliminate one attack vector, but it comes at a cost while not eliminating all risks. U.S. policy should recognize there is a wide array of potential security threats throughout the telecommunications supply chain and up the stack. The vast majority of malware actions are through email attachments, and are not sophisticated hardware attacks.

It is difficult but possible to evaluate individual technologies on an ongoing basis to ensure security. Any project or body to examine equipment destined for U.S. markets should not be comprised wholly of employees of the company in question, such as is the case in the U.K. HCSEC.

There should be a robust incentive structure in place to ensure strong repercussions if, for example, an insecure backdoor was discovered in a company's equipment. One potential mechanism is through an international agreement—several large markets should agree not to do business with a company if a deliberate insecurity is discovered.

There can also be a distinction for equipment that is destined for national security or public safety networks, rather than everyday consumers. Also, there should be a requirement that all components of equipment and handsets that are evaluated by this body be explainable.

to Ensure Continued Development of Next-Generation Connectivity

The U.S. government should support basic R&D to support the continued evolution of next generation networks. Basic R&D in particular, can be difficult for companies to monetize, and the government can play an important role here.

Consider, Huawei, for example, is intensely focused on R&D, having consistently invested over 10 percent of its revenue in R&D every year.[42] In 2016, the company had about 80,000 employees—about 45 percent of its workforce—engaged in R&D.[43] From 2015 to 2016, Huawei increased its patent holding by about 50 percent, rising to number 28th in the world.[44]

to Supply Additional Spectrum for 5G

5G will make use of a wide variety of spectrum. While there is currently a great deal of excitement around the ultra-high millimeter wave bands, next generation wireless networks will leverage lower frequencies as well. The 5G NR specification as well as advances in network core are "spectrum agnostic" technologies. The FCC, in coordination with Congress and the National Telecommunications and Information Administration, should work to ensure spectrum continues to be evaluated and potentially put to higher and better use.

More specifically, the FCC should be encouraged to move with haste to auction the 3.7 to 4.2 GHz band, as well as mmWave spectrum above 24 GHz. Thankfully the secondary market has already seen some spectrum in the 28 and 39 GHz bands being repurposed for what will likely be 5G, but additional auctions are needed. Thankfully the FCC is making strong progress on all of these fronts.[45] Before those auctions can take place, Congressional action is needed to resolve a conflict between the FCC's requirement that auction revenues be placed in an interest bearing account and recent changes to banking laws.[46]

It is also important that the State Department have a strong presence at the International Telecommunications Union (ITU) to advocate on behalf of U.S. interests at the World Radio Conference in 2019. The international spectrum coordination at the ITU is key for gaining economies of scale in some types of equipment, and is also necessary for satellite uses that can supplement 5G.

to Protect Intellectual Property

China is the world's leading source of intellectual property theft.[47] The "2016 China Business Climate Survey Report" the American Chamber of Commerce in the People's Republic of China lists IP infringement as a concern regarding doing business in China, with 23% of respondents listing it as a top challenge.[48]

The U.S. should also work to ensure reciprocity in technology and intellectual property licensing. The United States needs a new regime to contest China's strict technology-licensing laws.

The United States should also bring more trade cases against China at the WTO, in collaboration with international partners, where possible. One potential WTO case could concern China's continuing coerced technology and intellectual property transfer requirements. The prospects

for such a case would be greatly improved if U.S. law required notification to the U.S. government on a confidential basis of technology licenses to China and of transactions in China in which the Chinese government or Chinese government-affiliated entities are involved. When China joined the WTO in 2001, it agreed that foreign firms would not be pressured by government entities to transfer technology to a Chinese partner as part of the cost of doing business in China. But as ITIF documents in reports such as "Stopping China's Mercantilism: A Doctrine of Constructive, Alliance-Backed Confrontation" China continues to compel the disclosure of technology and IP as a condition of market access (or eligibility for benefits such as subsidies for the purchase of electric vehicles). The United States and like-minded trade partners need to more aggressively contest these policies.

to Spur 5G and IoT Deployment in the United States

Many of the policy challenges facing 5G and IoT deployment are at the local level. Experts Blair Levin and Larry Downes explored these dynamics in a recent essay, advocating for the "preempt[ion of] unnecessary intergovernmental conflict" in addition to four other policy recommendations for local communities: streamlining process and permitting to access poles and rights-of-way, partnering with operators to test early deployments, targeting applications for smart cities, and establishing pro-investment pricing policies.[49] These are exactly the types of polices that will assist in early deployment of 5G networks and support innovation of new types of applications they enable.

Thankfully, the FCC is taking steps to help streamline the deployment of wireless networks. It appears the commission is rolling out several changes to federal policy, and even considering further preemption of state and local siting rules to help streamline the process and remove regulations designed for a different technology. For example, the commission recently announced changes to how the small cells anticipated for 5G will be considered under the National Historic Preservation Act and the National Environmental Policy Act—changes ITIF supports.[50] The shift from large 200 foot-tall macro cells to much smaller, lower-power, but more numerous small cells requires a retooling of regulations and permitting processes at the local level as well. As the Center for Data Innovation has argued, United States should also have a comprehensive strategy for the Internet of Things.[51]

to Ensure Robust Platforms and Use of Next Generation Networks

The goal should be effective use of these 5G platforms. Commonsense policies to encourage further use of 5G, such as allowing continued innovation at the application layer and avoiding taxes on Internet uses.

Effective responses to constantly evolving cybersecurity risk require collaborative efforts between all of industry and the public sector. One opportunity may lie in the recently announced "Council to Secure the Digital Economy." Organized by leading companies in the tech and telecom industries, and coordinated through associations USTelecom and the Information Technology Industry Council, the group hopes to more effectively coordinate players up and down the Internet stack with government agencies.[52]

Thank you again for this opportunity to appear before you today.

REFERENCES

[1] Founded in 2006, ITIF is an independent 501(c)(3) nonprofit, nonpartisan research and educational institute—a think tank—whose mission is to formulate, evaluate, and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress. Ranked by the University of Pennsylvania as the world's leading science and technology think tank, ITIF's goal is to provide policymakers around the world with high-quality information, analysis, and recommendations they can trust. To that end, ITIF adheres to a high standard of research integrity with an internal code of ethics grounded in the core values of analytical rigor, policy pragmatism, and independence from external direction or bias.

[2] For broader discussion of 5G, *see* Doug Brake, "5G and Next Generation Wireless: Implications for Policy and Competition" *ITIF* (June 2016), https://itif.org/publications/2016/06/30/5g-and-next-generation-wireless-implications-policy-and-competition.

[3] *See* e.g., Ina Fried, "Everyone says they'll be first with 5G," *Axios* (Feb 22, 2018), https://www.axios.com/everyone-says-they-are-first-with-5g-cadcce03-7d59-4660-9bb1-b99368187fe2.html.

[4] Sanjay Dhar, et al., "Smart Cities: How 5G Can Help Municipalities Become Vibrant Smart Cities," (Jan. 2017), *Accenture Strategy,* https://newsroom.accenture.com/content/1101/files/Accenture_5G-Municipalities-Become-Smart-Cities.pdf.

[5] Ibid.

[6] James Manyika et al., "Unlocking the Potential of the Internet of Things," McKinsey Global Institute, June 2015, http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world.

[7] Andrew Brown, "IoT Cellular Connections by Industry Vertical, Bandwidth and Region," *Strategy Analytics* (Mar. 2017), https://www.strategyanalytics.com/access-services/enterprise/iot/market-data/report-detail/iot-cellular-connections-by-industry-vertical-bandwidth-and-region#.Wpg3H-dOmHt.

[8] *See* Andrei Frumusanu, "3GPP Completes First 5G NR Specification for Release 15" *AnandTech,* (Dec. 2017), https://www.anandtech.com/show/12182/3gpp-completes-first-5g-nr-specification-for-release-15.

[9] Rongpeng Li, et al., Intelligent 5G: When Cellular Networks Meet Artificial Intelligence" 24 *IEEE Wireless Communications* 5, (March 2017), http://ieeexplore.ieee.org/document/7886994/?reload=true.

[10] *See* Huawei, "Huawei and UC Berkeley Announce Strategic Partnership into Basic AI Research," *Press Releases* (Oct. 2016), http://www.huawei.com/en/press-events/news/2016/10/Huawei-UC-Berkeley-Strategic-Partnership-Research-AI.

[11] *See* Kelly Hill, "It's official: 5G New Raio standard is ratified by 3GPP" *RCR Wireless* (Dec 2017), https://www.rcrwireless.com/20171220/5g/its-official-5g-new-radio-standard-is-ratified-by-3gpp-tag6.

[12] *See*, GSMA and CAICT, "5G in China," *GSMA Intelligence,* (2017) https://www.gsmaintelligence.com/research/?file=67a750f6114580b86045a6a0f9587ea0&download.

[13] *See*, e.g., Robert Clark, "China Mobile Confirms Aggressive 5G Standalone Plan," *LightReading* (March, 2018), http://www.lightreading.com/mobile/5g/china-mobile-confirms-aggressive-5g-standalone-plan/d/d-id/741013?itc=lrnewsletter_lrweekly.

[14] Ibid.

[15] Ibid.

[16] Edison Lee & Timothy Chau, "The Geopolitics of 5G and IoT," *Jefferies Franchise Note*, (Sept 2017), http://www.jefferies.com/CMSFiles/Jefferies.com/files/Insights/TelecomServ.pdf.

[17] Ibid.

[18] LexInnova, "5G Network Technology: Patent Landscape Analysis" (2017) http://www.lex-innova.com/resources-reports/?id=67f.

[19] Ibid.

[20] Ibid.
[21] Remarks of FCC Commissioner Michael O'Rielly Before the Free State Foundation, Washington, DC "Next Generation 5G Wireless Networks: Seizing the Opportunities and Overcoming the Obstacles" (July, 2017) https://apps.fcc.gov/edocs_public/attachmatch/DOC-345941A1.pdf.
[22] Robert D. Atkinson, et al., "Stopping China's Mercantilism: A Doctrine of Constructive, Alliance-Backed Confrontation" *ITIF* (March, 2017), https://itif.org/publications/2017/03/16/stopping-chinas-mercantilism-doctrine-constructive-alliance-backed.
[23] Ibid.
[24] Ibid.
[25] *See*, GSMA and CAICT, "5G in China," *GSMA Intelligence,* (2017) https://www.gsmaintelligence.com/research/?file=67a750f6114580b86045a6a0f9587ea0&download.
[26] Ibid.
[27] Monica Alleven, "Nokia CEO: U.S., China lead 5G race, but U.S. needs to make mid-band spectrum available," *FierceWireless* (Feb. 26, 2018), https://www.fiercewireless.com/wireless/nokia-ceo-u-s-china-lead-5g-race-but-u-s-needs-to-make-mid-band-spectrum-available.
[28] *See* Doug Brake, "Standing in the Way of Next-Gen Wireless: What Gives, Mayor Liccardo?" *Innovation Files* (Nov. 2017), https://itif.org/publications/2017/11/06/standing-way-next-gen-wireless-what-gives-mayor-liccardo.
[29] Jonathan Swan et al., "Scoop: Trump team considers nationalizing 5G network," *Axios* (Jan. 28, 2018), https://www.axios.com/trump-team-debates-nationalizing-5g-network-f1e92a49-60f2-4e3e-acd4-f3eb03d910ff.html.
[30] Ibid.
[31] Josh Rogin, "National Security Council official behind 5G memo leaves White House," *The Washington Post* (Feb. 2018), https://www.washingtonpost.com/news/josh-rogin/wp/2018/02/02/national-security-council-official-behind-5g-memo-leaves-white-house/.
[32] Thomas W. Hazlett and Scott Wallsten, "Hey, we might need that wall … to stop Mexico's state-run 5G network," *The Hill* (Feb. 22, 2018), http://thehill.com/opinion/technology/374742-hey-we-might-need-that-wall-to-stop-mexicos-state-run-5g-network.
[33] Ibid. Some trade press reporters were more colorful, with one describing the memo as originating from the "intern's-brain-fart department." Karl Bode, "Leaked Trump Plan To 'Nationalize' Nation's 5G Networks A Bizarre, Unrealistic Pipe Dream" *TechDirt* (Jan 29, 2018), https://www.techdirt.com/articles/20180129/08390639107/leaked-trump-plan-to-nationalize-nations-5g-networks-bizarre-unrealistic-pipe-dream.shtml.
[34] Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger, "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," *U.S. House of Representatives* (112th Congress, Oct. 2012), https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf.
[35] *Id* .at 45.
[36] *See,* e.g., Todd Shields and Chris Strohm, "Huawei Loser in SoftBank-Sprint Deal Over Alleged Spying," *Bloomberg Technology* (May, 2013), https://www.bloomberg.com/news/articles/2013-05-29/huawei-loser-in-softbank-sprint-deal-over-alleged-spying.
[37] *See*, "S.2391 - Defending U.S. Government Communications Act" *Congress.gov*, https://www.congress.gov/bill/115th-congress/senate-bill/2391; "H.R.4747 - Defending U.S. Government Communications Act" *Congress.gov,* https://www.congress.gov/bill/115th-congress/house-bill/4747.
[38] Arjun Kharpal, "Huawei's rivals 'worry we are too strong' and may use politics to kick the tech giant out of the US, top exec says," *CNBC*, (Feb. 26, 2018), https://www.cnbc.com/2018/02/25/huawei-us-issues-rivals-using-politics-to-kick-it-out-of-us-richard-yu.html.
[39] Ibid.
[40] *See* "Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board, Annual Report" 2017 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/626110/20170413_HCSEC_Oversight_Board_Report_2017_-_FINAL.pdf.

[41] Ibid.
[42] *See* "Research and Development" *Huawei*, http://www.huawei.com/en/about-huawei/corporate-information/research-development (visited Feb. 25, 2018).
[43] Ibid.
[44] IPO, Top 300 Organizations Granted U.S. Patents in 2016 (May 2017), http://www.ipo.org/wp-content/uploads/2017/05/2016_Top-300-Patent-Owners.pdf.
[45] *See* Remarks of FCC Chairman Ajit Pai at the Mobile World Congress, Barcelona, Spain (Feb. 26, 2018), https://transition.fcc.gov/Daily_Releases/Daily_Business/2018/db0226/DOC-349432A1.pdf.
[46] Ibid.
[47] *See*, The Commission on the Theft of American Intellectual Property, "The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy" (2017), http://ipcommission.org/report/IP_Commission_Report_Update_2017.pdf.
[48] http://www.ipcommission.org/report/IP_Commission_Report_Update_2017.pdf page 21
[49] Blair Levin and Larry Downes, "How some cities are attracting 5G investments ahead of others," *Washington Post* (Feb 2018), https://www.washingtonpost.com/news/innovations/wp/2018/02/08/how-some-cities-are-attracting-5g-investments-ahead-of-others/.
[50] *See*, FCC, "In the Matter of Accelerating Wireless Broadband Deployment by Removing Barriers to Infrastructure Investment" *Second Report and Order* WT Docket No. 17-79 (Draft rel. March 1, 2018), https://apps.fcc.gov/edocs_public/attachmatch/DOC-349528A1.pdf.
[51] Joshua New & Daniel Castro, Why Countries Need National Strategies for the Internet of Things," *Center for Data Innovation* (Dec. 2015), http://www2.datainnovation.org/2015-national-iot-strategies.pdf.
[52] *See* Jonathan Spalter and Dean Garfield, "A Future Immune to Cyber Threats," *Morning Consult* (Feb. 26, 2018), https://morningconsult.com/opinions/a-future-immune-to-cyber-threats/.

PANEL I QUESTION AND ANSWER

HEARING CO-CHAIR WESSEL: Thank you both for your testimony.

I'll begin and also hope to focus our attention today on the U.S.-China aspects of this, whether we're talking about how it's deployed with more antenna, you know, all the various issues. That may be for a technology commission, which is not us. So we're looking at this really through the prism of what U.S.-China implications there are in terms of the economy, in terms of security interests, and what Congress should be looking at it through, again that window.

We had a meeting yesterday with some of our great public servants from NIST, and who do an exceptional job and I assume work with you, Mr. Brake, and probably with you, Mr. Benson. But in listening, it appeared to me that we have a somewhat neutral approach to technologies in terms of the provenance. That it's about setting the standards rather than worrying about the implications, if you will.

For me, as I look at China's activities in this area, you know, with their 13th Five Year Plan and all the associated documents you're well aware of, they view 5G, IoT, and other technologies as critical to their long-term economic development and inextricably intertwined with that is their national security.

What should we be doing, if anything, differently around standard settings? Mr. Brake, you said you were encouraged by Chinese participation in the ITU, and I believe they now chair--they're Secretary General there, et cetera. I think they learned from, whether it was--I'm forgetting the WiFi standard they promoted years ago, which didn't take off. We've had CDMA, all the various standards. They understand now that there has to be one standard, but they want to dominate it, in my view. They want to develop it. They want to dominate it, and they also want to be the one who provides all the equipment that supports it.

Is that in our interest? What economic repercussions does that have? Later we're going to deal with the security-related issues, but if you could talk a bit about economics and, again, through the prism of U.S.-China issues.

Mr. Brake, do you want to start?

MR. BRAKE: Sure. A lot to unpack there. So I mentioned that I was encouraged in some ways by China's participation, simply because it signals exactly that, that they are turning away from a more insular market to more global participation, recognizing that these are, you know, standards that have global implications in participating in international supply chains.

You're absolutely right that this is also a component of their broader efforts to be a leader, not just in making iPhones but in competing with iPhones; right. They are aggressively engaging in research and development throughout the entire IT stack chipsets--

HEARING CO-CHAIR WESSEL: And acquisitions.

MR. BRAKE: What's that?

HEARING CO-CHAIR WESSEL: And acquisitions.

MR. BRAKE: Yes, yes, exactly. Yeah.

And they are very aggressive in their presence in 3GPP and ITU, these sorts of international standard-setting bodies.

In many ways the U.S. could work to incentivize companies to take a more aggressive approach in these bodies. In many ways, standard setting institutions to the extent that companies do not capture standard essential patents, their participation in these standard-setting

bodies is something like a public good; right. They invest time, money, resources to create standards that flow to the entire economy that aren't fully captured by any one company.

And so I think that further support from the government in the form of tax incentives or something like that to allow for companies to further engage in standard-setting organizations like 3GPP would be wise. At the same time, we don't, we don't want to follow the worst aspects of China's innovation mercantilism. We want to avoid protectionism, support our industry where it makes sense, clear the barriers to investment in local infrastructure and allow economies of scale.

HEARING CO-CHAIR WESSEL: And appreciate. Let me interject here. So China, again, it appears to me, at these standard-setting bodies are seeking to advance their own interests. Clearly, there is a public good from what we're talking about as there is in medicine and many others and accept that. But their role seems to be to advance domestic interests. Do you agree with that?

MR. BRAKE: Yes, absolutely. Yeah.

HEARING CO-CHAIR WESSEL: Are we doing enough? And we've had ITIF and some of your associates, your leadership here, and we appreciate all that you do. Is the U.S. doing enough or are we taking a neutral stance in all these bodies as to sort of technology neutral: we want the best there can be but not worrying about provenance and economic benefits?

MR. BRAKE: I do think that we could take a more proactive stance towards these standard-setting organizations. But I think that our model of experimental incremental approach to developing the technology, finding where it makes the most economic sense, is the right approach, and so we should continue to rely on our competition market-based model and allow our U.S. operators to find where 5G makes the most sense.

HEARING CO-CHAIR WESSEL: Okay. Mr. Benson.

MR. BENSON: I couldn't comment on what I think a fix on IoT Systems will be with 5G. I'm not a 5G expert. From what I understand, the benefits of 5G, on the IoT side, it will bring more of everything. It will bring more potential benefit, economic benefit, opportunity for social benefit, but also more risks.

I have some concern that if it gets deployed too fast and haphazardly that some of these other issues that I brought up in my opening statement, we won't catch up with that, and that can actually leave us more open.

HEARING CO-CHAIR WESSEL: Okay. Thank you.

Commissioner Tobin.

COMMISSIONER TOBIN: Great. Thank you to both of you for being here and informing us. Again, thank you for joining us today, and we're spending some time briefing ourselves on the Internet of Things, and then as our co-chair mentioned, we're trying to understand the threat.

So I want to have a question of you first, Mr. Benson. You spoke--one of your recommendations related to greater data ethnography, and you would expect that to occur across cities, I guess, or the technologies doing that, and is this something that you see happening now or should be, and also is China doing this?

MR. BENSON: I'd like to see more of it. And two years ago, I couldn't have told you what a data ethnographer was. But the idea that we have so much data, and these IoT systems are generating so much, so much data, and it's being used to interact with our populace, that's a

new thing, and we really don't know how to consume that yet or how to deal with that yet, and there's lots of questions to be asked.

We need to understand how that data is being used to figure out is this IoT system good for our city or our institution or whatever. So I would like to see a lot more, a lot more work in that space. We can learn how to mediate data. And if we don't, we're not going to have a lot of utility out of it, I think.

One other place where--I'm going to hold off on that comment for a second. On China, I don't have a sense for what their investment is in this space yet.

COMMISSIONER TOBIN: And when you were giving your testimony, you spoke about how there's just such variance out there. So at the University of Washington, are you or any organization, are people putting together maps and trying to articulate what's going into the full organization? How do you--you have that work group. What is it doing as it looks at risks?

MR. BENSON: So we're trying to look at risks across the organization. A lot of it is developing awareness. A lot of it is getting some language out there to say that this technology is showing up in our laps now. For example, it is how these technologies come into a campus or a city.

And traditionally it would come in through a central IT organization, and it gets vetted there and gets deployed however. But now these systems are coming in from wherever. For example, a facilities management organization, that technology, there could be a substantial technology purchases coming in through there, the central IT people never even see it, and now--so the facilities people now have a complex technology system they really haven't dealt with before. And in a similar way, central IT groups could start to see some facilities kind of work, and they don't know what to do with that either.

And then a comment on kind of cultures between the two. So you like in a facilities group that's going to operate these technology systems, that's going to manage this across a campus or a city, the history there, they've come up through the trades. They're carpenters, electricians, plumbers and related things. So that's what their background is.

IT has a very different background, and it's a lot shorter, right, two-and-a-half decades, maybe that. We start to bring those two together, and those are two different worlds. On the facilities side, these people, these professionals tend to think in terms of decades, and the reason is they put up a building and manage a building for a decade. That's what they want to see, and that's what the mind-set is.

On the IT side, people think in terms of minutes, days and weeks and end up at very different time frames. Also, for example, a facilities management side, the mind-set understandably is if that building over there is getting heat and it's getting electricity, don't touch it. Just let it keep getting heat and electricity. Don't touch it.

On the IT side, you're constantly making changes. You're constantly patching, trying to deal with the next threat that's coming down or the threat that came out yesterday. So that culturally, there's two very different things. And so when you have this, these kinds of new technologies integrating into groups that have not worked with these technologies before, it's a different kind of animal.

So that's one of the recommendations I made about these skill sets because this operational technology skill set, the professionals that go in and go configure an endpoint, there's not many of them, and it's a different kind of thing than being a regular electrician or a typical IT person.

COMMISSIONER TOBIN: One other thing. Within the equipment that you are seeing deployed across that range, are you aware of the supply chain elements in that?

MR. BENSON: No. I mean I know there's lots of stuff in there that I don't know what it is. But my background as an electrical engineer, I know inside a device there is multiple different components, but I don't know--I don't know where those are coming from.

One example, what opened my eye to that, there's some services that are out there, and they're public and they're free and they're readily available. One is called Shodan where you can scan all the public facing addresses and see what's on those. What you started to see--what they look for, they look for critical infrastructure systems, and they look for IoT kinds of systems, and what you start to see, you start to see responses from software that were made by somebody else. So a device pops up, but inside this, there's some software that's made--

COMMISSIONER TOBIN: That's why I asked.

MR. BENSON: --over here.

COMMISSIONER TOBIN: I see my time is up. Thank you very much.

Mr. Brake, I have a question on a second round.

HEARING CO-CHAIR WESSEL: Chairwoman Cleveland.

CHAIRMAN CLEVELAND: Well, I'm an antique, and I'm still struggling with the concept of the Internet of Things, but there are a couple things that you raised, Mr. Brake, that I was curious about.

You said in your testimony that the Chinese have captured ten percent of essential patents. Is that right?

MR. BRAKE: Right. So that is one estimate that I've seen, and all those are very difficult to make, you know. Oftentimes what is determined to be a standard essential patent is determined years later in court after a big battle between telecommunications companies. But that's one estimate that I've seen.

Compare that to, for example, Qualcomm, generally considered one of the leaders in 5G technology, they have about 15 percent. So the Chinese around ten.

CHAIRMAN CLEVELAND: And these patents are registered in China because the experience we've had previously with emerging technology is they register patents for products that they have stolen. So I'm curious about the, in terms of protecting our interests here, what the nature of the patenting process is in this space.

MR. BRAKE: So I would have to--I apologize. I'd have to go back and check that exact study, what they looked at. I believe that they would be U.S. registered patents. Again, this is a signal of China moving away from a much more insular protectionist where they're trying to actually dominate the global innovation system. So--

CHAIRMAN CLEVELAND: If you would answer that for the record because that would be an interesting data point for me that it's been this shift from simply stealing and registering in China versus now moving into the global space.

Mr. Benson, working in a university environment, I really appreciate the facilities versus the IT construct that you've come up with, and I don't want anybody touching the heat or electricity to my building right now. We finally got it back on. No doubt the heat will run right through the summer, but--

[Laughter.]

CHAIRMAN CLEVELAND: So I was curious, and you didn't mention this in detail about--it's on page 16, I think, of your submitted testimony, talking about this living room workshop and the origin of a great deal of--well, not a great deal. You didn't characterize that

way. Could you talk a little more about the innovation at this kind of level that I suspect will be very hard to control or manage?

I was fascinated by this because I think one of the myths is that China's innovative capacity or sort of imagineering is limited, but this looks like there's been a significant sea change.

MR. BENSON: Yeah, the ability to innovate these devices here or China, in a garage, in a living room, wherever, it's just--we've just never seen it before. I mean I gave a couple pictures in there. For example, there's a little computer, it's called a Raspberry Pi. It came out of the UK in the past decade or so. But it's about this big, smaller than a deck of cards, and it's a full functioning Linux computer, 35 bucks.

Arduino is another one. It's a little circuit board, and it's kind of the core of the Maker revolution. And it's about 30 bucks. And they have all kinds of smaller boards with smaller circuits. And they have robust, this whole do-it-yourself movement is huge. And there's great training. There's great user support groups. So the innovation is going to come from all over.

How that gets industrialized, that's another question. In that particular article, I was interested in that as well because there were active activities to take all that, you know, thinking, and it could be, you know, 12-year-olds to 30-year-olds to whoever tinkering in their bedrooms. But that's where some of these ideas can come from, and that's a much bigger pool to choose from than what we've had before.

So how that gets industrialized and how that gets monetized, operationalized, that's an interesting space. In this article, to me, it changed that picture of, I have a picture like China being very regimented and maybe even stodgy or something.

CHAIRMAN CLEVELAND: Everybody in the same uniform. That's what struck me by--yeah.

MR. BENSON: But this was pretty hip. I mean--

CHAIRMAN CLEVELAND: Uh-huh. I think we're showing our age on that use of the word.

MR. BENSON: Yeah, I know.

[Laughter.]

CHAIRMAN CLEVELAND: So you anticipated my question, which is how is the Chinese government looking at these entrepreneurs and these innovators and how formal or systematic is the effort to kind of reach out, touch, and draw them into a competitive policy posture, industrial--how are they connecting with these entrepreneurs?

MR. BENSON: I can only reference from what I read in that article, but there were a variety of activities on design associations and specific activities to go from this Maker movement to actually begin to industrialize that and to turn that into a more formal operation.

We've got some of that here as well, and whether, who's got a leg up there, I don't know. One of the interesting things is that particular city, Shenzhen, from what I've read, that's like the Mecca of this kind of stuff. I mean everyone talks about that's the place. My understanding, you can walk down a market, and it's like where you might have fish at Pike Place Market in Seattle, this is like baskets of chips, of memory chips, of integrated circuits, and it's that--and if this one doesn't work, they'll take the label off and put this one on. There you go. That was an eye opener to me.

To extend on that just for a second, there's a video that I stumbled across about four or five years ago from a guy that was giving a talk on getting into, hacking into a card, a memory card, and I think there's some technical aspects to it, which is interesting, but in the course of

that, he talked about being in this marketplace in Shenzhen, and he said that, he said you could go into where these things are programmed. He said I've been in these places, and there's literally chickens running across the floor, and he said there's not badging, there's not identification, there's not auditing, there is not provenance guarantees.

But it's really open. And one could walk up and put in whatever file set they wanted to go configure that chip. Well, that was an eye opener to me because in my mind, what I thought before, I remember those old Intel commercials where the guy is in the moon suits and that's what I thought, well, that's where all the chips come from. But no, this is coming from a place that's not protected, and there's chickens running across the floor, and those are going to be--and that's not all, the way all are manufactured of course, but that's where a lot of them are, and they're going to be a lot cheaper than those that are highly regulated. So people will buy from that.

It was an eye opener to me, but I don't know what is in this thing. I don't know what is in it, who put what in it, I don't know what the--I don't know how it got there. I just kind of go, I hope it works, you know.

[Laughter.]

CHAIRMAN CLEVELAND: Thank you.

HEARING CO-CHAIR WESSEL: Commissioner Stivers.

COMMISSIONER STIVERS: Thank you. Thank you both for being here today.

Mr. Brake, you mentioned in your testimony that 2012 House Intelligence Committee report that found that Huawei and ZTE, China's big telecom companies, cannot be trusted to be free of foreign state influence and thus pose a security threat to the United States.

I know we'll talk more about the security issues in the second panel, but with that component, and in addition that we know the Chinese government employs protectionist policies to limit access to its domestic market, which is growing and will be quite large in the future.

In particular, Beijing guarantees that Huawei and ZTE each receive one-third of the domestic 5G network contracts. U.S. firms face data storage restrictions and are required to form joint ventures with Chinese firms that has all sorts of negative consequences, including intellectual property and R&D concerns.

But at the same time, Mr. Brake, you state in your testimony that blocking specific firms from U.S. market access is, quote, is "likely not the best route." If that's not the best route, then how do you, as you mentioned, guide China into a rules-based order when Beijing clearly thinks that it's benefiting from the status quo?

MR. BRAKE: Absolutely. I agree this is a very difficult line for us to walk in terms of U.S. policy. To try to put it succinctly, my recommendation would be to double down on our rules-based approach to, and institutional-based approach to make any potential security threat clear and public before denying access to the U.S. market, to lead by example of how we expect reciprocity to occur in China.

And so what we should do is coordinate with other Western markets to create an institution that can to the extent we would expect we would be treated, that we would hope we'd be treated, technology firms would be treated in China. Look under the hood and try to examine whether or not there are security threats.

We should also make clear that if one is found, if an intentional vulnerability is found, there would be severe repercussions that these firms would essentially be locked out of not just the U.S. market but other like-minded Western markets to change the economic calculus of this potential security threat.

COMMISSIONER STIVERS: I mean we've through the WTO and through bilateral negotiations, we've been negotiating with the Chinese government on market access issues for 30 years, and there hasn't been a whole lot of progress, including when China joined the WTO and made all sorts of commitments on a lot of things that haven't come to pass.

Don't you think that the status quo needs to be changed, especially as we move as the world moves into these very high-technology firms and Chinese government, it's a state-driven approach, are really changing the rules of the game so that they gain an advantage to a detriment, you know, in a long-term way of foreign firms and the United States too?

MR. BRAKE: Commissioner, I think you're absolutely right, that more needs to be done. I would point you to the work of my colleagues. We recently issued a rather extensive report on addressing Chinese innovation mercantilism, and again this is exactly the approaches that we need to rely on, organizations like the WTO, to bring formal processes to combat these unfair trade practices.

To simply state that this is a national security threat with no more process behind that and to block these companies, I think encourages similar behavior by the Chinese. But absolutely correct that this is a problem that needs to be addressed.

COMMISSIONER STIVERS: Mr. Benson, do you have any thoughts on the topic?

MR. BENSON: Just one comment on that regarding looking under the hood. I agree, we want to be able to do that. A danger that we have is that that will get harder and harder to do because things get more and more complex so there's so many different device types and thing types, to include the stuff that's actually driving 5G and routers and switches and things like that. So we do want to look under the hood. But that won't be an end in itself, and I'm not suggesting Mr. Brake was saying that.

But it just gets harder and harder to do because the technology is getting more and more complex.

COMMISSIONER STIVERS: Thank you.

HEARING CO-CHAIR WESSEL: Senator Talent.

COMMISSIONER TALENT: Well, I'm going to follow up on what Commissioner Stivers was asking about and maybe go at it this way with you, Mr. Brake.

So we know what they've been doing in a whole lot of different areas: requiring joint ventures if you want to invest; requiring that they turn over the technology; requiring you store data in China; discriminatory regulatory enforcement. I mean the list goes on and on; right?

MR. BRAKE: Yes.

COMMISSIONER TALENT: And they know they've been doing those things. They may deny it, but they know they've been doing those things. So, you know, what about an approach where we just say to them, look, we've been putting up with this all this time because we don't want the world system to move into this direction, but we now think that the only way to keep the world system from moving into this direction is to begin doing some of these things to you so there's actually a cost.

See what I'm trying to get into is the approach, the model, that you have, very understandable. It's like we don't want to do this because then they'll do it, but I guess what I'm suggesting to you is that it's had exactly the opposite of that impact. By not doing it over the years, it's enabled them to continue doing this because they gain, they don't get any cost.

So I don't, you know, I don't want you to--you can tell the concern here, which is across the Commission. I don't want to--because I think you recognize the problem and you're

exploring for solutions. But I just think doing what we've been doing in the past--301 actions and the rest of it-- that's not going to have any different result.

MR. BRAKE: Absolutely.

COMMISSIONER TALENT: So if you want to make a further comment on it, that's fine. But that's, that's the area that I want to explore with you.

MR. BRAKE: Absolutely. Senator, absolutely appreciate your point, and I think you're exactly right, that we need to do more in this area, and I appreciate that you recognize the fine line where we don't want to encourage further protectionist behavior on behalf of China.

Again, I think that the answer should be reliance on existing institutions' mechanisms in further cooperation with like-minded allies. This can't be a go-it-alone U.S. approach of simply denying access to the U.S. market. It has to be coordinated with other, other allies, other Western markets.

COMMISSIONER TALENT: I agree that that's ideal, but as you work with partners, which is an important thing to do, that makes it, I mean that adds orders of magnitude to the complications of actually doing anything because you've got to get agreement across more than one government.

I just think that those who believe, and I believe as you do, I do not want the government running this. I think our approach, a decentralized innovative approach is going to beat their approach unless they're able to short-circuit it in some fashion. I just think that scholars and organizations that believe that really need to apply yourself to the idea of what solutions, some hardball solutions we can use because otherwise, I mean if some of the things Mr. Benson is talking about come to pass, and it's traced back, your concerns about, I mean the backlash here then is going to be very intense and maybe an overreaction.

If you want to comment, you can. That's all I have, Mr. Chairman.

MR. BRAKE: I would just note that it may very well be that there are, as, for example, Christopher Wray, the FBI director, has noted, that as a classified matter, there are severe security concerns. That might be true, but I wish that there was more forthcoming, more public information to back that up in order to not give the perception that it is, that it is pure protectionism.

COMMISSIONER TALENT: Right, yeah. And the problem they have, of course, is they can't talk except in terms of generalities because so much of it is classified.

MR. BRAKE: Exactly, yeah.

HEARING CO-CHAIR WESSEL: Dr. Wortzel.

HEARING CO-CHAIR WORTZEL: Thank you both.

I guess we've really, as a Commission, we've had some success with taking what the federal government refused to discuss about cyber security and cyber penetration and making it public with our Mandiant report, both the Mandiant reports we did.

I think we're moving toward a point where the Commission may have to do that with a topic like this because we really there documented penetrations and had companies document penetrations, which brings me to your testimony.

You talked about the problem of inserted security threats and trapdoors. So my--the first thing I'd like to hear both of you discuss is if you just open things up and said, sure, even though the FBI director had--and cities have done this--said even though the FBI director said worry about Huawei, worry about ZTE, we like them, they're cheap. We're going to use them. And we know that not only is their hardware in there, but there are software updates that go back and forth.

Can you talk a little bit about how we might be able to figure out what's being sent back and whether that's a problem and malicious so we can document these things?

The second part of both your testimonies is the question of security and best practices. We just got--I just got a copy of China's Standardization Law. They standardize it across the country at the county level everything, and then lower level municipalities just have to follow the county regulation.

Are there states, cities or universities that you know of in the U.S. that have such exemplary regulatory networks standardization and supply chains that you could use, we could use, someone could use as an education effort because if we can't regulate it, you're going to have to educate a lot of people?

MR. BRAKE: So, Commissioner Wortzel, if I may, so I'm not a cyber security expert--

HEARING CO-CHAIR WORTZEL: We've got that this afternoon.

MR. BRAKE: --if I may address the second part of your question. Yeah. So I think the point you made is absolutely spot on. To my mind, there are all the issues with the competition in developing the standards and the IT, but what really makes the biggest difference is the success and deployment in actually using these, these next generation platforms.

The big sticking point are policies on the local level when it comes to siting small cell equipment, access to rights-of-way, access to utility poles, and there are some examples of very exemplary cities. Kansas City, Boston, Las Vegas have all worked with operators to significantly lower the cost of deployment, the fees for siting.

There are also some examples of cities moving in the other direction. ITIF, we've noted some concerns with, for example, the city of San Jose, California, where they have been seeking fees for siting of small cells on light poles that are a percentage of revenue, not just profit, but revenue, and seeking to get significant fees.

We worry that this, you know, allows what's essentially a tax to the city. The city can, we know, put this towards general use funds in a way that is spread over the entire user base of the wireless networks. So a problem with the externalities there.

So lowering the costs of deployment, the siting, and fees is I think the number one policy lever that the U.S. can help to standardize the deployment of these 5G networks.

MR. BENSON: One comment on the last thing Mr. Brake said. I have heard anecdotally that some providers have been pretty heavy-handed regarding pole attachments, that kind of policy, and it's looking for long-term no-fee access for decades. That sounds to me a little problematic. That's just one piece of it.

Commissioner, you mentioned before, you said what's being sent back, were you talking about data that's being sent back? There's no limits. It could be anything. It could be anything that's sensed. It could be audio, video. It could be something that's going on in a sensitive or a critical area. There's no limit on the type of data that could be sent back if something was maliciously developed or there's a vulnerability in it.

There might be a limit to volume because in a lot of institutions, you do try to detect changes in volume in looking at traffic in a general sense. But there's no limits to what types of things could be sent back.

You mentioned standardizing at the county levels across China. I mean I would like to see some more, more move towards standardization here without being completely authoritative because right now it's pretty wild west at the institution and city level. We depend a lot on vendors, and one of the things I try to do at our university and other universities, I try to get us to

raise the bar when we have these vendor relationships and say these are our expectations of deployment.

I want default passwords changed. I want any extra services that aren't being used, I want those turned off. I want to know where you put stuff. I want to know what IP addresses you have. I want a list of versions and version numbers. I want to know what's patchable and not. I think you indicated this awhile ago. That's a big thing too. We all talk about, well, we'll go patch these things.

Some of that is just fantasy. I mean with what we have out there now it just won't be patched. So one of the things we try to do is, okay, what is the critical stuff that I know that's got to be patched, acknowledging that some of it is not going to get patched. Ideally, yes, it all would be.

I think in that new cyber bill that came out last summer, that was one of the things you had to, to sell to the federal government had to demonstrate that it was patchable. I think that's a good thing to ask. I wonder how successful that will be.

HEARING CO-CHAIR WESSEL: I'd just make a quick note that the first thing Lenovo did after they bought IBM's PC division was they changed where patches were deployed from--New York to Shanghai. So I'm not necessarily confident that patching strategies are going to be in our interest, but we'll deal with that this afternoon.

Senator Talent. Senator Goodwin.

COMMISSIONER GOODWIN: He can have my question.

HEARING CO-CHAIR WESSEL: No, it's all for you. Sorry.

COMMISSIONER GOODWIN: Thank you, Mr. Chairman. Thank you, gentlemen, for your time this morning.

I want to follow up on the discussion you were just having about standardizing some of those location and installation requirements. Obviously, I think a lot of folks were intrigued by the leaked memo from the National Security Council about nationalizing the 5G network. Obviously, that raises significant concerns about stifling innovation in a private sector, but also raises similar concerns of federalism stepping on the toes of states, cities and municipalities to impose their own rules for the location and installation of this equipment.

But my question is, is there a value to the federal government given the risks raised in that memo to providing some guidance and standards and principles for where these antennas and other pieces of equipment can be located?

MR. BENSON: I think, because there is a risk of over-centralization, of being too prescriptive, and not being sensitive to individual deployment needs, I think one of the places the federal government could add value is to support meetings and conferences that are not vendor driven to have these conversations around governance and maybe establish a loose framework from which cities could build on for their own particular, for their own particular use.

But the opportunity for cities to get together and have that conversation, again without vendors, and I'm not knocking vendors, but it's a very different conversation--

COMMISSIONER GOODWIN: True.

MR. BENSON: --when it's vendor driven. So I think there's some opportunity there to facilitate that governance development.

COMMISSIONER GOODWIN: In those international bodies when you were, Mr. Brake, earlier answering some questions from Commissioner Wessel, you talked a little bit about what the federal government could do to encourage American companies to gain a more prominent role and voice in those bodies.

But I noted in your written testimony that you included a passage from an FCC commissioner who noted that the internal processes of those bodies need overhaul to prevent authoritarian governments, like China, from pushing their own myopic agenda.

What are those internal governance standards, rules and processes that he was referring to and how can we combat those?

MR. BRAKE: So the ITU is an incredibly complicated body with arcane processes and very difficult to navigate. My expertise only goes so far.

My understanding, one of the greatest concerns is that leadership within the ITU has not been adequately represented by the United States. It has been quite some time since the ITU was led by an American individual. What Commissioner O'Rielly had pointed out was that we are giving outsized amounts of money as compared to the amount of leadership and influence that we have within the ITU.

COMMISSIONER GOODWIN: Thank you.

HEARING CO-CHAIR WESSEL: I'll get the name right. Commissioner Bartholomew.

VICE CHAIRMAN BARTHOLOMEW: Thank you, Mr. Chairman, and thank you to our witnesses. It's interesting. Thank you particularly for being able to have this conversation at a technical level that those of us who are not technologically adept can understand.

It seems to me that one of the reasons we're all here is there's sort of two sets, two buckets of issues that overlap. One, of course, is the economic, the trade, the unfair, lack of reciprocity, but then there's this whole other set of issues that I think a lot of the Internet of Things also really raises.

One of the reasons we are concerned about China's participation in all of this is if you look at what they're doing in their own society and exporting--massive surveillance, use of artificial intelligence for facial recognition, controlling-- it's a mechanism ultimately to control what people say and do, who they feel free that they can talk to, where they can go, and they're exporting that technology.

So the Internet of Things, I'm always struck, you know, Kellyanne Conway was ridiculed when she said that basically you can do, you know, surveillance through microwave, through your microwave, and yet all of these things that are in our homes, all of consumer products that are going on are providing information, and who controls that information, how that information is protected is a really important thing.

So I was very interested, Mr. Brake, that you note in your testimony that there can be a distinction for equipment that is destined for national security or public safety networks rather than everyday consumers, first, because, of course, people take their personal devices into all sorts of places. I'm not even talking secure facilities, but places that have information. And also it is tracking consumer information that is, or what consumers are doing that is a big part of what China is trying to do for its social control inside its own society.

So I'm having trouble understanding how you would distinguish between national security at public safety networks instead of just everyday consumers. That's one set of things.

I think we have a little bit of time so I'm going to put another one out there, which is obviously our society has benefited enormously from the private-led sector innovation and experimentation, but the role and the responsibility of companies is to make a profit, to provide returns to shareholders when they are a publicly listed company. It is not about protecting the national security. There's a whole other basket of issues that is not their main responsibility.

And I'm concerned about whether when we are up against--I'm going to use that phrase--up against a society that is centrally controlled, that's authoritarian, whether we are protected

enough, using simply just an example that my brother's identity was just hacked. Somebody ported his telephone number. It was multiple company failures. Somebody ported his telephone number to another telecom company. Somebody probably, obviously the same people went into his financial, they went into his bank account and transferred money because they had been able to get his Social Security number from another hack.

So that's failure of at least three companies, and how do we tie this all together in a way that protects people, protects our national security and protects people, as it all expands? You know you're talking about smart cities, smart universities. Everything is connected in a way.

Well, let's of questions. There are two.

MR. BRAKE: Absolutely. So if I can jump on your first point, and point well taken, the distinction between equipment destined for public safety national security critical networks and more consumer oriented devices is a fuzzy one. At the same time the point I was trying to make, and forgive me if it wasn't clear in the written testimony, if we are standing up an institution to evaluate the security risks of equipment from foreign supply chains like Huawei, ZTE coming into the U.S. market, we could have a much more robust, maybe even a screen for saying, you know, you know what, we're only going to trust, you know, particular vendors for critical networks security infrastructure and make it as simple as that.

When it comes to broader consumer mass market, then have some institution, some process stood up to evaluate that on a more ongoing basis if that makes sense. The point simply being that you can make those sort of distinctions. But point well taken.

On your second point, absolutely, it is a brave new world of all sorts of potential security vulnerabilities that have to be addressed going forward on a case-by-case basis. I don't think that this is a reason to take our foot off of the gas when it comes to driving towards innovation. The mission is incredibly important to drive productivity economic growth.

At least to the particular example, this number porting threat vector, relatively new problem that you would think could have been addressed earlier. But there are absolutely steps--pin numbers or other ways to identify someone as having the actual phone number instead of just porting it at a request. So I think that individual security vulnerabilities like this number porting vector can be addressed going forward. It's a difficult unfortunate experience--

VICE CHAIRMAN BARTHOLOMEW: Yeah. Oh, yeah. It's fortunate that it wasn't a significant amount of money, but it was just quite astonishing that it was a cascade of failures, and it was at least three different companies that were involved in a cascade of failures. And so my concern there is both how, what expectations we have of private companies, how we communicate those expectations, how you knit that together, not just for the individual consumer, but for our larger security concerns, as more data is being gathered?

I know they're big challenges, but we are up against a country that has none of the constraints in terms of what their government is doing and how they're using that information that we do because of the values that we have.

MR. BENSON: One thing to keep in mind in this is we give a lot of it away, like Facebook, for example, we just, there you go, you can have it. We do a lot of things for convenience so we have to, I mean as consumers, that's what we do. If it's easy, we do it. And it seems if you push down the age, they're more willing to give stuff away, giving away privacy.

I've got an 11 and a 13-year-old so we're starting to have those conversations about what you do and don't do and what you might get pressured into. So that is a challenge, and we do tend to give these things away on our own.

One thing about what, how companies can be liable or what their roles and responsibilities are, in the IoT space, one of the things I've thought a lot about is I think some of the big companies, they're going to be motivated to protect their brand to some degree. I'm not saying that's the end that's going to solve everything. But they're going to be more willing to make some investment in security protocols and risk management protocols than a small to medium-sized company.

And I still want small to medium-sized companies to be in the game, but I think they're going to be motivated, to some degree, by brand protection to try to be a better player.

VICE CHAIRMAN BARTHOLOMEW: I wish I could believe that.

[Laughter.]

HEARING CO-CHAIR WESSEL: We're going to do a second round, and I'll kick it off. I'm not trying to pick on you, Mr. Brake, but when I was listening to you about a rules-based multilateral approach, I was thinking of the arguments that were made when we granted PNTR [permanent normal trading relations], and as I think you've seen, and also from documents done by your organization, the mercantilism report, et cetera, work on the 301, on IP theft, forced technology transfers--I could go on--we're not dealing with a country that respects the rule of law.

We're on the verge here, not only on the verge, we've already begun certainly on IoT, which is out there, 5G, which is well advanced, some deployments are expected to start later this year, as you know, here in the U.S., and there are deployments elsewhere. So if you believe any of the estimates in the NIC report, the National Intelligence Council report was based on private sector work about the 12.3 trillion and 22 million jobs.

It seems to me you're arguing, okay, let's, let's not worry about provenance, let's not worry about, you know, what the motivations are. Let's try and do this the right way. We all want to do it the right way, but doing it the right way requires countries that respect the rule of law. So as we see this $12.3 trillion opportunity, again, from every public utterance, from the 400 plus billion dollars that China has already announced publicly it's putting here, it seems they're hoping that, you know, we will be the good government rule-of-law country we've always been while they capture all the benefits. Am I wrong?

MR. BRAKE: It absolutely is a sizable challenge. I don't think that you're wrong in identifying the challenge here. There are, the Chinese have made significant investments in R&D in supporting these companies--Huawei, ZTE. Though they profess to be employee owned and distance themselves from Beijing, they do get significant amounts of capital from state-run banks at very favorable rates; they sell to the largest carrier in the world, state-run China Mobile.

They are playing a different game than a lot of Western companies, but, again, I think--and I would direct you to the work of my colleagues on the recent report to rely on existing institutions. Even if we are effectively blocking these companies from the U.S. market, to put process and institution behind that I think is very important.

HEARING CO-CHAIR WESSEL: I don't think we're blocking those companies. I mean handsets, you know, is sort of a shiny object, but as I understand it, again not being a technician, Huawei, that the ten percent figure you identified, you know, is Huawei, ZTE and others. Huawei is the leader in software defined radio and a lot of enabling technology.

So it may be that, you know, the representation of Huawei that has the name on it that is public-facing for an average consumer has been blocked because of Director Wray's and others' comments, but, you know, Huawei has advanced its own opportunities here in the U.S. market significantly.

MR. BRAKE: So I would only note I think we should make a distinction between different types of telecommunications equipment. ZTE, Huawei have been--though my understanding is some small rural carriers have been using their equipment, and it is present in the U.S. market, but large U.S. companies, not just handsets, but the actual underlying equipment.

HEARING CO-CHAIR WESSEL: Agreed. For the routers and switching, agree.

MR. BRAKE: Their accomplishments in the IPR realm, most notably, I think very importantly, they have one of the essential patents. They developed the technology that is being used for that control anchor for the version that at least we'll be using in the United States. The LTE communication with the sort of new 5G technology is Huawei developed.

But again I think that those, we should try to evaluate the cost/benefit, the risk evaluated with bringing those sorts of technologies in. For that coding methodology, that's just math, right. That's not, there's not, no way to fill--

HEARING CO-CHAIR WESSEL: But again I'm not looking at the security risk. I'm looking--again, we're going to do that later. It's about the economics, you know. We don't have any--as far as I know, we have no handsets under $400 that are made in the U.S. anymore, et cetera. I mean we've seen the outsourcing of significant amounts of technology to China.

We had, last year I believe, was 114, if the number is correct, billion dollar trade deficit in advanced technology products. You know we may be developing the next wave of the technologies, but the products aren't being produced here largely. Is that--

MR. BRAKE: I mean especially with the networking equipment, the wireless equipment, there aren't really U.S. companies. That's all Nokia, Ericsson, Samsung. You're absolutely right. This is largely--

HEARING CO-CHAIR WESSEL: There are some, Infinera and some others, but they are smaller players and maybe we can do something about increasing the volume there.

Did you have a comment, Mr. Benson?

MR. BENSON: I don't.

HEARING CO-CHAIR WESSEL: Commissioner Tobin.

COMMISSIONER TOBIN: Thank you, Mr. Chair.

You both outlined what one of you called a "brave new world." And I think for the record what we've all got to be aware of fully is this is a competition. This is a competition where we've heard the numbers on the Chinese patents. We heard yesterday the numbers of increased Chinese leading the standards organizations, and at NIST, they were also telling us what most of you know, that the numbers of engineering graduates are diminishing. The United States has almost always led the standards organizations to be able to provide that world view we're talking about where businesses can innovate, et cetera.

So with Commissioner Stivers and Commissioner Talent's questions, they were pushing you to think about how do we combat, how do we take this to WTO, et cetera. But I think a major part of the problem is also we've got to get our act together as a country and play ball and step things up, and you had a recommendation, Mr. Brake, on supporting basic R&D, and I'd like you to expand on that a little bit more on specifics on where and how you would do it so we can get some results if we're playing.

And then, secondly, the Chinese have numbers at these standard setting bodies. They're getting leadership positions. Have you thought about what we could do? Who incentivizes that? It was something this country pursued with pride, and I just don't see us--back to the "brave new world"--we've got to compete. We've got to stay on top.

So, Mr. Brake, first, and then Mr. Benson, please.

MR. BRAKE: Absolutely. So to your first question, absolutely the government should be supporting basic R&D to help see a continued innovation in wireless networks. In some ways--

COMMISSIONER TOBIN: Through what channels?

MR. BRAKE: Absolutely. So some success stories within the 5G story itself. NYU within their engineering department is responsible for some of the major breakthroughs in using the very high frequency spectrum. It was expected to be incorporated to 5G. So continue to rely on university research and support through National Science Foundation grants and the like, expand those sorts of programs.

There is also--forgive me--I believe--I can look this up for the record--but I believe that it's through the National Science Foundation, but there is a program where an organization has devoted $4 million to building out four different sort of test platforms within different cities and taking on the expense of developing expensive software defined radios to build out for, as a platform for universities to experiment upon. I think that can built on and expanded, as an example.

COMMISSIONER TOBIN: For the testing like out of the Maker movement and things like that? That kind of testing?

MR. BRAKE: Like the advanced networking technology, software defined networking and software defined radios combined can allow for a wide array of different innovation, essentially moving what was done in hardware for networking to be moved into software. That opens up a whole new realm of innovation and to allow for different platforms for that experimentation to not just occur within private companies but also within the university research institutions.

COMMISSIONER TOBIN: So leadership.

MR. BRAKE: An example.

COMMISSIONER TOBIN: Governance organizations, standards organizations? Do you have any?

MR. BRAKE: Absolutely we need to be encouraging our companies to invest more in the standard setting process. I'm not sure the exact right mechanism to do that. I believe it could be done through a tax incentive. We don't want to go down the same route as China, directly subsidizing, that sort of participation.

Another key point when it comes to spectrum allocation, every three to four years, the International Telecommunications Union hosts what's known as a World Radio Conference where international spectrum allocations are coordinated. This is an incredibly complex important process that our delegation is led by the State Department. I think it's incredibly important that the State Department engage early in developing regional agreement coordination going into that process.

We're looking at WRC-19 hopefully developing consensus at the U.S. level later this year to develop regional coordination going into that process by April, late in spring of next year, and that's a State Department-led effort.

COMMISSIONER TOBIN: That's useful. Mr. Benson.

MR. BENSON: So I come back to my perspective as how these systems are deployed is a big gap for us. There's lots more we could do with technology, but how--we are not good at how we deploy it, and I think we, a concern I have as we keep developing new technology, we

don't deploy it well, we don't govern it well, we don't make good decisions, and I think that will come around to bite us.

You could google and you could see that there are different universities, they've got some IoT curriculum, and to me that's not super hard to put into place because it's more technology and more development. You can make a device instead of this. But I would like to see that kind of technical development as a curricula that integrated with the governance pieces, the data ethnography pieces, the ethics pieces.

I think that's relevant because we talk about cyber--

COMMISSIONER TOBIN: Interesting.

MR. BENSON: --security a lot, but also we want these investments to be good investments; right? For a city or institution, we want to make a good investment. So we see a return on that. And if we don't get a handle on some of this, we won't see a return, and we will have burned that money up, and we could have used somewhere else.

COMMISSIONER TOBIN: Before I close, I'd be interested in--in time--to hear how your working group is functioning because that, too, could be a model for universities.

Thank you very much, both of you.

HEARING CO-CHAIR WESSEL: Dr. Wortzel.

HEARING CO-CHAIR WORTZEL: We've talked a lot about security here although this panel is supposed to be on the economic implications. So I'm going to try and move back toward that.

But it kind of relates to security. You know, Mr. Benson, you had the example of going through a camera in Turkey, I think it was, entering an industrial control system and blowing up a pipeline--or a pipeline blowing up. We just found that--I mean the U.S. government--Congress just found that an entire U.S. military base had all its cameras coming out of a particular company in China that was getting its patches and everything through that. So there's potential vulnerabilities there.

But the economic implications that I'd like you to address are what if you really tried to establish trusted networks of suppliers and supply chains? What would that mean for our existing industry and what would that do to costs?

And a second part of that I'd ask is I guess the intelligence community just recommended eliminating an entire class of cyber security software by a Russian vendor because it was a Russian vendor and they felt it was doing bad things.

What are the economic implications of eliminating an entire nation from our supply network? Not necessarily because we found everything was bad but because we feel the potential for it being bad is very high.

MR. BENSON: On the cost of trusted networks and supply chains, it is--I don't have a dollar figure on it, but it is substantial. In universities and cities, there's legacy systems, and I say legacy, I don't mean like super, super old, but they're configured in a certain way, and they're managed in a certain way, and there's a network segment over here that does this, and a segment that does this, and a segment that does this.

When you want to go to reorganize that within a big bureaucratic institution like a university or city, it is a lot of work, and it is a lot of work managing these networks and managing these pieces. That's a part we, we frequently we miss--the work to actually manage a network or manage a network segment. So there's a real cost to that.

On the supply chain piece, I think there's a cost to that too because right now we largely don't track that. And there's lots of different pieces and lots of different components to each of these devices. The cost, it's nontrivial.

Regarding the Kaspersky, it's a problem, I mean from way back, and most of us didn't pay attention to cyber security. You talk about that, but you've always had one eyebrow kind of hiked. It's like, well, where is this, where is this coming from? But to your point, but to cut off the whole thing, that's problematic also.

I don't--

HEARING CO-CHAIR WORTZEL: Right. You know, I don't care what the Russians--the Russians don't go after me, the Chinese go after me.

MR. BENSON: It's a complicated problem.

[Laughter.]

HEARING CO-CHAIR WESSEL: He's just being paranoid.

[Laughter.]

MR. BENSON: Reasonably so. I wish I had a better solution to that, but I don't.

MR. BRAKE: So I would just note, a lot of the difficulties we've seen around China, unfair trade practices, support subsidies, all sorts of those issues, absolutely important. Huge economic significance for ICT sector, and those problems should be addressed.

I do think it's important to keep in mind that compared to the platforms that these enable, the economic innovation that is built on top of this, that is a tremendous question mark. We don't know exactly--just like you couldn't imagine what, you know, innovations 4G networks were going to enable back in 2005, we're not quite sure what will come out of having real-time latency, very secure communications, but especially when combined with artificial intelligence machine learning.

This is new technology that can enable, you know, very real innovation. And so there we have to lean in on actually deploying these networks, getting them built out within the United States. Those we have very clear policy levers on.

HEARING CO-CHAIR WORTZEL: I mean the interesting thing is this Chinese standardization law actually links standardization across the country to the import-export law and the quality control law to allow measures to be taken against foreign imports of both material and services. So that's pretty protectionist.

MR. BRAKE: Absolutely.

HEARING CO-CHAIR WESSEL: Before I turn to Commissioner Bartholomew, a quick question, and I've had a presentation on smart light poles and all the various other things.

Are you aware of any U.S. vendors in this area having access to Chinese markets for what they're doing in smart cities?

MR. BENSON: I can't speak to that authoritatively. I mean I can't imagine that--I mean I would image that Cisco has got a play in there somewhere; Intel has got a play in there somewhere. I would assume that there's some of that, and how that's regulated on the Chinese end, I don't know.

HEARING CO-CHAIR WESSEL: Okay. As you do your work, if you come across any information and you can share it with us, that would be helpful.

Commissioner Bartholomew.

VICE CHAIRMAN BARTHOLOMEW: Yeah. Two comments. Again, thanking our witnesses. I just want to clarify one thing that Commissioner Wortzel said about the U.S.

government finding that these Chinese-produced surveillance cameras were on a U.S. military base, and that was because of our freedom of the press.

It was a U.S. journalist who actually found this who then brought it to the attention of the U.S. government. So I think that's an important thing for us to remember as we talk about our values.

The second thing is--and this hasn't come up at all, but when we talk about, talk about the economics of all of these things, that the pressure that everybody is under in this country, our universities, our communities, to get lowest cost producers, and that the Chinese government, which has demonstrated that it's protectionist in any number of ways, is subsidizing the companies so that they can make sure that the lowest cost equipment is what is available, and that is a tactic.

It's a tactic both to get the equipment in here and to get the sales, and it's something that I think that we're going to have to also deal with as we look at all of these issues.

So thank you.

HEARING CO-CHAIR WESSEL: With that, we will recess for 15 minutes. Thank you both for all your work and hope you will keep us advised of your ongoing work. It's very helpful and appreciate it.

We'll break for 15 minutes till 11:20.

[Whereupon, a short recess was taken.]

PANEL II INTRODUCTION BY COMMISSIONER LARRY M. WORTZEL, PH.D.

HEARING CO-CHAIR WORTZEL: Our second panel today is going to assess security, safety and privacy risks from the U.S. usage of Chinese-made and Chinese-developed Internet of Things and fifth generation networks, equipment, and software, and how the United States could mitigate risks.

We're joined by an expert group of panelists to discuss the challenge. It's International Women's Day. I was just reminded. So I'm making an executive decision and changing the order. In fact, this year, we elected two women as our chairman and vice chair in honor of International Women's Day--Women's Year.

[Laughter.]

CHAIRMAN CLEVELAND: Done?

HEARING CO-CHAIR WORTZEL: Done.

[Laughter.]

HEARING CO-CHAIR WORTZEL: So first we'll hear from Jennifer Bisceglie. Did I pronounce that right?

MS. BISCEGLIE: Uh-huh, perfect.

HEARING CO-CHAIR WORTZEL: She's president and CEO of Interos Solutions, a supply chain and vendor risk management platform company that serves the public and commercial sectors.

Ms. Bisceglie is also the lead author on the forthcoming Commission-contracted report on U.S. federal IT supply chain vulnerabilities from China.

She is the chairperson for the Public Awareness and Outreach Working Group for former Virginia Governor McAuliffe's First Cyber Security Commission, and she's an active member of Women Impacting Public Policy, and CEO of Quantum Leaps.

The next panelist will be Anthony Ferrante, Senior Managing Director and head of the Cybersecurity practice at FTI Consulting and an adjunct professor of computer science at Fordham University's Graduate School of Arts and Sciences.

He's got more than 15 years of cybersecurity experience providing incident responses and preparedness planning to more than a 1,000 private sector and government organizations.

Prior to joining FTI Consulting, he served as Director for Cyber Incident Response at the U.S. National Security Council.

Our third panelist is Dr. James Mulvenon, general manager of the Special Programs Division of SOS International. He's a contributor to another Commission-contracted report on "China's Internet of Things."

Dr. Mulvenon has published widely on the Chinese People's Liberation Army, as well as on cyber and espionage issues. He's the author of a 2013 book China's Industrial Espionage. He's chairman of the Board of the Cyber Conflict Studies Association and a member of the National Committee on U.S.-China Relations.

Thank all of you for being here and for your written testimony. We're going to try and limit each of you to seven minutes of oral testimony. The first panel had more, but there were only two.

Ms. Bisceglie.

OPENING STATEMENT OF JENNIFER BISCEGLIE, PRESIDENT AND CEO, INTEROS SOLUTIONS

MS. BISCEGLIE: Thank you, Co-chairs Wessel and Wortzel, Commission members. Thank you for the invitation to speak with you today on the concerns of technology coming from China and being used in our federal IT networks.

By way of introduction, Interos is a company I founded 13 years ago to evaluate risks in the global economy and the business partnerships, alliances and distribution networks that make up our supply chain. The company is built on my over 25 years in global supply chain industry, having helped multiple U.S.-based companies create maximum advantage from different skillsets, labor pools and competitive business arrangements with partners around the world.

During those years, I've watched risk concerns in the supply chain move from quality to physical security, to resiliency, and now to product integrity. Interos recently submitted its final report, as was just mentioned, to this Commission on the Supply Chain Vulnerabilities when sourcing technology from China and using that technology specifically in U.S. federal IT networks.

We stress several solutions in the report, the most important being that the U.S. establish a national strategy for supply chain risk management--we heard a little bit about that this morning--with supporting policies so that the nation's security posture is forward-leaning versus reactive and based on incident response, which it normally is right now. Our adversaries are very public about executing a strategy against us, and the time has come for us to stand strong and visibly protect ourselves, which was your point.

In being invited here, I was asked to speak to six different areas that are directly related to our report. I have submitted written testimony addressing all six areas. I will be summarizing them for this hearing, focusing on three, and then opening the remaining time for your questions and discussions.

By addressing specific--before addressing specific areas of the report, we would like to stress that whether it is 5G, or blockchain, the Internet of Things, or any other emerging technology, an underlying foundation for security is understanding who the stakeholders are, where your vulnerabilities lie, and having a strategy for managing the associated risk.

Given our position in the market, Interos has had the opportunity to work with public and private sector organizations spanning multiple industry verticals and the situation is literally always the same. If the organization doesn't take a focused and comprehensive approach to risk management, prioritized by senior leadership, there will be unnecessary exposure and invariably negative impact.

We'd also like to stress that the supply chain attacks will continue to become easier and more prevalent as emerging technologies increase the attack surface exponentially over the years. Gartner predicts that by 2021, there will be 25.1 billion IoT units installed, and by 2020, IoT technology will be included in 90 percent of new computer-enabled product design.

One point of clarification before we dive into the specific ares--I'm going to use the term "SCRM" a lot today, and it's a standard spoken acronym for supply chain risk management. It just makes it quicker to get through the testimony.

[Laughter.]

MS. BISCEGLIE: So three main questions we were asked to focus on. One, how reliant are the U.S. government and U.S. IT firms on Chinese firms and Chinese-made IT products and services?

And honestly, in short, the answer is "very." Over 95 percent of all electronic components and IT systems supporting federal IT networks are called "commercial off-the-shelf," or COTS products, and China's role in the global supply network is significant.

China assembles most of the world's commercial electronic devices--again, we heard a lot of this this morning--produces parts such as microprocessors and flash cards, and dominates the world in volume of IT industrial capacity and manufacturing.

For our report, we reviewed transactional data and found that the import/export information shows that between 2012 and 2017, China is the overwhelming source of products for Hewlett- Packard, IBM, Dell, Cisco, Unisys, Microsoft and Intel, which are some of the top enterprise IT providers to the U.S. federal government.

Second question, to assess the government's success in managing the risks associated with Chinese firms and Chinese-made products and services to its IT procurement supply chains.

We focused on three main areas here. One, federal government laws and policies do not currently address risk management comprehensively. Two, in the current SCRM ecosystem, responsibility for risk management is held at different levels within the agencies, resulting in SCRM offices that function largely as under-resourced stovepipes, often lacking an executive sponsorship or oversight and only catering to the needs of procurement policies of individual programs, leaving huge gaps in opportunity.

Third, policy needs to be instituted to support effective unclassified information sharing to end the redundant efforts within the agencies and to maximize the investment in SCRM programs. We touch on this a lot in the report. The classified community has been talking about this, but they're barely scratching the service, and a lot of the solutions and the people that are needed to execute the solutions don't have the tickets and the clearances needed to access the information.

Third question: what steps should the U.S. government and U.S. Congress take to address the emerging security and economic risks from next generation connectivity and technologies?

For this we have four steps, and again they are fully laid out in the report. The first is to embrace an adaptive SCRM process. Global commercial supply chains are constantly changing, as are our adversaries' methods. So should our security processes and procedures.

Two, promote supply chain transparency, and we heard about this this morning. Mapping, understanding who's in the sub-tiers. This would enable the federal government to source responsibly and securely and improve the government's ability to respond to cyber security incidents in the very likely event of a supply chain attack.

Third, centralize the federal IT supply chain risk management efforts. The government right now, as I mentioned, lacks a consistent, holistic supply chain risk management approach. The conflicting and confusing laws and regulations result in loopholes, duplication of effort, and inconsistently applied policies.

Last, craft and implement forward-looking policy. Future risks will include software, cloud-based infrastructures, hyper-converged products, not just the hardware that we're talking about right now.

A supplier's business alliances, investment sources, joint R&D efforts are all sources of risk that are not routinely evaluated in traditional procurement practices. Identifying these risks and addressing them creatively will be important to the success of all federal policy efforts.

While a national strategy is needed to protect--to provide strategic guidance, an impactful, tactical policy opportunity is to address the lack of supply chain risk management in the Management Act of 2017. The Act called for a $500 million fund for new technologies,

commercial technologies, with no requirements for the evaluation of the security implications of the commercial products and services being sourced.

In summary, the threat that China and other nation-states pose to the U.S. federal IT system via the supply chain is real, it's significant, and it's growing. Our reliance on China as a supplier will remain high. Meltdown and Spectre are engineering flaws that have already had a global impact and a global response. We cannot afford to identify an intentional "flaw" when our nation's economic or national security is on the line and fully dependent on the flawless operation of our IT systems.

The time has come to address the supply chain threat and not risk our nation's national security. The time is now, not after a major incident, the scale of which we may not yet have envisioned, is realized.

I thank you again for inviting me, for allowing me to go first on International Women's Day, and pleased to take your questions during the remaining time. Thank you.

PREPARED STATEMENT OF JENNIFER BISCEGLIE, PRESIDENT AND CEO, INTEROS SOLUTIONS

Testimony before the U.S.-China Economic and Security Review Commission
Hearing on "China, the United States, and Next Generation Connectivity"

March 8, 2018

Jennifer Bisceglie
CEO and President of Interos Solutions, Inc.

Chairman Cleveland, Vice Chairman Bartholomew and Commission Members, thank you for the invitation and opportunity to speak with you today on the concerns of technology coming from China.

By way of introduction, Interos is a company I founded 13- years ago to evaluate risks in the global economy and the business partnerships, alliances and distribution networks that comprise our supply chains. Interos is built on my over 25 years in the global supply chain industry, having helped numerous US-based companies off-shore their manufacturing and take advantage of different skillsets, labor pools and competitive business arrangements with partners around the world.

During those years, I've watched risk concerns in the supply chain transition and grow from quality, to physical security, to resiliency and now to include product integrity. Interos recently submitted a final draft report to this Commission on Supply Chain Vulnerabilities from China in the U.S. Federal Information and Communications Technology (ICT) [hereafter referred to as "the Report"] which outlines several recommendations, the most important being that the U.S. establish a "National Strategy for Supply Chain Risk Management in U.S. ICT" with supporting policies so that the Nation's security posture is forward-leaning vs reactive and based on incident response. Our adversaries have strategies they are executing; it's my opinion that is missing in the U.S. and providing easy opportunities for nefarious actors to drive up risk exposure and cost.

In being invited here, today, I was asked to address six (6) areas that are directly related to the Report. However, I would like to stress that whether it is 5G, blockchain, the Internet of Things (IoT), or any other emerging technology, an underlying foundation for security is an understanding of who the stakeholders are across your business partnerships, alliances and distribution eco-systems, where your vulnerabilities lie, and having a comprehensive strategy for security and risk management.

Given its position in the market, Interos has had the opportunity to work with many public and private sector organizations across industries and the situation is always the same – if the organization's leadership doesn't take a focused and comprehensive approach to risk management - there will be unmanaged exposure and invariably negative impact.

As a final note prior to addressing the questions within the Report, I would like to state that this testimony is an abbreviated perspective based on the Report under review by this Committee. I urge all Commissioners to review the Report once completed to get a more complete perspective and answers to these questions.

The rest of my testimony is organized as follows to respond to the questions asked:

- *A brief assessment of the emerging economic and national security risks from next generation connectivity and devices (particularly the IoT and 5G networks) for the U.S. with specific reference to*

the risks posed by China. What additional risks, if any, does use of IT, standards, and/or equipment developed in China pose to U.S. security? Are existing authorities and regulations adequate to address these challenges?

- *How reliant are the U.S. government and U.S. IT firms on Chinese firms and Chinese-made IT products and services?*

- *What are the potential vulnerabilities from U.S. usage of Chinese IT, standards, and/or equipment? How will the deployment of 5G and greater usage of IoT affect these vulnerabilities? How should the U.S. government ensure the development of a secure 5G network?*

- *How, if at all, has the Chinese government leveraged IT and IoT for the purposes of intelligence collection, censorship, or to launch or enable cyber-attacks? What are the implications for the integrity of U.S. government IT supply chains, for U.S. economic health, and for U.S. national security interests?*

- *Assess U.S. government's success in managing the risks associated with Chinese firms and Chinese-made products and services to its IT procurement supply chains. How is the U.S. government seeking to address mitigate its supply chain risks? How successful have those efforts been? What are the remaining challenges? Is existing legislation and regulations adequate to address these challenges?*

- *The Commission is mandated to make policy recommendations to Congress based on its hearings and other research. What steps should the U.S. government and U.S. Congress take to address the emerging security and economic risks vis-à-vis China from next generation connectivity and technologies?*

1. Briefly assess the emerging economic and national security risks from next generation connectivity and devices (particularly IoT and 5G networks) for the U.S. with specific reference to the risks posed by China.

Software supply chain attacks will become easier – and more prevalent - as developing technologies such as fifth generation (5G) mobile network technology and the IoT exponentially increase the avenues for attack.[1] Gartner predicts that by 2021 there will be 25.1 billion IoT units installed,[2] and by 2020, IOT technology will be in 90 percent of new computer-enabled product designs.[3] This growth in IoT connectivity will have a significant impact on the ICT SCRM challenge. Relevant to this Report, increasing IoT installations will expand the attack surface of federal ICT networks while decreasing the time required to breach them, yet to date, the time required to detect breaches is not decreasing. The

[1] The Internet of Things refers to a system of interrelated computing devices, mechanical and digital machines, objects, and living beings equipped with network connectivity that enables them to connect and exchange data.
[2] Peter Middleton, Tracy Tsai, Masatsune Yamaji, Anurag Gupta, Denise Rueb, "Forecast: Internet of Things — Endpoints and Associated Services, Worldwide, 2017," Gartner, Inc., December 21, 2017. https://www.gartner.com/doc/3840665/forecast-internet-things--endpoints.
[3] Benoit J. Lheureux, et al., "Predicts 2018: Expanding Internet of Things Scale Will Drive Project Failures and ROI Focus," Gartner, Inc., November 28, 2017. https://www.gartner.com/doc/3833669/predicts--expanding-internet-things.

responsibility of both the public and private sector in improving their approach to risk awareness and management in the commercial technology supply chain cannot be overstated.

The information technology (IT) supply chain threat to U.S. national security stems from products produced, manufactured, or assembled by entities that are owned, directed, or subsidized by national governments or entities known to pose a potential supply chain or intelligence threat to the U.S. , including China. These products could be modified to 1) perform below expectations or fail, 2) facilitate state or corporate espionage, or 3) otherwise compromise the confidentiality, integrity, or availability of a federal information technology system.

In the past, this concern was exemplified by counterfeit components entering the supply chain of U.S. defense systems, such as counterfeit integrated circuits from China discovered in the U.S. Navy's P-8A Poseidon airplane, in a U.S. Air Force cargo plane, and in assemblies intended for Special Operations helicopters.[4] In 2011, the Senate Armed Services Committee investigated 1,800 cases of counterfeit components which created vulnerabilities throughout the Department of Defense's supply chain, and reported that 70 percent of all counterfeits come from China, and a majority of the remaining counterfeits could be traced back through the supply chain to China. In these cases, recycled, obsolete, or modified components passed off as genuine circuits had potential to perform below expectations or fail, threatening U.S. national security and the safety of U.S. service members.

Increasingly, the importance of an ICT component's physical structure pales in comparison with the firmware and software operating within it. In 2016, researchers identified vulnerabilities that allowed hackers to surveil and manipulate users by hacking the embedded firmware of their computer monitors.[5] In 2017, researchers uncovered vulnerabilities in printers manufactured by Hewlett-Packard, Dell, and Lexmark that allowed attackers to steal passwords, shut down printers, and even reroute print jobs.[6] The mid-2017 CCleaner supply chain attack, in which hackers accessed the code development structure of Piriform in order to install malware into the company's Windows utility product, typifies the types of threats federal ICT systems will continue to face. Over 2.2 million users downloaded CCleaner and unwittingly installed the hacker's embedded malware at the same time. This malware compromised 40 international technology firms, 51 international banks, and at least 540 computers connected to various governments.[7] Firms targeted by the hackers included many within the federal ICT ecosystem, including Cisco, Google (Gmail), Microsoft, Intel, Samsung, Sony, HTC, VMware, Vodafone, Epson, and Oracle.[8]

---

[4] U.S. Senate Committee on Armed Services, "Senate Armed Services Committee Releases Report on Counterfeit Electronic Parts," Press Release, May 21, 2012. https://www.armed-services.senate.gov/press-releases/senate-armed-services-committee-releases-report-on-counterfeit-electronic-parts.

[5] Lorenzo Franceschi-Bicchierai, "Hackers Could Break Into Your Monitor To Spy on You and Manipulate Your Pixels," *Motherboard*, August 6, 2016. https://motherboard.vice.com/en_us/article/jpgdzb/hackers-could-break-into-your-monitor-to-spy-on-you-and-manipulate-your-pixels.

[6] Tom Spring, "Flaws Found In Popular Printer Models," *Threat Post*, January 31, 2017. https://threatpost.com/flaws-found-in-popular-printer-models/123488/.

[7] Lucian Constantin, "Researchers Link CCleaner Hack to Cyberespionage Group," *Motherboard*, September 21, 2017. https://motherboard.vice.com/en_us/article/7xkxba/researchers-link-ccleaner-hack-to-cyberespionage-group.

[8] India Ashok, "CCleaner Hack: Chinese Hacker Group Axiom May Have Carried out Attack to Target Major Tech Giants," *International Business Times*, September 21, 2017. http://www.ibtimes.co.uk/ccleaner-hack-chinese-hacker-group-axiom-may-have-carried-out-attack-target-major-tech-giants-1640208; Catalin Cimpanu, "Avast Publishes Full List of Companies Affected by CCleaner Second-Stage Malware," *Bleeping Computer*, September 25,

As information technology advances, and connectivity increases, these risks will multiply. Concepts such as the IoT, are but one avenue by which risk to federal IT systems will increase. The National Institute of Standards and Technology stated in Draft NISTIR 8200, released in February 2018, that "the adoption of IoT brings cybersecurity risks that pose a significant threat to the Nation."[9] Other aspects of supply chain risk depend on technologies that are not yet fully developed or deployed, such as fifth generation (5G) mobile network technology, which is expected to start deploying in 2020. The full deployment of 5G networks is expected to dramatically expand the number of connected devices, reduce network energy use, and decrease end-to-end round trip delay (latency[10]) to under one millisecond.[11] 5G is important for subsequent developments in virtual reality, artificial intelligence, and seamless integration of IoT.[12,13] Faster connectivity supplied by 5G networks will enhance productivity, efficiency, and facilitate greater interconnectedness through the IoT. But these benefits come with increased cybersecurity risks.

What additional risks, if any, does use of IT, standards, and/or equipment developed in China pose to U.S. security?

The Chinese government and Chinese firms are hoping for a larger stake in the new 5G developments than they had in 3G and 4G-LTE.[14] Key decisions on these standards will be made in international organizations such as the International Telecommunication Union (ITU) and the Third Generation Partnership Project (3GPP). The ITU is a specialized agency of the United Nations responsible for ICT issues; the 3GPP is a collaborative organization among telecommunications associations. In both arenas, China has sought leadership positions to increase its influence. In the 3GPP, China has been represented by members of Huawei and China Mobile. In October 2014, Houlin Zhao was elected secretary general of the ITU.[15] His four-year term began January 1, 2015 and concludes at the end of 2018.

Although the finalization of 5G standards may be years away, Chinese entities (specifically Huawei and ZTE) have made large strides in patenting ICT innovations, and China could emerge as an industry leader

---

2017. https://www.bleepingcomputer.com/news/security/avast-publishes-full-list-of-companies-affected-by-ccleaner-second-stage-malware/; Dan Goodin, "CCleaner Backdoor Infecting Millions Delivered Mystery Payload to 40 PCs," *Ars Technica*, September 25, 2017. https://arstechnica.com/information-technology/2017/09/ccleaner-backdoor-infecting-millions-delivered-mystery-payload-to-40-pcs/.

[9] National Institute of Standards and Technology, *Draft NISTIR 8200 Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)* (Gaithersburg, MD: Computer Security Division, February 2018). https://csrc.nist.gov/CSRC/media/Publications/nistir/8200/draft/documents/nistir8200-draft.pdf.

[10] Latency refers to the delay before a transfer of data begins following an instruction for its transfer. Decreasing latency to under one millisecond is seen as vital to successfully developing safe self-driving vehicles and producing virtual reality programs that can deliver data at a rate that feels near-instantaneous to humans.

[11] Jo Best, "The Race to 5G: Inside the Fight for the Future of Mobile as We Know It," *TechRepublic.* https://www.techrepublic.com/article/does-the-world-really-need-5g/.

[12] The Internet of Things refers to a system of interrelated computing devices, mechanical and digital machines, objects, and living beings equipped with network connectivity that enables them to connect and exchange data.

[13] Sebastian Moss, "ITU and Huawei Call for Government-backed Broadband Investment," *Data Center Dynamics*, October 7, 2016. http://www.datacenterdynamics.com/content-tracks/core-edge/itu-and-huawei-call-for-government-backed-broadband-investment/97066.fullarticle.

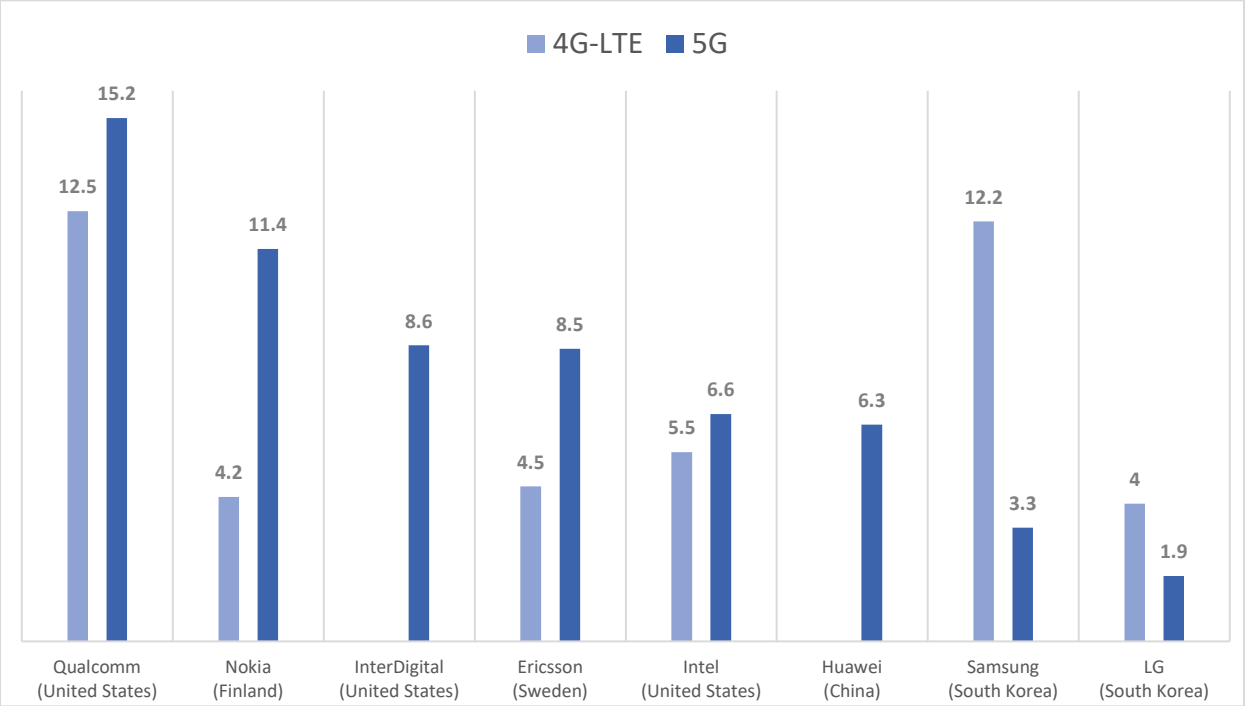
[14] 4G-LTE, or long-term evolution is a telecommunication standard for high-speed wireless communication for mobile devices and data terminals.

[15] "Biography—Houlin Zhao," International Telecommunication Union, 2017. http://www.itu.int/en/osg/Pages/biography-zhao.aspx; Xinhua, "China's Zhao Houlin Elected as Secretary-general of ITU," *China Daily USA*, October 23, 2014. http://usa.chinadaily.com.cn/world/2014-10/23/content_18791007.htm.

in this technology.[16] Of the 4,123 patents that ZTE applied for in 2016, more than 1,500 are 5G-related.[17] Huawei's 5G research dates to 2009 and includes advances in polar coding and network splicing routers. Huawei has also bought technology patents from Sharp, IBM, Siemens, Harris Corporation, and other U.S., Japanese, and European companies. These patent acquisitions focus on communication technologies such as the Session Initiation Protocol.[18]

A March 2017 report by LexInnova laid out the major players in the 5G network technology IP landscape.[19] **Exhibit 7** of the report shows the share of 4G-LTE and 5G IP among top firms. Qualcomm, Nokia, InterDigital, Ericsson, Intel, and Huawei are the top six firms for 5G IP. Qualcomm, Samsung, Intel, Ericsson, Nokia, and LG were the top six firms for 4G-LTE IP. Many of the top firms from 4G-LTE development remain competitive in the 5G sphere, with Qualcomm continuing to lead the group, and Nokia, Ericsson, and Intel increasing their share of relevant IP rights in 5G with respect to 4G-LTE. Although Samsung was a close second to Qualcomm in 4G-LTE innovation, it has fallen to 10th in 5G IP, according to the LexInnova data. LG has similarly struggled, losing influence in 5G innovation to its competitors. Newly important players include InterDigital (a nonparticipating U.S. entity that owns IP but does not produce products) and Huawei.

Exhibit 7: Percent Share 4G-LTE and 5G Wireless Network IP Rights by Firm



[16] Ben Sin, "How Huawei Is Leading 5G Development," *Forbes*, April 28, 2017. https://www.forbes.com/sites/bensin/2017/04/28/what-is-5g-and-whos-leading-the-way-in-development/#1d015f0e2691.
[17] Saleha Riaz, "ZTE, Huawei Top Patent Application Table in 2016," *Mobile World Live*, March 16, 2017. https://www.mobileworldlive.com/featured-content/top-three/zte-huawei-top-patent-application-table-in-2016/.
[18] Jack Ellis, "A Peek Inside Huawei's Shopping Basket Reveals How Patent Purchases Further Its Expansion Plans," IAM, May 7, 2015, http://www.iam-media.com/Blog/Detail.aspx?g=0351e5a1-3675-43a9-a552-7c8206af6be3.
[19] LexInnova, "5G Mobile Network Technology: Patent Landscape Analysis," March 15, 2017. http://www.lex-innova.com/resources-Reports/?id=67.

Sources: LexInnova, iRunway, Jefferies.

According to the LexInnova data, Huawei may control as much as 6.3 percent of critical 5G mobile network technology IP, a shift from its lack of influence in 4G-LTE. All Chinese entities together (including contributions from Huawei, ZTE, the China Academy of Telecommunications Technology, Zhejiang University, and Lenovo Group) control 9.8 percent of the IP LexInnova deemed critical to the 5G standard. Chinese firms have the largest presence in the Radio Front End/Radio Access Network category, where Huawei has 41 patents, China Academy of Telecommunications Technology has 14, ZTE has 11, and Zhejiang University has 10. In the area of Modulation/Waveforms, Huawei has 27 patents, while Lenovo Group has 7. In the area of Core Packet Networking Technologies, Huawei has 24 patents and ZTE has 8. However, Chinese entities still lag behind ICT powerhouses such as Ericsson, Qualcomm, and Nokia, which represent the bulk of 5G-related patent holders.[20] The LexInnova report notes that the presence of Chinese entities among the top IP assignees may indicate that China's 5G deployment timeline is similar to that of the U.S. .

Are existing authorities and regulations adequate to address these challenges?

In short, the answer is 'no'. An example is the recently implemented Modernizing Government Technology Act (MGT Act), introduced by U.S. Representative Will Hurd (R-TX), chairman of the House Information Technology Subcommittee, in September 2016. The Act creates a $500 million central modernization fund against which agencies can borrow to update aging IT systems. The Act also creates working IT capital funds that allow agencies to retain savings achieved from ongoing modernization efforts, provided they are used for future modernization projects. The Bill was amended to the Senate version of the FY18 National Defense Authorization Act, which was passed by Congress in November 2017 and signed into law on December 12, 2017.

The MGT Act seems to presume that legacy equipment and systems are the primary source of risk, and that this risk can be mitigated through modernization. But modernization will increase risk if newly adopted technologies, which have stronger supply chain connections to China, are not assessed appropriately before being integrated into federal IT networks. The Bill establishes responsibilities and provides financial rewards to agencies for modernizing their IT infrastructure, naming OMB and GSA as permanent members of a supervisory board. However, it does not require any measure of supply chain security as part of modernization efforts. In the 'Implementation of the Modernizing Government Technology Act' signed by Director Mick Mulvaney on February 27, 2018, there are multiple pages of guidelines for the execution of the program, but no requirement for supply chain risk management (SCRM) as part of an Agency's modernization effort.

An understanding of emerging technologies, their pedigree, and their interconnectivity is crucial to proactively identify and mitigate future supply chain risk to federal ICT systems. The Chinese government and Chinese companies have developed joint strategies to influence future developments to the advantage of Chinese ICT products. China's role in setting international technology standards is likely to increase, and similar strategies are likely to be used in the future in fields beyond ICT, such as pharmaceuticals, biotechnology, medical technology, nanotechnology, virtual reality, and artificial intelligence. Until U.S. leadership takes this vulnerability seriously, it will remain an 'easy button' for our adversaries.

[20] Guy Daniels, "If You Thought Patents Got Ugly with LTE, Just Wait until 5G," *Telecom TV.* http://www.telecomtv.com/articles/5g/if-you-thought-patents-got-ugly-with-lte-just-wait-until-5g-13458/.

2. How reliant are the U.S. government and U.S. IT firms on Chinese firms and Chinese-made IT products and services?

Over 95 percent of all electronics components and IT systems supporting U.S. federal IT networks are commercial off-the-shelf (COTS) products, and China's role in this global supply network is significant. The supply chain for civilian IT is a global enterprise dominated by suppliers in East Asia.[21] In addition to Chinese firms, many companies headquartered in Taiwan and Singapore base their manufacturing operations primarily in China. China assembles most of the world's consumer and commercial electronic devices, produces parts such as flash cards, and dominates the world in volume of IT industrial capacity. A recent report from the Government Accountability Office (GAO) noted that China is the largest importer and exporter of IT hardware globally, as well as a key manufacturing location of workstations, notebook computers, routers and switches, fiber optic cabling, and printers.[22]

Many of the top enterprise IT providers to the U.S. government are also among the largest manufacturers of federal ICT equipment, including leading providers of COTS products, such as Hewlett-Packard, IBM, Dell, Cisco, Unisys, Microsoft, and Intel.[23] Their supply chain is potentially influenced by China due to the fact that many of the companies and/or their sub-tier suppliers have manufacturing locations there.

3. What are the potential vulnerabilities from U.S. usage of Chinese IT, standards, and/or equipment?

The Chinese government considers the ICT a "strategic sector" in which it has invested significant state capital and influence on behalf of state-owned ICT enterprises. Since 2013, China has accelerated its efforts at indigenous production and independence in ways that have created a more restrictive environment for companies doing business in China, extracting concessions from large multinationals in exchange for market access.

New policies requiring companies to surrender source code, store data on servers based in China, invest in Chinese companies, and permit the Chinese government to conduct security audits on its products open federal ICT providers—and the federal ICT networks they supply—to Chinese cyberespionage efforts. China also continues to directly target U.S. government contractors and other private sector entities as part of its efforts to gain economic advantage and pursue other state goals.

Specific risks include intellectual property theft, theft of Personally Identifiable Information of U.S. citizens that can be used for financial gains, and the insertion of counterfeit products and services meant to create disruption and do harm.

---

[21] Danny Lam and David Jimenez, "US' IT Supply Chain Vulnerable to Chinese, Russian Threats," *The Hill*, July 9, 2017. http://thehill.com/blogs/pundits-blog/technology/341177-us-it-supply-chain-vulnerable-to-chinese-russian-threats.

[22] U.S. Government Accountability Office, "State Department Telecommunications: Information on Vendors and Cyber-Threat Nations," *GAO-17-688R State Department Telecommunications*, July 27, 2017. https://www.gao.gov/assets/690/686197.pdf.

[23] "Top 25 Enterprise IT Providers to Government," *FedScoop*, August 30, 2017. https://www.fedscoop.com/federal-it-top-25/federal-it-top-25-full-list/.

The use of Chinese standards further complicates any security strategy the U.S. may have in place as it provides a documented path of access for our adversaries.

How will the deployment of 5G and greater usage of IoT affect these vulnerabilities?

These new emerging technologies are just two (2) more examples that need to be proactively evaluated through a security lens as part of a national supply chain risk mitigation strategy. These, and other emerging technologies will expand the attack surface and increase the potential vectors for opportunists.

4. **How, if at all, has the Chinese government leveraged IT and IoT for the purposes of intelligence collection, censorship, or to launch or enable cyberattacks? What are the implications for the integrity of U.S. government IT supply chains, for U.S. economic health, and for U.S. national security interests?**

There are multiple documented examples of the Chinese government leveraging IT for intelligence collection and economic and state espionage efforts. One of the most infamous is probably the breach of Office of Personnel Management's database in 2015, a mammoth break-in that exposed the records of more than 22 million current and former federal employees.

In 2014 and 2015, the Chinese government ramped up implementation of laws and policies that raise market access concerns among ICT manufacturers and suppliers in the U.S. by threatening to decrease competition, favor Chinese firms over foreign firms, or extract concessions from multinational firms seeking to do business in China. These new regulations present a serious dilemma for U.S. multinationals and a threat to U.S. national security. If U.S. multinationals fail to adhere to Chinese government regulations, they may face restricted market access in China, which could decrease their revenues and global competitiveness. But if U.S. companies—which are the primary providers of ICT to the U.S. federal government—surrender source code, proprietary business information, and security information to the Chinese government, they further open themselves and federal ICT networks to Chinese cyberespionage efforts.

Bottom line, we need our full defenses up at all times to thwart enemy attacks.

5. **Assess the U.S. government's success in managing the risks associated with Chinese firms and Chinese-made products and services to its IT procurement supply chains. How is the U.S. government seeking to address mitigate its supply chain risks?**

A challenge facing federal SCRM efforts is that federal government laws and policies do not address risk management comprehensively. Rather, supply chain risks to federal ICT systems has been divided in multiple ways— among federal information systems and other initiatives designed to protect critical infrastructure or high-value assets and among national security systems (NSS) as a subset of federal information systems

How successful have those efforts been? What are the remaining challenges?

In some instances, very impactful. Interos supports one federal agency where over 75% of the supply chain risk assessments conducted in the past three (3) years have identified concerns that altered

acquisition decisions or influenced market analysis. That said, this mature program is in the minority when compared to those of other agencies where such programs exist. Not to mention, there are agencies that have not been resourced to implement a SCRM program at all.

In the current supply chain risk ecosystem, responsibility for risk management is held at different levels within agencies, resulting in offices and lines of effort in several agencies that function largely as under-resourced stovepipes, often lack executive sponsorship or oversight, and cater to the needs and procurement policies of individual clients. The DoD and the intelligence community maintain largely separate policies, many of which are not transparent to or applicable to the broader federal government due to procurement practices and classification concerns, among other reasons.

Is existing legislation and regulations adequate to address these challenges?

In short, no. There is little to no priority placed on SCRM, minimal leadership taking charge and limited accountability. I do not know what it will take to get this level of attention or how many other incidents need to occur before Congress or the Executive Branch gets more involved, but I see this as a major flaw in U.S. national security. At the same time, I would like to commend the agencies that have taken their own initiative to set up programs for internal security reasons – they are making a difference, but unfortunately these models are not scalable or shareable in their current form.

6. **The Commission is mandated to make policy recommendations to Congress based on its hearings and other research. What steps should the U.S. government and U.S. Congress take to address the emerging security and economic risks vis-à-vis China from next generation connectivity and technologies?**

As previously mentioned, I have expounded on this specific point in the Report to the Commission. Federal ICT supply chain risks can be best managed by focusing on four (4) areas: 1) embracing an adaptive SCRM process, 2) promoting supply chain transparency, 3) centralizing federal ICT SCRM efforts, and 4) crafting forward-looking policies.

This concludes my testimony. I thank the Commission and I would be pleased to answer your questions.

OPENING STATEMENT OF ANTHONY FERRANTE, SENIOR MANAGING DIRECTOR, FTI CONSULTING

MR. FERRANTE: Thank you.

Chairman Cleveland, Vice Chairman Bartholomew, and commissioners, thank you very much for the opportunity to testify before you today.

I'm glad that the Commission has taken an interest in this topic, as it directly impacts the United States--our business interests, our citizens and the safety of our nation overall.

For 14 years, I served as an adjunct professor, teaching computer science and cybersecurity to undergraduate and graduate students. I began each semester with the same challenge: name one aspect of your life that does not rely on a digital network. In an effort to outsmart the professor, the students would often pose creative answers that at first seemed, quote, "off the grid."

But further discussion would reveal that every suggestion ultimately relied on digital networks in some way. In each of these discussions, I was reminded of how much technological innovation has changed the world we live in.

Today, digital and mobile devices are available to broad populations at cheap prices. And these devices need the Internet. We call this the Internet of Things. In this room the average person owns and operates at least four devices that connect to the Internet--your cell phone, maybe a smart watch, a laptop, for starters. The temperature in this room may even be controlled by a computer network.

Last fall, as Hurricane Irma swept through Florida, those who had to evacuate were left agonizing over the impacts of their homes and property. All those except anyone who had a Tesla sitting at home in their garage. My friend, and Tesla owner, told me that he regularly connected to his Tesla from his smartphone to check for the presence of water damage, for the presence of water and damage to his home, learning in real-time that his home had escaped largely undamaged.

Our devices bring convenience, efficiency, and even peace of mind to our daily lives. And these efficiencies are equally realized by industry.

For example, companies with infrastructure or equipment that requires monitoring or maintenance can use sensors across their equipment to track and test every component, to anticipate when maintenance is needed or if the equipment is malfunctioning. In the pipeline industry, hundreds of thousands of miles of pipelines line the country, which present a maintenance and observation challenge.

In this industry, embedded IoT sensor technology enables the collection of operational data from critical points across the operating environment, minimizing risk to the system and reducing personnel and equipment costs. This is just one example of predictive technology that can provide real benefits and cost savings to companies.

The success of our interconnected world depends on the scope and speed of the networks that power these IoT devices. 2G networks were designed for voice, 3G networks were designed for voice and data, 4G networks were designed for broadband Internet experiences. Now 5G networks are being developed to fuse computing capabilities with communications in real time.

5G networks matter because they have the power to run technologies of the future--streaming virtual reality, driverless cars, instantaneous downloads of movies, and billions of devices in constant communication sharing data every second.

To quote one of my favorite senators on Capitol Hill, Angus King, when discussing this topic: "This is awesome."

[Laughter.]

MR. FERRANTE: But the awesome power of these advanced networks brings inherent risk.

The increased interconnectivity and data sharing creates vulnerabilities for our society, as cyber threat actors can use the expanding capacity of 5G networks to increase the power of their malicious attacks.

Nation states like China, Russia, Iran and North Korea are becoming increasingly advanced in their abilities to engage in malicious cyber activity.

And you don't need to be a sophisticated, state-sponsored hacker to have a big impact. This was made clear in October 2016 when malware written by three Minecraft-playing college students shut down many of the Internet's biggest websites across Europe and North America, sites like Amazon, Twitter, and CNN.

A company called Dyn, an Internet domain name provider, experienced a distributed denial of service attack that exploited the weak security of IoT devices to introduce malware called Mirai. Harnessing the power of these devices to attack Dyn, the malware essentially, and I quote, "turned off the Internet" that day.

But malicious use of these networks is not the only way that risk is introduced into our society. China has publicly declared its intention to become a global leader in the development and deployment of 5G and is making huge industry investments.

News reports indicate that China has set the course for industry dominance by funding research and development, working on the development of standards, and establishing their footprint in developing countries for deploying 5G services.

The United States government is showing signs that it recognizes the need for action and collaboration when it comes to cybersecurity more generally.

In May of 2017, President Donald Trump issued an Executive Order that called for the Departments of Commerce and Homeland Security to identify and promote action to reduce cyber threats. A report on their findings is due to be published in May.

But it's clear that when it comes to policy choices that address the challenges associated with IoT and 5G, the United States still has some decisions to make.

Though any specific national security concern held by the United States remains classified, at a Senate hearing last month, FBI Director Chris Wray expressed clear concern with losing control of our telecommunications infrastructure to a foreign power. All six United States intelligence officials appearing at this hearing expressed concerns related to American use of telecommunications services headquartered in potentially adversarial countries.

So what should the United States do? We all know that the world needs secure and sustainable 5G ecosystem that will support continued innovation across all sectors.

Historically, network expansion has been a largely commercial endeavor. But given the increasing threats and dependence on interconnected technology, the United States has some serious decisions to make on its involvement in the 5G platform.

The threats I've discussed today represent a global problem, and the United States can play an active leadership role. For example, the United States can increase its involvement in 5G standards development and increase its regulation of its own supply chain.

The United States should also recognize more clearly the role that backbone Internet service providers play in ensuring the safety of the Internet and do all they can to promote and incentivize behavior that increases the security and privacy of the end user.

Lastly, the United States must recognize that meeting these challenges demands a strong cybersecurity workforce and strategic decisions on this topic must be made to position our nation for long-term success.

Thank you for the opportunity to discuss these issues before you today and I look forward to answering any questions you may have.

PREPARED STATEMENT OF ANTHONY FERRANTE, SENIOR MANAGING DIRECTOR, FTI CONSULTING

Prepared Statement of
Anthony J. Ferrante
Senior Managing Director and Global Head of Cybersecurity
FTI Consulting
Before
The U.S.-China Economic and Security Review Commission

Hearing on China, the United States, and Next Generation Connectivity

Thursday, March 8, 2018
2255 Rayburn House Office Building
Washington, DC 20515

Chairman Cleveland, Vice Chairman Bartholomew, and Commissioners, thank you very much for the opportunity to testify today on a very important issue.

My name is Anthony J. Ferrante, and I am a Senior Managing Director and the Global Head of Cybersecurity at FTI Consulting, a global advisory firm. I focus on cybersecurity resilience, prevention, response, remediation, and recovery services. Over the last 15 years, I have provided incident response and preparedness planning to more than 1,000 private sector and government organizations, including over 175 Fortune 500 companies and 70 Fortune 100 companies.

Before joining FTI, I served as Director for Cyber Incident Response for the United States National Security Council at the White House, where I regularly coordinated responses to domestic and international cybersecurity incidents. I also led the development and implementation of Presidential Policy Directive 41, the United States government's key policy guiding cyber incident response efforts. Before joining the National Security Council, I spent several years in the Federal Bureau of Investigation's (FBI) Cyber Division. I was on the FBI's Cyber Action Team, which deploys around the world to respond to the most critical cyber incidents on behalf of the United States government, and I eventually became Chief of Staff of the FBI's Cyber Division. I also served as an Adjunct Professor of Computer Science at my alma mater, Fordham University, where I founded the International Conference on Cyber Security in 2007.

I'm extremely pleased that the Commission has taken an interest in such a crucial area for both the future of United States businesses and citizens as well as the safety of our nation overall.

Today, I want to talk about the significant wave of innovation that has overtaken the world in the last few decades, both the benefits and risks associated with new technologies, and what businesses and governments are doing to respond to these risks. In closing, I would like to share a few recommendations in terms of how we can be doing more to safeguard our society.

The Global Race to Innovate

In today's tech-driven society, countries recognize the key to economic well-being and overall security is their ability to innovate. Successful businesses are keenly aware of this fact, and governments are focused on creating advantageous environments where companies are incentivized to invest in technology. In addition to domestic growth, companies are encouraged to invest abroad through joint ventures and acquisitions in order to gain access to new market share and critical technologies.

Without a doubt, the focus on technological innovation has been wildly successful. As a result, high-quality devices have become available to broader populations at cheaper prices. Cell phones are a perfect example. In 2002, a little over half of adults had cell phones - today, 95% of adults have them.[1] It's crucial to remember that these devices, and the many others that now power our daily lives, require Internet connectivity. Today's refrigerators, cars, and even buildings are connected to the Internet. It's estimated that more than 200 billion Internet-connected devices will be in use around the world by 2020.[2]

In order for these devices to communicate effectively, networks are continually growing in scope and speed to support this unprecedented level of connectivity. A look back at past generation networks shows the massive leaps we've made in order to support our increasingly tech-driven world. 2G networks were designed for voice, 3G networks were designed for voice and data, 4G networks were designed for broadband Internet experiences, and now 5G networks are being developed to fuse computing capabilities with communications in real time.[3] The speed at which these improvements have occurred is staggering. Already, companies and countries alike are exploring the implementation of advanced 5G networks.[4] There's no reason to think that this breakneck pace will slow, and before long we will be talking about 6G, 10G, or even later generation networks. These networks will support a fundamental platform for new services and applications in tomorrow's economy, such as public safety, intelligence transportation, smart grid management, and mobile applications – all of which are integral to our national security and economic prosperity. This ever-increasing level of connectivity, often referred to as the Internet of Things (IoT), is the future, and the benefits are felt across the board.

The Benefits of IoT

IoT Strengthens our National Defense: Our forces' command centers traditionally relied on troops on the ground and aerial intelligence to communicate pertinent details on areas of operation. With new IoT technology, command centers collect data from devices, sensors, and cameras—mounted on unmanned vehicles, like drones, manned vehicles, soldiers, and

[1] http://www.pewInternet.org/fact-sheet/mobile/
[2] https://www.intel.com/content/dam/www/public/us/en/images/iot/guide-to-iot-infographic.png
[3] https://qz.com/179980/the-plans-for-5g-to-power-the-Internet-of-things/
[4] http://www2.itif.org/2016-5g-next-generation.pdf

weaponry— enabling them to develop comprehensive battlefield situational awareness in real time.[5] Such intelligence helps our forces achieve objectives and minimize casualties.

IoT Unlocks Efficiencies for Businesses: When running large infrastructures or equipment, such as oil rigs, a malfunction or mishap can cost companies millions of dollars. To prevent this, oil companies closely monitor each small component of their rigs, doing their best to anticipate when maintenance is needed or if a part needs to be replaced. IoT technologies can now link information on these machine components to companies' repair departments and supply chains. Then, when a part is not working or appears to be failing, the appropriate personnel are notified, and they can carry out the necessary repairs. This predictive maintenance technology can save companies on personnel costs and minimize the risks of machine failure.[6]

IoT Brings Convenience to Consumers: Let's take a look at smart home technology. Currently, I can turn on the air conditioning system in my apartment with a simple voice command or with my smart phone, and our networks have the capability to support these interconnected devices. While these technologies have made our day-to-day lives easier, technological innovation is only going to take things a step further. Imagine driving home from work on a very hot summer day, and you have on a wearable device that recognizes your body temperature and sends the data to your phone—this is happening today. Once you reach a certain point in your commute, your phone recognizes your location and automatically sends a signal to your air conditioning system to power on. When you enter your home or apartment, it's the perfect temperature, and you did not have to press a button, open an application, anything.

The Risks Associated with IoT and 5G

While governments, businesses, and consumers are reaping the benefits of IoT technologies—particularly the significant amounts of data that enable the development of new technologies—increased interconnectivity, coupled with faster, more powerful networks, creates new vulnerabilities. Today, the biggest global cybersecurity threat derives from IoT technologies. Governments, businesses, and consumers have eagerly incorporated these devices into their daily activities. But they usually do so without even baseline security measures, such as changing the factory setting passwords on these devices. Unfortunately, this lax, plug-and-play culture makes us far more susceptible to cyberattacks.

The best analogy I can think of is the example of automobiles in the United States. Automobiles are everywhere. Almost every household has at least one and businesses of all sizes utilize vehicles – we're talking anything from a small pizza shop using a single car for deliveries to distributors operating huge fleets. But the drivers in these vehicles all operate within relatively well-established "rules of the road." When people get in their cars, they know that the brakes need to be functioning or that seat belts need to be on; they know that they drive on the right

[5] http://www.windriver.com.cn/downloads/whitepaper/wind-river_IoT-in-Defense_white-paper.pdf
[6] http://www.digitalistmag.com/iot/2017/05/08/5-real-business-uses-of-internet-of-things-05072303

side of the road or need to use their blinkers when they shift lanes. It's not a perfect system, but it's also not total chaos.

But we can't say the same for the IoT technologies. The proliferation of these devices and the development of these complex networks has been so fast, and the devices so easy to use, that there has been no time to take a step back and establish foundational "rules of the road." People don't change the password default settings on their devices; they don't pay attention to the ways they are streaming data; they don't take care when storing personal or sensitive information on different devices. The same is true of businesses. And without those underlying "rules of the road," vulnerabilities start to open up which can and have been exploited.

With the current trend, this problem is only going to become more pronounced. Again, these networks are developing at a breakneck pace, as are the devices we are using on them. The longer we go without a culture shift that emphasizes safety and preparedness, for governments, businesses, and consumers alike, the harder it will be to instill order and maintain safe networks. We're already seeing the consequences with the level of exposure our networks have to attacks. And not only are we becoming more vulnerable to attacks, but the tools used by malicious actors are becoming more effective and widely available. By 2019, the cost of data breaches to companies will reach $2.1 trillion globally, increasing nearly four times the estimated cost in 2015.[7] To meet these threats, 85% of organizations are considering, exploring or implementing an IoT strategy.[8] But while awareness is growing, concrete steps to improve preparedness and response have lagged behind.

In order to accurately assess our risk vulnerability, it is important to know where the threats are coming from and in what form. Rogue actors are certainly something that we need to be mindful of. But nation-states—like China, Russia, Iran, and North Korea— are becoming increasingly advanced and sophisticated in their abilities to engage in malicious cyber activity. Most importantly, they have shown a willingness, and in many cases a preference, to use cyber aggression as a tool due to relatively low operational costs and the ability to deny affiliation. As a result, the line between criminal and nation-state activity is becoming increasingly blurred.[9]

Types of Attacks - DDoS

Before delving into some contemporary examples, I wanted to touch very briefly on "distributed denial of service" (DDoS) attacks. Because of their simplicity and function, this specific type of attack provides a great example of how the addition of many IoT devices and stronger networks will increase the scope and scale of cyberattacks we face. With DDoS attacks, hackers use groups of Internet-connected devices, known as botnets, to overwhelm servers,

[7] https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion
[8] https://www.business.att.com/cybersecurity/archives/v2/iot/
[9] https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf

websites, and networks. Essentially, the devices are used to spam networks with so much traffic that they shut down.

These DDoS attacks are the blunt tools of cyberattacks – they don't attempt to infiltrate or steal data and sensitive information. Instead, they use brute force to disrupt whole portions of networks. Nevertheless, these can be incredibly disruptive attacks. Some have shut down websites or smaller servers used by banks or other critical businesses. Others have been so large that they've crippled entire networks. Crucially, DDoS attacks utilize the insecure and unprotected devices in the IoT to carry out these attacks. Thus, electronic devices that have become part of our everyday lives can be coopted and used for nefarious purposes by malicious actors. Ultimately, more unsecured devices coming online will result in larger, more expansive botnets, and powerful networks—whether it be 5G now, or 8G five years from now—which will create additional, and faster, avenues for hackers to exploit.

Rogue Actors

Cyberattacks from rogue actors pose a serious threat and can have major implications for millions of unsuspected individuals. Take, for example, a cyberattack in October 2016, where hackers targeted a domain provider company, Dyn, and subsequently disrupted a broad array of the Internet's biggest websites, such as Twitter, Netflix, Reddit, and CNN. This DDoS attack exploited the weak security of devices in the IoT to introduce malicious software called Mirai. These devices were only protected by factory default, out-of-the-box security measures and were thus easily accessed and corrupted by the software. The software exploited these "soft targets," which are designed so owners can simply plug in and use them immediately. Again, many people don't even consider applying security updates or advanced settings. Their top priority is simply using the new device.

While the identity of the perpetrators of this particular attack has still not been confirmed, it's believed that it was not the work of a nation-state sponsored group, as multiple hacktivist groups claimed responsibility for the attack. One article even alleged that the attack was perpetrated by a "single very angry gamer."[10] Regardless, the Dyn attack highlights our vulnerabilities and the scope of the threats we need to be prepared for. The malicious software preyed upon everyday devices that are a part of the IoT. And the source code for the software, the actual tool itself that the attackers used, had been made publicly available on the Internet just a few weeks prior to the attack.[11] Even more troubling is the fact that our vulnerabilities are expanding at a rapid pace. As 5G and later generation networks come online and as the IoT grows, it is likely that the overall frequency of attacks, and the intensity of individual attacks themselves, will only increase.

[10] https://www.forbes.com/sites/leemathews/2016/11/17/angry-gamer-blamed-for-most-devastating-ddos-of-2016/#8bb93a42dac6

[11] https://www.eyerys.com/articles/timeline/ddos-dyndns-Internet-breaks#event-a-href-articles-timeline-facebook-and-billion-userfacebook-and-a-billion-user-a

Nation-States

Perhaps the greatest cyber threat comes from organized actors, often "countries of concern" that seek to gain access to sensitive information about the United States and its citizens. For example, in September 2012, massive DDoS attacks were carried out against dozens of large banks, including Bank of America, JPMorgan Chase, Wells Fargo, US Bank and PNC Bank, shutting down their websites for extended periods of time.[12] At the time, the volume of traffic was 10-20 times the volume seen in standard DDoS attacks. Numerous groups claimed responsibility, but it was ultimately determined that Iran had sponsored the attacks.[13] And last year, a grand jury in New York indicted seven Iranian individuals—who were employed by two Iran-based companies, ITSecTeam and Mersad Company, both of which were sponsored by Iran's Islamic Revolutionary Guard Corps—for carrying out the largescale DDoS attack.[14]

The event illustrated the ease with which nation-states can use their resources to conduct large-scale attacks against the United States. Despite the fact that the United States was spending $3 billion on cyber defenses at the time, $2 billion more than Iran, we were unable to defend ourselves from the attack, thus crippling our financial services industry. Experts have indicated that the attack marked a shift in Iran's cyber policy which emphasizes offensive capabilities and exploits the myriad of vulnerable targets available in the United States.[15]

In another example, in February of 2014 employees of a subsidiary of Anthem, the health insurance giant, received phishing emails. These are designed to appear as normal emails, but instead give malicious actors access to company networks. [16] One unknowing employee opened the email, giving a hacker remote access to the computer. This allowed the hacker to gain access to Anthem's core systems. The hacker then continued to operate within the system for approximately a year, exploring ways to retrieve sensitive information.[17] Ultimately, in February 2015, Anthem announced that the information of 78.8 million individuals (both customers and employees) had been compromised in a large-scale cyber incident.[18]

Though unconfirmed, the hackers are believed to be a part of China's military cyber-espionage division.[19] Experts suggest that the evidence, such as IP addresses and email accounts, indicate that China was behind the attack.[20] This is a perfect example of how nation-states can use to tip the balance in their favor. For the low price of outfitting a small cyber strike force, China gained access to the healthcare information of millions of Americans. This information could give a

[12] http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/index.html
[13] https://www.cnn.com/2012/10/15/world/iran-cyber/index.html
[14] https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged
[15] https://www.wsj.com/articles/SB10000872396390444657804578052931555576700
[16] https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/
[17] https://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627
[18] http://www.insurance.ca.gov/0400-news/0100-press-releases/2017/release001-17.cfm
[19] https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/
[20] https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/

competitive edge to China's biotechnology industry.[21] And this is just one incident. There are opportunities for nation-states to replicate such attacks across all American industries.

Response

How Businesses Are Responding

The scope of vulnerabilities and threats posed by these expanding networks has generally exceeded the ability and willingness of businesses to respond to them. The fact is that the combination of automation, machine learning, artificial intelligence, digitized supply chain management and communication technologies create massive vulnerabilities for all businesses. According to a recent study, cyber incidents are at an all-time high, with 86% of the companies surveyed saying they experienced at least one cyber incident.[22]

And it's not only the business operations that pose a threat – individual employees also present an opportunity for malicious actors to gain entry. For example, thousands of executives are targeted by cyber actors every day.

Unfortunately, the response to these threats has been weak. Businesses continue to operate with a large gap between their information technology (IT), security departments, and their core business functions. Failure to integrate cybersecurity into daily operations drastically reduces business' ability to defend and respond to cyber threats and incidents. Essentially, they are failing to both fortify their networks and to effectively manage breaches once they occur.

Further, an unwillingness to accurately report on cybersecurity status exacerbates the issue. There is often a habit of hush-hush management and underreporting of incidents across the board, from retail businesses, which store customer information, to utility companies that provide the power necessary for our nation to function on a daily basis. This opacity is a real problem because it conceals the ubiquitous nature of the threat we face. I don't think individual businesses or the public understand the scope of these vulnerabilities, and without that knowledge there is no impetus to develop the necessary defenses. We need to work towards a culture shift that incentivizes and rewards businesses to report breaches, communicate with each other, and coordinate responses.

How the Government is Responding

Thankfully, the United States government is showing signs that it recognizes the need for action and collaboration, as evidenced by today's hearing. And this recognition and subsequent discussions are already showing early signs of coercing the government to take action. For example, in the wake of several large cyberattacks, President Donald Trump issued an Executive

[21] https://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627

[22] https://www.prnewswire.com/news-releases/businesses-report-all-time-high-levels-of-fraud-cyber-and-security-incidents-during-2017-300585657.html

Order in May of 2017 calling for the Departments of Commerce and Homeland Security to identify and promote action to reduce cyber threats. Last month, Commerce and Homeland Security released a preliminary report, which included a series of goals to reduce the threat of automated, distributed cyberattacks and focused on the need for collaboration among stakeholders—including business executives, thought leaders, and elected officials—to combat new cyber threats.[23]

The Administration's FY19 Budget Request called for $80 billion in IT and cybersecurity funding ($45.8 billion for civilian agencies), representing a 5.2% increase from last year.[24]

The Administration is not alone in its efforts to mitigate these threats; Congress has increased government funding for cyber initiatives. Between 2007 and 2016, spending on unclassified programs to combat cyber threats rose from an estimated $7.5 billion to $28 billion.[25] In 2016 the Defense Department spent $18.5 billion in cyber-related efforts, nearly 30% above the prior year; Homeland Security spent $1.7 billion, a 9% increase; and Treasury spent $2.8 billion, a 42.7% increase.[26]

Such measures and funding are a good first step in guarding against the use of strategic legal investments. But we must also be vigilant in guarding against nation-state actors using illegal tactics to gain access to United States technologies and information.

Recommendations and Conclusion

1. We cannot operate in a bubble. The reality is cyber warfare and cyberattacks are not a United States problem, but rather a global one. With no existing "cyber norms," we have an opportunity to set the standards for 5G networks and IoT devices, where other nations will then follow suit. When it comes to cybersecurity, the adage "a chain is only as strong as its weakest link" certainly holds true. But the potential to begin a culture-shift in the approach to cybersecurity and the willingness to do so are two very different things. The United States government and businesses need to take concrete steps to lead by example and address cyber threats.

2. We need to help Internet service providers (ISPs) protect the end users – United States businesses, consumers, and the American people. ISPs are the first line of defense in both identifying and mitigating cyberattacks. If I were to use an analogy to describe ISPs, they would be the state troopers, with highways serving as the networks. In order for state troopers (ISPs) to guard against risky activities on highways (networks), they need proper resources. And, with highways getting even larger as a result of increased traffic

[23] https://www.ntia.doc.gov/files/ntia/publications/eo_13800_botnet_report_for_public_comment.pdf
[24] https://www.whitehouse.gov/wp-content/uploads/2018/02/FY19-Budget-Fact-Sheet_Modernizing-Government.pdf
[25] http://www.thefiscaltimes.com/2017/08/06/US-Spends-Billions-Cybersecurity-No-One-Sure-Exactly-How-Much
[26] http://www.thefiscaltimes.com/2017/08/06/US-Spends-Billions-Cybersecurity-No-One-Sure-Exactly-How-Much

(more IoT devices), we need to ensure state troopers have the necessary resources to prevent malicious actors from harming the end users.

3. We need to invest in cyber education. This is absolutely crucial. Of course, we need to ensure that the current everyday consumers recognize the vast risks associated with IoT devices and are armed with an understanding of how to contribute to overall security. But we also need to take the long view and invest in educating teenagers and young minds charged with developing our future software and technology. These generations are going to grow up with this technology, and given the pace of technological improvements we need to assume that their lives will be much more tech-centered than has been the case in the past. It is our responsibility to arm our younger generations with an understanding and appreciation for the potential threats an interconnected, IoT-driven world will present. An underlying culture shift in cybersecurity awareness must be fully integrated into future developments as new generations write code, invent new devices and improve network capabilities.

4. We need to educate the public about cyber threats. As I previously mentioned, individuals have greatly benefited from innovative new devices, many of which are connected to the Internet. While we should celebrate these advances, people must understand that these devices can serve as a pathway for uninvited cyber criminals to enter their homes. Beyond simply understanding that the threat is real, the government and industry leaders should continue to play an important role in educating the public about ways in which they can mitigate the risk of cyber attacks

OPENING STATEMENT OF JAMES MULVENON, PH.D., SPECIAL PROGRAMS DIVISION, SOS INTERNATIONAL LLC

HEARING CO-CHAIR WORTZEL: Jim.

DR. MULVENON: Chairman Wortzel, Chairman Wessel, other commissioners--Larry, that just, it still doesn't feel right. I can't do it. I can't do it.

[Laughter.]

HEARING CO-CHAIR WORTZEL: I know. I know. We ain't drinking it--

DR. MULVENON: Too many long nights at PLA conferences. So as you mentioned, my team of nearly two dozen cleared Chinese linguist analysts right now are actually completing a study for the Commission on Internet of Things, and so my testimony in part reflects some of the early findings of that but also my own personal prurient interest in the area for many years.

My three top concerns. First, the supply chain challenges and threats that have already been laid out posed by China-based production of IoT devices that are deployed in the United States, and here I would include devices produced by both U.S. and Chinese companies largely produced in China, but with a particular focus on the challenges posed by the Chinese companies.

And I'll come back to this. Less concern about mechanisms or plans for front-end inspection of hardware and software, which I, you know, which is the preferred Huawei model for how they're going to get the clean hardware and software into the network. I'm much more concerned about post-installation maintenance and upgrades, which if I was running the op would be the vector where I buy would insert the malware into the system.

And then finally some little noticed but I think very important articles in some of the new Chinese laws that have come out that I think not only reinforce the legal basis for the extraterritoriality of Chinese companies operating in the United States but also mandate intercept access of those Chinese telecoms operators and equipment suppliers to the Chinese security services globally. And I think that those are very telling.

Now, first looking at Internet of Things. To those upset about my testimony today, I would only say that my home is protected by a range of secure IoT devices, including perimeter door systems and cameras, and I also engage, of course, in sophisticated tracking of my teenage daughters' electronics, some of which they even know about.

But increasingly these devices which are being deployed, the first generations of those devices were largely built without security in mind and often are un-upgradable and the firmware can't be changed. And so we can't even contemplate strategies for some of these devices of retroactively securing them, and that's largely a consumer issue in terms of understanding default logins and passwords.

But increasingly these unprotected networks are being used for malignant purposes, as has been described, either as bonnets or frankly for use as unwanted surveillance.

And three of the largest companies in the space--Dahua, Hikvision, and Foscam--are in fact Chinese companies, and the production of their devices is global, and they are ubiquitous in the United States if you go to Best Buy and other places.

There has been a series of cyber incidents involving equipment by these Chinese companies. Hikvision DVRs have been used for large-scale bitcoin mining. The Dahua's cameras were integrally involved in the spreading of the Mirai worm that was mentioned earlier. Foscam was putting out cameras that had an embedded peer-to-peer network feature that was not

in any of its manuals and was sharing the data back with a Chinese company called ThroughTek, and the consumer had no idea that that was happening.

And Hikvision, a large number of their cameras are, in fact, deployed with--they're exploitable through the default login and password, and they've only recently changed that so that you have to actually change the password.

And as a result of this, Hikvision cameras have been removed from Fort Leonard Wood and the U.S. Embassy in Kabul, and the GSA has banned now Hikvision from its approved suppliers list.

5G, which has been mentioned earlier, is the advanced next generation telecommunications networking protocol that will enable all of these things plus self-driving cars, which based on my commute and today's testimony can't come soon enough, as well as immersive networking.

China is clearly one of the leaders because of its state-directed investment strategy in protocols, and this Commission has heard me testify previously about how China uses, the Chinese government uses information and communication technologies standards as a trade weapon and has invested billions of dollars to create competing standards.

They are clearly a leader in 5G development and are actively promoting the R&D and commercial activities of Huawei and ZTE's 5G, and really many people in the Tier 1 infrastructure at AT&T and Sprint and Verizon believe that 5G will be the final thin wedge that finally facilitates inclusion of Huawei equipment widely in the Tier 1 infrastructure in the United States.

However, I'm often mischaracterized as someone who is a sort of keep-Huawei-out-of-the-USA person. Huawei is already ubiquitous in two dozen Tier 3 telecoms providers in the United States so that barn door has long ago been slammed. The word "resilience" was used earlier.

I much prefer a strategy where we develop a resilient strategy knowing that it is inevitable that Huawei equipment and ZTE equipment is in the Tier 1 networks, and again not getting sucked into what in my view is the failed British telecom GCHQ model of relying on front-end inspection to the equipment and then finding out later that that lab is staffed entirely by Huawei employees, but instead one in which we continue to do life cycle monitoring of the equipment, much as I do all the equipment in my corporate network. I assume that I have compromised hardware and software inside my network at all times.

But I think two, two key points, though, that often I think get lost in the sort of keep Huawei out of the U.S. debate. First, you know, Huawei is a legitimate globally competitive $90 billion plus company. It is not a front company or a platform for Chinese intelligence.

If they were, based on pure market forces, to win a contract to supply 5G equipment in the United States, the more troubling part of the system for me is that as the largest privately owned company in China, but given the nature of the political and legal environment in China, they would not be able to refuse a request, a subsequent request, from the Chinese government for access to that network.

More recently, the National Security Law, the Counter-Espionage Law, the Counterterrorism Law, and the new Cybersecurity Laws that have been passed in China explicitly call out that Chinese telecom operators and Chinese equipment companies must provide unfettered access to their networks and equipment to the state security services without prior notification for intercept.

And so my question would be, if, in fact, there is a NOC or a SOC operating in Plano, Texas, is, in fact, that considered from an extraterritoriality perspective, even if it's Huawei USA, is that a scenario in which the Chinese security services using these laws, which they believe cover Chinese companies operating globally, as a mechanism by which they could then legally enter without prior notification and conduct intercept against networks being monitored by that Chinese company?

That I don't think has been sufficiently explored, and one only needs look at the rendition strategies that the Chinese government was using with respect to Guo Wengui, for instance, who carries a UAE passport but is clearly regarded by the Chinese government still as a Chinese citizen, to get a sense and flavor for this extraterritoriality perspective that the Chinese government holds.

Thank you.

PREPARED STATEMENT OF JAMES MULVENON, PH.D., SPECIAL PROGRAMS DIVISION, SOS INTERNATIONAL LLC

Statement before the
U.S.-China Economic and Security Review Commission
"China, the United States, and Next Generation Connectivity,"

A Testimony by:

James Mulvenon, Ph.D.
General Manager, Special Programs Division
SOS International

March 8, 2018

2255 Rayburn House Office Building

Introduction and Main Points

Chairman Cleveland, Vice Chairman Bartholomew, and Commissioners, thank you for inviting me to testify today.

My testimony focuses on the Internet of Things (IoT), 5th generation telecommunications (5G), and the role that these technologies could potentially play in national security and information security issues between the United States and China. The top three concerns are:

- Supply chain challenges and threats posed by China-based production of IoT devices deployed in the United States
- Post-installation maintenance and upgrades of those IoT devices as vectors for malware and exfiltration
- Recent Chinese laws that create the legal basis for extraterritoriality of Chinese telecommunications companies and potential intercept access to U.S. communications infrastructure.

Before dealing with these concerns, let me first address the general issues associated with IoT and 5G in a U.S.-China context.

Internet of Things

The so-called "Internet of Things," or IoT, has quickly become a ubiquitous part of our daily lives. Our homes are increasingly filled with WiFi-connected hubs, garage door openers, lights, doorbells, and security cameras. Unfortunately, information security was an afterthought with many of these devices, and many are not designed to be upgradeable. As a result, IoT objects are increasingly being used for malignant purposes, either as part of botnets[1] or for unwanted surveillance. The fact that many of these devices are being produced in China by foreign or Chinese firms only adds an additional layer of potential concern. For example, the three largest Chinese network camera firms (Dahua, Hikvision, Foscam) have been linked in the last two years to major cyber incidents, primarily because of the low levels of information security in their products:

- A researcher at the SANS Technology Institute identified malware designed to infect security camera recorders and routers and use the devices to attempt to mine Bitcoin virtual currency. The malware is designed to run on ARM infrastructure and was spotted on Hikvision DVRs, which have a simple default root password that users often do not change.[2]

[1] Brian Krebs, "Dahua, Hikvision IoT Devices Under Siege," *Krebs on Security*, March 2017, accessed at: https://krebsonsecurity.com/tag/hikvision/.
[2] Eduard Kovacs, "Cybercriminals Abuse Security Camera Recorders and Routers to Mine for Bitcoins," 2 April 2014, *Softpedia*.com, accessed at: http://news.softpedia.com/news/Cybercriminals-Abuse-Security-Camera- Recorders-and-Routers-to-Mine-for-Bitcoins-435427.shtml

- Network cameras manufactured by Chinese company Dahua (dahua.com) were main targets of the Mirai internet worm,[3] which "has been used in some of the largest and most disruptive distributed denial of service (DDoS) attacks" in the history of the Internet.[4]
- Many network cameras manufactured by Shenzhen-based Foscam (foscam.com) connect to a peer-to-peer network called the "Kalay Network" run by a Chinese company called ThroughTek, though there is almost no mention of this feature in Foscam manuals and it is very difficult to disable.[5] Moreover, information security experts such as Nicholas Weaver call the embedded P2P feature "an insanely bad idea" because "it opens up all Foscam users not only to attacks on their cameras themselves (which may be very sensitive), but an exploit of the camera also enables further intrusions into the home network."
- Large numbers of network cameras manufactured by Chinese company Hikvision were hacked in early 2017 by exploitation of default login and passwords,[6] though more recent Hikvision releases require the creation of a unique password.[7]

Other Chinese IoT companies have been scrutinized for their potential threat to U.S. national security. In May 2017, the Department of Homeland Security issued a cybersecurity warning saying some of Hikvision's cameras contained a loophole making them easily exploitable by hackers, assigning its worst security rating to that vulnerability.[8] It was later discovered that Hikvision cameras were deployed at Fort Leonard Wood in Missouri and the U.S. Embassy in Kabul, Afghanistan.[9] The cameras were later then removed for security concerns. The General Services Administration, which oversees $66 billion of procurement for the U.S. government, subsequently removed Hikvision from a list of automatically approved suppliers. On 30 January

---

[3] Brian Krebs, "Who Makes the IoT Things Under Attack?" *Krebs on Security*, October 2016, accessed at: https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/
[4] "Mirai (malware)," *Wikipedia.org*, accessed at: https://en.wikipedia.org/wiki/Mirai_(malware)
[5] Brian Krebs, "This is Why People Fear the 'Internet of Things'," *Krebs on Security*, February 2016, accessed at: https://krebsonsecurity.com/2016/02/this-is-why-people-fear-the-internet-of-things/
[6] Brian Karas, "Hikvision Defaulted Devices Getting Hacked," *IP Video Market* Info, 2 March 2017, accessed at: https://ipvm.com/reports/hik-default-hack
[7] "IP Cameras Default Passwords Directory," accessed at: https://ipvm.com/reports/ip-cameras-default-passwords-directory
[8] "Advisory (ICSA-17-124-01): Hikvision Cameras," Department of Homeland Security Industrial Control Systems Computer Emergency Response Team, accessed at: https://ics-cert.us-cert.gov/advisories/ICSA-17-124-01.
[9] Dan Strumpf, Natasha Khan, and Charles Rollet, "Surveillance Cameras Made by China Are Hanging All Over the U.S.," *Wall Street Journal*, 12 November 2017, accessed at: https://www.wsj.com/articles/surveillance-cameras-made-by-china-are-hanging-all-over-the-u-s-1510513949; and Dan Strumpf, Army Rips Out Chinese-Made Surveillance Cameras Overlooking U.S. Base," *Wall Street Journal*, 12 January 2018, accessed at: https://www.wsj.com/articles/army-rips-out-chinese-made-surveillance-cameras-overlooking-u-s-base-1515753001.

2018, the House of Representatives Committee on Small Business held a hearing on foreign cyber threats to small businesses, and singled out the threat posed by Hikvision cameras.[10]

5G Telecommunications

The next-generation mobile Internet, known as 5th generation or 5G, is the infrastructure upgrade necessary to facilitate billions of IoT devices communicating with each other, as well as emerging technologies like self-driving cars and immersive networking. 5G networks, now in the testing stage, will rely on denser arrays of small antennas and the cloud to offer data speeds up to 50 or 100 times faster than current 4G networks and serve as critical infrastructure for a range of industries.[11] China is widely regarded as one of the leaders in 5G development, allocating billions in state investment and actively promoting the R&D and commercial activities of Huawei and ZTE. Huawei has signed 25 agreements with telecommunications companies around the world to test its 5G technologies, and China Mobile in 2018 plans the world's largest 5G trial.[12] According to Chinese regulations, Huawei and ZTE are each guaranteed one-third of the Chinese 5G market, leaving foreign firms like Ericsson and Nokia to compete over the remaining one-third sliver.[13] The concerns about Huawei or ZTE 5G equipment in the United States telecommunications infrastructure are two-fold:

- If Huawei or ZTE were to win a contract to supply 5G equipment under market terms, the political and legal environment in China would prevent either company from refusing a subsequent entreaty from either the Chinese intelligence services or military for access to the technology or services.
- The PRC government treats Chinese companies operating abroad as subject to PRC law, and multiple new Chinese laws dictate that telecoms operators must provide the Chinese intelligence services with unfettered access to networks for intercept, which raises concerns about Huawei or ZTE 5G support facilities being used for intelligence operations.

At the same time, the barn door long ago slammed on a "keep Huawei out of the USA" strategy, as several dozen Tier 3 telecommunications providers, primarily in rural areas in the United States, already extensively use Huawei base stations and handsets. It is also likely inevitable that Huawei equipment will be eventually deployed in Tier 1 networks run by AT&T, Verizon, and

[10] "Small Business Information Sharing: Combating Foreign Cyber Threats," accessed at: https://smallbusiness.house.gov/calendar/eventsingle.aspx?EventID=400565
[11] Eric Auchard, Sijia Jiang, "China's Huawei Set to Lead Global Charge to 5G Networks," *Reuters*, 23 February 2018, accessed at: https://www.reuters.com/article/us-telecoms-5g-china/chinas-huawei-set-to-lead-global-charge-to-5g-networks-idUSKCN1G70MV.
[12] Arjun Kharpal, "China 'Has the Edge' in the War for 5G and the US and Europe Could Fall Behind," cnbc.com, 7 March 2018, accessed at: https://www.cnbc.com/2018/03/07/china-has-the-edge-in-the-war-for-5g-us-and-eu-could-fall-behind.html
[13] Eric Auchard, Sijia Jiang, "China's Huawei Set to Lead Global Charge to 5G Networks," *Reuters*, 23 February 2018, accessed at: https://www.reuters.com/article/us-telecoms-5g-china/chinas-huawei-set-to-lead-global-charge-to-5g-networks-idUSKCN1G70MV.

Sprint. It is imperative, therefore, to adopt a “resilience” strategy, designing a security framework that assumes the presence of Huawei equipment in U.S. networks. While this strategy should include independent review of hardware and software and supply chains, the results of the “front end” inspection must be tempered with the understanding that subsequent maintenance and upgrades of the equipment would be the more likely vector for insertion of malware and exfiltration of data. Thus, the security framework should cover the entire “life cycle” of the equipment and software.

PANEL II QUESTION AND ANSWER

HEARING CO-CHAIR WORTZEL: Thank you.

I want to use Ms. Bisceglie's discussion of a national strategy for supply chain risk management as kind of a point of departure for a little more broader discussion to address what Congress can do about supply chain security, if anything.

In 2017, a really good GAO report on the Department of Defense found significant deficiencies in military service policies and practices in operation security and mission security assessments across the services. So if we want--with separate policies and regulations at various echelons--so if we want policies and regulations or strategies out of the executive branch, you really could hope that somebody on the National Security Council would recognize the need and get a presidential directive or executive order out. But if you want to require it, it takes legislation.

So I would ask all of you if you have some idea of the forums of legislation that might help us with that, and then related to that is, if you could help us understand what you think critical infrastructure is and what requirements should be put on that? Might as well take the same order.

MS. BISCEGLIE: Well, thank you. And I think it's a great question. I will tell you that there's a lot of discussion about it at all different levels, and I think there's two things that are going on, in my opinion.

One is the concern about from a policy or from a legislative standpoint about getting too prescriptive.

HEARING CO-CHAIR WORTZEL: Uh-huh.

MS. BISCEGLIE: Where we can't actually operate, and I would call government operations a business, so we can't actually operate the business that the agencies are responsible for. So when we start looking at what we want legislatively, we can't be too prescriptive, and then you--but at the same time, it needs to ensure that everyone understands this is a priority. And I think that's really lacking.

And so if I would, you have, you have policy out there through Circular A-130. You have law that was put out by Congressman Wolf in 2013 that is only adhered to by three or four agencies, and the challenge with that is that it's open to interpretation and so--and none of it has ever been resourced.

And so if I were looking to legislate something, I would call it out so that it's a priority. I would make sure that before anything from a technology standpoint was funded--as I mentioned before, this whole Management Act. I was on the Hill multiple times talking to the entire committee under Congressmen Hurd and Connolly about you have an opportunity here to get security and supply chain risk concerns into a $500 million fund, and I understand the priority to get it done so I'm not saying anything against, you know, the congresspeople, but it was a huge miss.

And so I think besides making it a priority, making sure that folks understand before they are just given money to do additional things--you have the Management Act, you have FITARA, you have a whole bunch of things out there--is that a common understanding of what all of the agencies are being held to before they're actually given funding to buy new technology, to modernize existing technology.

And then the last thing is to make sure that these policies are resourced. There's so much focus on--I'm never going to get it right--you know, it's the whole thing about time, schedule,

making sure that everything is done on time and, you know, according to the schedule, and the money that's expected. But nothing really talks about security, and if it is, it's always called like a fourth dimension. And I have no idea in the world that we're talking about and that we're living in, the fact that we're so connected, why that's not part of the initial focus. So those three things.

Thank you.

MR. FERRANTE: So I would just add that I think it's important that the United States does take a comprehensive strategic approach to this issue, and most importantly I think it starts with understanding the risks, understanding the threats.

In my experience in government and in private industry, we have a lot more to learn, and I think at some of our most senior levels of government, fully appreciating the threats that we face, not only from nation state actors but criminal actors, and the impacts that those threats can have on our society is just not, not fully appreciated at the most senior levels of government.

Me personally I've worked thousands of cybersecurity incidents. I've worked with thousands of clients in private industry, and it always starts with sensitizing my audience to the effects of these threats. People do not fully appreciate it until it really affects them personally.

I remember working with an organization that had a massive breach, and every single piece of data that the organization owned had been stolen, all their intellectual property was stolen, and when I briefed the chairman of the firm, he took notes and nodded his head, and then I said, and, sir, please understand we believe that your home computer was targeted, and he sat right up and said "my home computer." He didn't care about his organization until it affected him.

And I think that's important as we continue to educate our leaders in government on this issue.

DR. MULVENON: Well, Larry, I'm going to once again go against type, which is to say perhaps there are things we can learn from China on this issue. China has a set of guidelines known as MLPS, the Multi-Level Protection Scheme, which was the mechanism by which they actually developed a five-tier category system of their own critical infrastructure and then determined which ones of those tiers, because we can't protect everything, and we have to prioritize, were such that they required that the equipment in those networks be only domestically procured through supply chain.

And, of course, there are national security exceptions under the WTO that allow any country to do that, to protect critical networks. And so using the ICS cert guidelines, using the NIST guidelines, I think it is possible for us to engage in that type of categorization so that we're not, you know, over--trying to scale this too large but actually identifying what really needs to be protected.

And on the other side, on the strategy side, I will say that I believe that the media portrayal of the White House's 5G initiative was a caricature of the actual initiative, and that it has great historical precedent in previous U.S. infrastructure challenges, and that the current lack of U.S. companies capable of building out the entire infrastructure lays out a nice rationale for why, in fact, it could be a national initiative.

And so I'm hoping that after the political dust has settled, we can relook that issue because I think there was a lot, really a lot of merit to it, and it was largely misunderstood.

HEARING CO-CHAIR WORTZEL: Thank you.

HEARING CO-CHAIR WESSEL: I'm up.

HEARING CO-CHAIR WORTZEL: You're up.

HEARING CO-CHAIR WESSEL: I got to seek permission though. Thank you.

And just to your last point, Jim, you know, the leak of that report had and I think was probably designed to have a chilling effect on any activity, and certainly we all understand the power and importance of the private sector in terms of technological development, the speed at which it can bring things to market, you know, creativity, et cetera, but there is a role for government in terms of assuring protection.

Mr. Ferrante and others who have had some experience with the private sector, you know, part of the problem here--and, you know, we're looking at, for example, the administration's effort to promote a 301 action on Chinese theft of intellectual property, coerced or forced technology transfers--is companies don't want to come forward and participate.

You know they are happy to have their trade associations bloody their nose while they hold the coats, as they say. But, you know, whether companies are worried about, number one, having to make the expenditures to truly have a secure system or have a secure system as they can because nothing is truly secure, whether they're worried about derivative shareholder suits for lack of adequate steps to protect the infrastructure, I'd be interested in, you know, all of your views on what we can do to try and have a more cooperative approach from private sector, understanding the legal exposures that exist.

And second, which is sort of the big question we're here with as well, and as evidenced by the NSC leak, you know, 5G is well underway, IoT is deployed, you know, well deployed. It's, you know, 5G is the enabling technology to allow and talk faster, et cetera, is the--I don't remember which one of you already said that the horse was out of the barn, or whatever the comment was--have we already lost the 5G IoT battle?

Mr. Ferrante, do you want to start?

MR. FERRANTE: Sure. So your first question hits close to home. Having been an FBI agent for 12 years and interfacing with thousands of victim companies, I struggled with that very same question. So I can fully appreciate the question.

And I will start with a very simple statement that I learned through my experiences that an entity, an organization, whether it be a person or a large corporation, when they experience a data breach, they are a victim, a victim of a crime, and they should be treated as such.

So we, as a government, have a difficult time fully appreciating that unless it affects us; right? Remember when our government knocks on the doors of private entities and advises them that they are a victim of a crime, the first thing that comes to mind is their reputation, their operation, internal communications, external communications.

I can't tell you how many times I've met with senior leaders in private industry and verbatim they said to me is this going to wind up on the cover of the New York Times?

And it was my job as a government employee, as an FBI agent, and I applaud the FBI and their cyber task forces in working diligently to protect the identities of those who have been the victim of a crime. That said I can fully appreciate the question because as long as these breaches continue to happen, and we do not have an open and honest dialogue about it, the less we're going to be able to do something about it.

Breaches are happening everyday. In private industry, my phone rings off the hook. Our clients call us. They have breaches large and small. In government, we had armies of people available to assist private organizations, and they were busy dealing with breaches.

The question is, is how do we create a culture and incentivize organizations to come forward, and if they do come forward, what assurances do we have that we're going to do everything we can to protect them because I assure you, and the breach in Equifax is a great

example, that when a breach occurs, this is no longer something that falls on low level staff members. This is going straight to the top to the CEO, the chairman, who may be held responsible for this.

So we need to find that balance in respecting victims' rights, but also bringing awareness to the issue because it is an issue, and it's not going to stop.

And candidly, I've forgotten your second question.

[Laughter.]

CHAIRMAN CLEVELAND: Me too.

HEARING CO-CHAIR WESSEL: Me too. Is the horse already out of the barn as it relates to 5G IoT in terms of sourcing, other issues? You know we talked earlier today about, you know, ITU, et cetera. I mean, you know, deployments are either starting for 5G or well-defined. Are we going to be able to put in place the protocols, the security measures, et cetera, to try and address this?

MR. FERRANTE: Yeah. I don't think it's ever too late. Yes, this technology is evolving very quickly. I mean just in the last five years the new devices that have come on line, it's incredible, and that's great. The technological advancements are great. And they're only going to become more advanced.

I talk to companies all the time about this, and I use a statistic I read in study that said the next 20 years we will be a million times more advanced. I wish I knew what that looked like; right? I think we all wish we knew what that looked like. The reality is, is that it's going to keep evolving, and it's okay. It's never too late, but we do need to act. I think the worst thing we can do is exactly what I said earlier what these companies do, is pretend it didn't happen. Pretend the breach didn't happen and just close our eyes and hope it goes away because it's not. So it's time to act, and I think we can do it. We just need a comprehensive strategy.

HEARING CO-CHAIR WESSEL: Others?

MS. BISCEGLIE: So I'm in full alignment. I think the first question, to the first question, I'd like to repeat what was just said as far as culture. I will tell you with both our customers in the public and the private sector, the concept of trust.

So it's the incentives, but it's also making sure they're not going to be retaliated against because we're all getting breached. I mean personally I got hit four times in one week; right. Not my business but me personally. But we kind of, like for Interos, we kind of assume that this is happening to everyone, and cyber concerns and breaches is one piece when we give an assessment of a supplier or the multiple tiers. It's one piece of what we look at because it doesn't make you bad. It makes you living and operational anymore.

And so it's more of what do you do with it? Do you tell your partners? Do you understand, and Jim made a really good point that we focus on, it's really understanding the prioritization and kind of methodology of how to look at this because you can't afford to--you can't afford to protect everything. Nor does everything need to be protected.

And so what you really need to understand is where you're exposed, what the consequences are, risk management tradeoff, and if you have other partners in your business relationships that you're connected to that are ultimately going to protect you if a bad thing happens, and the more, you know, with Gartner saying 90 percent by 2020 of what you buy from an IT standpoint is going to be connected, it's out there--right. This is happening.

So if we could really kind of calm down the conversation, and I do think a national strategy would help with that, and kind of boil it down to say these are the things you need to

focus on, it kind of takes a lot of the fear and the emotion out of that and starts building that cultural shift and that conversation that really needs to occur.

We're seeing a lot of that with some of the major weapons programs between the intelligence community and some of your big defense aerospace contractors, where it used to be, you know, you guys watch your stuff, and risk transference almost, you have to protect us, you are the contractor. The more that they share the information--because we're all a piece of the puzzle, and we are all connected--and so if somebody, if somebody else comes into your world, you know, somebody else is going to find out about it, it's just kind of--it's going to continue, and we're all connected from an IoT standpoint. And the more that we share that information, just the stronger that we all become.

So I agree. I don't think the horse has left either. I just think we really need to focus on building that trust and building in mechanisms that we understand what we need to protect and applying the resources there.

DR. MULVENON: I deal with a lot of companies. You write a book called Chinese Industrial Espionage, people call you about the Chinese conducting industrial espionage against their companies.

And I've had many conversations with companies that are privately outraged and publicly mute because of the potential consequences. Now, some companies have really distinguished themselves in my view by their courage like Intel and others for standing up.

But my point is that companies won't stand up and they won't step from behind their trade associations unless they are convinced that the U.S. government has their back. And since reciprocity is how I would describe the new order of the day in our trade posture with China, we have to ask ourselves what is the basis for our leverage for the U.S. government to be able to push back against these efforts against our companies and try and level the playing field.

And the greatest leverage, of course, that we have is investment access to the U.S. market, which is why I publicly supported FIRRMA and testified in support of FIRRMA to reform the CFIUS system.

But I think that's directly applicable to your second question, which is that there are alternate 5G equipment suppliers. Nokia and Ericsson are two examples, as well as U.S. companies. Nokia, obviously from Finland--I tend not to mess with Finns, as a rule--and Ericsson from Sweden, you know, who have secure supply chains for, in other industries in the United States.

And I would only highlight from, you know, you can call it protectionism, you can call it national strategy, that China's 5G development strategy domestically specifically calls out that one-third of 5G development will be for Huawei, one-third will be for ZTE, and the remaining one-third sliver will be divided up among any foreign competitors. And they use their national security exceptions under WTO as the rationale for that.

There's no reason in my mind why an exactly similar and reciprocal situation cannot be put forward in the context of a national 5G strategy in the United States.

HEARING CO-CHAIR WESSEL: Thank you.

HEARING CO-CHAIR WORTZEL: Commissioner Tobin.

COMMISSIONER TOBIN: Thank you.

The security issue, I want to come at it, my questions, from two angles. One, from the idea of best practices and the other from what you spoke about, Mr. Ferrante, in your written testimony, and both Ms. Bisceglie and Dr. Mulvenon spoke about it just now in the last round of questionings.

And what you said in your written testimony is "an unwillingness to accurately report on cybersecurity status exacerbates the issue. There's a habit of hush-hush management and underreporting of incidents across the board, from retail businesses," and you went on after that.

So how can the American public, be they in business, in education, or in government, who can they learn from? Who are the best practices? You saluted Intel a minute ago. Who is going far on this to try to address the issue of supply chain risk?

Are the audit companies, either the Ernst & Youngs or PCAOB, who is doing work most successfully there? And I think I'll save another question to a second round. But best practices and then what do we do to take care of that underreporting?

And we'll start with Mr. Ferrante.

MR. FERRANTE: Thank you. I think it's an excellent question. And best practices is actually a topic that I talk about with my clients every single day. And, yes, there are standards. NIST has published the Cybersecurity Framework, which is a great blueprint for which organizations can follow, but it's very high level. Okay.

And best practices are only going to get you so far. The other very critical element to cybersecurity, which essentially is risk management, is understanding the risk and where it comes from. One of the very first conversations I have with my clients when I speak with them about cybersecurity is I work with them to identify their critical assets, their critical operation, or their critical data.

Okay. And then we work together to understand who might target them. Okay. If you're a financial institution, organized crime. Financially motivated actors. If you're a pharmaceutical firm, it may be an organization looking to steal your intellectual property. If you're a political entity, it may be an activist looking to make a political statement.

So you need to first understand your adversary and then build best practices defenses around those critical operations, that critical information utilizing this cybersecurity framework as a baseline and building up from there.

COMMISSIONER TOBIN: And with that risk management built into the whole governance structure; right?

MR. FERRANTE: Correct.

COMMISSIONER TOBIN: Thank you.

MS. BISCEGLIE: I would agree, and I'd like to add that the idea of standards, I agree, they get you so far. I find often that when you have standards, you get into kind of a compliance activity.

COMMISSIONER TOBIN: Uh-huh.

MS. BISCEGLIE: Which is not really how business works. Business is very operational. It's constantly changing. Your relationships are constantly changing. And so I think to use a different term, it's almost like an awareness, and so when I was on Governor McAuliffe's Cybersecurity Commission, I was chair for the Public Service and Awareness, and we traveled to six different universities across the state of Virginia.

COMMISSIONER TOBIN: Interesting.

MS. BISCEGLIE: And had forums, and we had people that were independent, you know, LLCs, or just, you know, older people that had a computer at home that had no idea where to go to find information or what to do when something happened to them, and, you know, I laughed sometimes, not often, but I'm my mother's geek squad, and, you know, she'll click on 23 different links--

COMMISSIONER TOBIN: Yes.

MS. BISCEGLIE: --and wonder why her computer isn't working. So the Governor before he became the chair of the Governors Association had this idea of being the person who put the stake in the ground for the states, if you will, that the governors should lead a cybersecurity information sharing, and it goes back to my testimony.

COMMISSIONER TOBIN: Smart.

MS. BISCEGLIE: The idea of having unclassified information sharing builds awareness. It educates people on what the threats are. I'm not a big fan of supporting that everybody needs to have it happen to them to feel the pain because I really like to learn from other people's mistakes.

But I think that it's low cost but big benefits, and when you start having those information sharing, whether it be through the governors associations--I know Virginia, and there were 13 other states, that have like fusion centers that brought the FBI--InfoGuard, InfoGuard--InfoGuard in, as well as DHS and the local police forces in there. So they had protection. They had people that could help them take action. There was education going on.

The second thing, the secondary, if you will, benefit of that is that you start building the trust and changing the culture. And I think that's really big, to your second question, which is getting people to start reporting. These people realize it's okay to talk about--

COMMISSIONER TOBIN: Yeah.

MS. BISCEGLIE: --because they're not the only person this is happening to.

COMMISSIONER TOBIN: There's no shame.

MS. BISCEGLIE: Exactly.

COMMISSIONER TOBIN: And if I may go beyond the red light because I'd like to hear Dr. Mulvenon.

DR. MULVENON: And I'll be brief. As a classified defense contractor who is--

COMMISSIONER TOBIN: Thank you.

DR. MULVENON: --under strict reporting requirements, sort of humorless and vindictive levels of reporting requirements--

[Laughter.]

DR. MULVENON: --I'm not sure the emotion I feel about companies choosing not to report. I don't know whether it's jealousy or a lack of sympathy, but having, but living under that regime and the discipline of that regime, you very quickly develop preemptive practices.

And so in my discussions with people on the SEC side where they're talking about strengthening the requirements to report losses of shareholder value and making it more of a statutory requirement versus a guideline, you know, that's something that needs to seriously be looked at.

But in the course of talking to many different companies, particularly about their China supply chain problems, I have run into some, I have run into some firms that I think are engaged in best practices and do it right.

Verizon has a fantastic supply chain program in place. And the people I've dealt with at Ernst & Young who work on their supply chain consulting team are really first class. And so I think that there are pockets of places where people have really thought through the problem in a significant way, but it is certainly not ubiquitous and spread evenly across any industry sector or in the consulting sector.

COMMISSIONER TOBIN: Thank you all.

HEARING CO-CHAIR WORTZEL: We got rid of my list.

HEARING CO-CHAIR WESSEL: Sorry.

HEARING CO-CHAIR WORTZEL: I think Jon.

COMMISSIONER STIVERS: Thank you. Thank you.

I'd like to focus on your comments in your testimonies about legislation specifically. So I'll kind of throw out a number of ideas and then maybe I'll have each of you speak to that, if that works for you.

Ms. Bisceglie, right--Bisceglie--you mentioned the Modernizing Government Technology Act by Representative Hurd. It creates a fund for modernizing IT systems, and you said that because these new modern systems could be more susceptible to risk than even the older ones, and you mentioned that it didn't include a requirement for supply chain risk management.

While it may have not been required, I mean aren't departments and agencies, don't they still have this in their modernization plans? They don't? That's scary. And so what--we would require that, but my question would be do we need a whole-of-government approach? I mean because we do let the different departments, and obviously different departments and agencies have different security issues, but, you know, would you advocate for a bigger United States government approach to supply chain risk management? So that would be my question so you.

And Mr. Ferrante, you mentioned the Defending U.S. Government Communications Act by Representatives Cheney and Conaway, which prohibits U.S. governments from contracting with China's IT, China's telecom companies, and you stated in your testimony that you thought that legislation falls short because really any device has parts made in China and other places. And so that wouldn't--the legislation falls short for that reason.

And Mr. Mulvenon had mentioned that the barn is out of the door or--I'm sorry--the barn door is shut on that anyway so there's no reason to--

DR. MULVENON: No more metaphors.

[Laughter.]

COMMISSIONER STIVERS: So it wouldn't make any sense to ban Huawei from the United States. And so if you could make some comments about that in terms of--my question is, isn't there a difference between components in a device and the systems that those devices are connected to? And maybe I'm showing a little bit of my ignorance of how this all works.

But just because my phone, maybe it's a U.S. phone or a Samsung phone, just because it has a device, a piece of it made in China, does that make it, is it as susceptible to security risks as say if I'm connected to the Huawei system? That's my question to you.

And to Mr. Mulvenon, you make the case in a broader, in a broader way, that we need a resilience strategy. And so as a policy option, could you kind of explain what that would look like? Would that--and going back to Ms. Bisceglie's comments and her testimony, do we need a whole-of-government resilience framework and security framework? Is that a reasonable--obviously it's ambitious--a reasonable policy option?

So Ms. Bisceglie, maybe if you could start.

MS. BISCEGLIE: So my answer is yes. No.

[Laughter.]

MS. BISCEGLIE: Okay.

DR. MULVENON: Next.

MS. BISCEGLIE: Exactly. Next. You asked about the whole-of-government approach, and we are a big fan, and to answer the question publicly, there is no single place. There is no single legislation, policy, what have you, that is holding all of the agencies accountable.

And to that end, without naming a name, we've had a program with an agency that is responsible for a lot of critical infrastructure for the last six years, and when IT modernization popped up as being something more important, they actually took money out of our supply chain risk management program to put it into the bucket to buy more commercial technology.

And the challenge that's happening, and I do, again, I support the Management Act for the basis of what it's trying to do, which is to replace old technologies, which have their own concerns, but just because you're legacy does not mean that, just because you're newer does not mean that you're safer is a better way to say that.

And we've had this discussion already today that commercial technologies because of the economies and the nation state actors that are at play and the politics that are at play bring their own dangers with them that aren't being looked at.

So when I hear that a $500 million fund is being put in place, that all of the agencies can apply for, it's a slush fund to allow commercial technologies and all the vulnerabilities and nobody is watching to make sure we're secure. I think it's a huge opportunity for a whole-of-government approach.

I mentioned before actually when I spoke about the Wolf provision, Congressman Wolf put out there and said, you know, no to China, and it was a big sledgehammer approach, but it got people's attention, and the year after that, they kind of backed off a little bit and said, okay, it's not just China because we have other problems, too, so it's a better risk management approach.

And I think if I was to look at a whole-of-government approach and national strategy and legislation, again, it's got to be prioritized at the leadership level. So you're talking at the secretaries level. You have to be right-sized to the risk and the threat, and I think that's the point that Jim and I both mentioned, its fit for use, whether it be categorization. You don't have to protect everything that you're buying at the same level, but you at least have to understand why you're protecting things and how you're protecting them.

It needs to be resourced appropriately, its own budgetary line item. And then I think the last thing that I would put in from a legislative standpoint is when the agencies are applying for money to get new technologies, not only do they have to report that they have a plan, but they have to report what the plan has done for them so it's not a compliance activity, but I think to the point that was brought up before, this is happening to all of us.

We're all in this together. So the answer did something happen is yes. Let's get past that. What did your program do? How did you have to, you know, change that to have a larger impact for what your mission is and how you're protecting yourself? So that's what I would look at.

COMMISSIONER STIVERS: Thank you.

Mr. Ferrante.

MR. FERRANTE: So cybersecurity and the risks associated with cybersecurity evolve every single day, and so when it comes to legislative fixes, it's an extremely complicated topic, and there is no black and white solution.

And I think it's really important for us to understand that we cannot operate in a bubble; right? Whatever legislative fixes we propose and enact here in the United States, it's not going to prevent malicious cyber actors around the globe from targeting our infrastructure and causing the effects that they have.

This was a reality that some senior members of government learned in October of 2016 during the Mirai botnet attack on Dyn DNS. When that distributed denial of service attack

occurred, there were some very senior level meetings in and around government on IoT device reform and setting standards and ensuring that this never happens again.

And I'm happy to say that I raised my hand in that meeting and said but what if these devices exist overseas; we have no control of those devices? And everyone looked at me and said that's a really good point because that's just the world that we live in. This is a global Internet. What we do here in the United States definitely has an impact in setting standards, but I believe that a smarter approach would be to work with our allies and maybe even our adversaries around the globe to set these standards and to work together to find standards of behavior, cyber norms, in short.

HEARING CO-CHAIR WORTZEL: Vice Chairman Bartholomew.

VICE CHAIRMAN BARTHOLOMEW: Thanks.

HEARING CO-CHAIR WORTZEL: Oh, I'm sorry. Jim. What the hell, man. I didn't even know you were here.

VICE CHAIRMAN BARTHOLOMEW: Do you have something to add, Jim?

DR. MULVENON: It's your hearing. So just briefly, you know, when I started going out to Pacific Command and TRANSCOM in the late '90s talking about how the Chinese military wanted to hack our automated logistic systems on NIPRNet to impede us getting to a Taiwan scenario, that was the heyday of the answer was, well, we just need to make the perimeter harder. We need a better firewall at the gateway.

I'm happy to report that not only experts but also even laymen in the field now understand that a perimeter-oriented sort of assumption about how we need to fix this is completely outmoded, and in fact resilience is the order of the day, and resilience assumes, as I said before, that you have compromised hardware and software inside of your network, that you have to have defense in-depth, that you have to have internal monitoring, and that you have to be able to then, you know, fail gracefully, if you will, rather than have a strategy where you falsely assume that you have 100 percent failover.

I will tell you this because I've spent two nights in the last two weeks in my server room for six hours dealing with power outages from wind-maggeden and everything else. And, you know, when we did have failover policies that actually saved us in both cases, but we had to sort of explicitly think them through.

To your question, though, about specific componentry, many people on this Commission have heard my story about my iPhone 7 plus, and the Chinese WAPI, you know, chipset that's in here, which is the rejected failed Chinese WiFi replacement protocol. You ask Apple about this chipset, they say it's a blackbox given to them by the Chinese government. You ask about the crypto algorithms, they say the Chinese told them they were state secrets. You ask them the frequency it operates at, and they claim that they don't know although I don't believe that because of the antenna interference studies.

But the implication is if there's a rogue WAPI node, and we know the frequency is different than for WiFi, operating in this room, communicating with my phone, God knows how, I have almost no visibility as a consumer into what's going on with this phone, and that's just simply a component within this device. And why is it in all the global iPhones? Because Apple builds all of them at Foxconn, and they want a global supply chain.

They want a single phone, and China, by the way, from a regulatory and product certification perspective won't allow Apple to build a China phone and then a rest-of-world phone. And so that's where they get boxed in on the supply chain side.

COMMISSIONER STIVERS: Thank you.

VICE CHAIRMAN BARTHOLOMEW: All right. Thank you.

It's just an observation, which is interesting that we're talking about hardware, software, and we haven't talked about the cloud at all, which means I could have the safest, most up-to-date equipment to protect myself, but I don't know where my ISP is storing all of the stuff that gets backed up to the cloud, which is another issue that consumers and companies need to be thinking of.

Jim, I want to follow up a little bit--for all of you--first, I thought it was really interesting what you talked about learning from Chinese, the sort of the structure of their prioritization. One is, of course, because they are producing so much of it, it's easier for them to do that. I mean they have been able to determine, you know, through their five year plans what they're going to subsidize, what they're going to develop, and so it's both easier and economically positive for them to shut other companies out as they make their--as they make their priorities. And I wonder if you could just expound on that a little bit more?

And then there's the issue of cost, which when we know that the Chinese government is subsidizing in one way or another, through tax incentives, through free land, through whatever, these companies, how is it that our government agencies--local, federal--even companies that are trying to reduce costs, they can't necessarily afford to buy Nokia or Ericsson if Huawei stuff is cheaper, and the reason it's cheaper is because the Chinese government is under--it's underwriting what they're doing, how we overcome that?

That's one set of issues, and as usual, I have another one, which is on the private sector participation in any of these initiatives. I mean we know again that they're driven by the profit motive, that's what they do. But what are their responsibilities in this, and as we watch the Chinese government put pressure on companies, most recently we've seen Marriott and the pressure that they've put on Marriott, can we reasonably expect that our tech companies, our companies working in these sectors, are going to be willing to take the risk that the Chinese government will punish them for sort of participating in the kinds of things that we need to be doing in order to I'm going to use the word "harden," but harden everything that we're doing? And I'm not limiting harden to the use of, you know, your perimeters. But--

DR. MULVENON: Well, and perhaps this reflects my bias. As a good analyst, I have to be explicit on my bias. The single greatest, most powerful and capricious weapon that the U.S. government has is called the Federal Acquisition Regulations, and the Federal Acquisition Regulations right now are written in such a way that cheapest is best; right? Okay.

VICE CHAIRMAN BARTHOLOMEW: Uh-huh.

DR. MULVENON: There has not be a sufficient lashing of the FAR to the NIST cybersecurity framework and the guidelines such that there are minimum threshold floors on particular technologies and on the supply chains necessary and the level of supply chain check necessary.

Now I know the Department of Defense has gone through a long painful process and has decided that, you know, semiconductors and integrated circuits is the hill that they want to die on because it is the foundational technology that basically undergirds all of the other capabilities and really having a better understanding through the Office of Commercial and Economic Analysis about the supply chains that bring those chipsets and those circuits into, into DoD systems, but that's--and that's an early good start.

But that's an example, I think, of a better mind-set about how to move forward with this given the fact that we're not going to be able through import substitution to create an American,

you know, hardened trusted foundry industry and those sorts of things like we've seen on the Chinese side.

To your prioritization question, I would only say that one of the interesting things about the Chinese system, and I realize that there's an allergy in this town about regulation, is that the way the Chinese were able to do MLPS is that the standards people who did the prioritization analysis of the five tiers of networks and which ones had to be 100 percent Chinese equipment are the same people that do the product certification and do the industrial planning.

And so you can call that fox in hen house or you can call that a whole-of-government strategy, depending on your ideological persuasion. But that allows them to have this seamless connection between their understanding of the critical infrastructure priorities, the state subsidies and industrial planning that then give the metrics to companies as to what they need to develop and the resources to be able to do it, and then the product certification regulatory apparatus that then approves those for use inside those networks.

And that kind of a connective system does not exist in the United States. Each one of the institutions involved at each of those levels are not connected to the other. And that's just a fundamental difference in the nature of their system versus ours.

MS. BISCEGLIE: So I'm going to answer your second question first, and I mean this very respectfully, but the whole point about how can you hold industry responsible for the--back to the question that was asked before--the government has never asked. They've never asked industry to hold them to a specific level.

And I think that's where a whole-of-government, a national strategy, is a real opportunity. So story from six, seven years ago. I was in a meeting with a DoD CIO who said--not the CIO, but a CIO, who was having a conversation with Dell, and they said, Dell, we need you to sell us a secure machine. And Dell said, well, what's a secure machine to you? And they said, well, you're Dell; you know what it is. So came back with a huge price tag. Because the buying entity couldn't describe where they were concerned, what risks they were concerned about, so that industry knew how to react.

And so that's where this categorization, this right-sizing is incredibly important, and I think to have a policy in place would make it a lot easier because then industry can focus on what they can and can't afford, which is not a government responsibility; it's a business responsibility. Because then it becomes a tradeoff of where they spend their money, and it becomes a natural operation, a natural evolution of how business operates.

And so I wouldn't worry--you know, there's another conversation that is very common out there about what medium and small businesses can and can't do when it comes to cybersecurity. We're a small business. We put protections in place because I know based on what I do what risks I could hand off to my customers.

And so it's all about right-sizing, and from a buying entity, it's asking the right questions, which takes me to kind of the first point, and the point that Jim just mentioned, we've been in conversations with OFPP, and we've been in conversations with DHS and GSA when they're looking at the FAR, and the contracting officials, their biggest concern is limiting competition by looking at too much concern of risk in the supply chain, and as a taxpayer and somewhat smart person, I'm like if they're bad actors why would I want to buy from them anyway?

And so I don't understand why that's a tripping block. I think that that's another opportunity to help them that says, you know what, if they're bad people, we don't want them on a GSA Schedule. We don't want them on NASA SEWP, which is the number one vehicle used to buy equipment in the federal government.

We don't want them on CIO-SP3. That's another place to go. These are really easy business discussions, but the first thing is that from a government standpoint, we need to be able to articulate what our tolerance is so that industry knows how to react.

VICE CHAIRMAN BARTHOLOMEW: Mr. Ferrante, anything?

MR. FERRANTE: I don't have much more to add. I think my colleagues have made excellent points. The only thing that I might say is that in my experience in government and working with organizations and now in private industry, yes, the costs associated with this risk management is definitely a key factor. But I also think we, as a government, and by evidence of this Commission, can educate consumers and educate industry of the risks.

I can think back to a couple of different scenarios when working with my clients where, yes, price point may have been considerably less, but when considering price point and the associated risks, that was something they just didn't want to take on.

And I think that's an important conversation to have, and I think we as a government, the United States, should consider educating industry as much as we can, whether it's an open hearing like this or maybe even classified briefings of these real threats because they are real threats, and it's hard, it's difficult to expect industry to support us and get on board if they don't know.

VICE CHAIRMAN BARTHOLOMEW: Thank you.

HEARING CO-CHAIR WORTZEL: Senator Goodwin.

COMMISSIONER GOODWIN: Thank you, Mr. Chairman.

I'd like to hear a little bit about the challenges in attempting to address and mitigate these risks in the face of disinterest or indifference from the consuming public. I would suspect that the American consuming public's risk tolerance for these sorts of risks corresponds directly with their familiarity with the products, with their use and with the convenience that these products have brought and will bring.

You know, clearly American consumers will--I mean who knows what I've signed away in that Apple terms and conditions sheet; right?

[Laughter.]

COMMISSIONER GOODWIN: We know American consumers will allow some monitoring of their location for ride services. Will the view the fact that using a bike sharing service is sharing their personal data to a company in China differently?

What can we do to educate the public in such a way that it helps the government's ability to mitigate these risks? All of you, all of the panelists.

DR. MULVENON: Senator, I believe it was Patrick Henry who said give me convenience or give me death.

[Laughter.]

DR. MULVENON: I may have that wrong. I'm not sure. But the most astonishing thing--and the younger the person is the more willing they are to give up enormous amounts of their personal privacy on line--is the extent to which the American consumer is their own worst enemy in this regard, and some of the consequences of it have been masked from them. I've had to replace, I won't mention the company, but the very reputable company that I very much enjoyed, I've had to replace my Visa card five times in the last 18 months because of fraud.

And every single time, they just eat it, and so it hasn't had an impact on me except the three days I have to wait for the Fed-Ex to arrive with the new card. But to the extent to which those kinds of costs and that kind of pain, you know, there is going to be an inflection point

where that simply becomes unacceptable, and then that's the point at which you finally may get the clamor to say, you know, we need to have a better system.

But I would think for all intents and purposes, much of that has been masked from the consuming public because of the willingness of companies to either hush-hush, as was said earlier, or simply to eat the costs as risk.

And this is also why the cyber, the nascent cyber insurance industry has had such a difficult time even developing the actuarial tables for this kind of risk because of a lack of an understanding of really what the true costs are, and therefore an inability to actually register out insurance products to companies to be able to measure that because so many of the numbers in this industry--no offense--are just complete FUD, you know, made up for marketing purposes. It's very, very difficult to estimate the level of losses without getting into sort of a Rumsfeldian poetry reading about "known unknowns" or something like that. It's quite a challenge.

HEARING CO-CHAIR WORTZEL: Mr. Ferrante.

MR. FERRANTE: Sure. So I think this is a great question, and I think it drives home a lot of points that I think we've all made today, which is this is going to affect every single person in the United States whether we like it or not.

And educating the public is critical. You mentioned the bike share program. That's a great example. And what people probably don't realize is when they use their credit card and take that bike off the bike rack and ride it, that there's probably a GPS tracking device on that bike, and when you dip your credit card, it's, the owners of the bike share program can determine where you picked up that bike and where you stopped riding that bike.

And what's even more scary, what people don't realize, is through data analytics, they can probably determine who you were riding with, and don't forget, to get one of those bikes, you need a credit card. So there's a true name tied to a human.

So those risks are there. The question is, is educating the public on those risks without scaring them. That's what's critical, and I think we all have a responsibility. These are great efficiencies. Remember what I said earlier. Twenty years from now there will be a million times more advancements, right. We'll be talking about something else "really awesome," as Senator King said, but we need to embrace these advancements without, while also understanding the risks and not scaring the American people.

And I think this is just the tip of the iceberg. These IoT devices are just starting to come into our homes. Five years ago I remember giving an interview, and the reporter was talking to me about control systems, SCADA systems, in factories, and I said, yes, they're definitely at risk, and it worries me, but what about IoT devices that people are bringing into their homes--cameras, locks, microwaves, coffeemakers--right. They all generate data that an adversary could intercept, could steal, could manipulate, and then it gets personal.

Remember what I said when working an incident at a major corporation, it didn't hit home until I briefed the gentleman that his home computer may have been compromised, and then it hit home. And I think that's what's critical; right? We read about breaches everyday in the media, and almost to the point where, they don't even affect us. We don't care, which is too bad, because they are significant. It's not until we get that letter in the mail that says you may have been a victim of this breach, your credit card, your identity, your driver's license, your Social Security number, your home address, your children's Social Security number, do people then sit up and take notice, which unfortunately it's too late.

COMMISSIONER STIVERS: Or you have to pay.

VICE CHAIRMAN BARTHOLOMEW: Well--

COMMISSIONER GOODWIN: Thank you.

MS. BISCEGLIE: I'll just say real quick, I go back to years ago when the number one Christmas gift was the electronic, the frame, that you could upload your pictures to.

HEARING CO-CHAIR WORTZEL: Oh, yeah.

MS. BISCEGLIE: And the whole idea is--and it was very public--China had put backdoors in them so they could get to your, you know, your local computer to get to your banking information. And then you kind of fastforward, and all my stuff, China has got it. I was part of the OPM breach. So that's gone.

And then wearable athletic equipment is going to be a $700 billion industry here, right around the corner, to your point. It's just coming faster and faster. And I think totally agreement about educating the companies, what they're responsible for, the people as much as possible. I like a little fear. I think it wakes people up.

But I think your question about what should the federal government focus on, I don't know, and this is just I don't know if it's--if I could pick out one place like that you would protect my mother because of what she gets, you know, the IoT equipment that she's in, but I think if we focus on what's critical to the government, critical infrastructure, where they're stealing our secrets, let's focus on the big important stuff, like we talked about having a whole-of-government plan, that's where I would think the federal government could have the most impact because I think a lot of this is going to be much more of the wild, wild west, as it just continues to grow.

COMMISSIONER GOODWIN: Thank you.

VICE CHAIRMAN BARTHOLOMEW: Just if I can just make a comment again, which is I agree with you, Ms. Bisceglie, that I think a little bit of fear is what people need because they do these things without thinking about them. I mean recently there was the whole thing about take a picture of your face and they would--this was Google, I think--wasn't it--would match you up with a piece of art, and I said to people do you understand that they're capturing images of your face, and when you--to me a big piece of this is when you look at what China is doing with all of the data that it is gathering on the Chinese people, and we suspect on other people, that riding your bike from Point A to Point B might not be such a big deal when you think about it, but when you think about how that information could be used by a country that's hostile to our interests, it's a real problem.

That's all.

COMMISSIONER TALENT: Yeah. Would you all--and thank you very much for this--would you summarize the number one thing that you would recommend that we recommend, keeping in mind the thing you would pick, keeping in mind, you'd have to--I'd ask you to balance the beneficial effect of this thing if it were done against the difficulty of doing it--right.

So, Ms. Bisceglie, you talked about the whole-of-government approach, which I really agree with, but when you actually think about how do I get a whole-of-government approach in the executive branch, who does it, I'm not saying we shouldn't.

So the one thing that you would like to see happen that you think can happen and would have some beneficial effect?

And the other thing, if somebody here would just tell me, the reference to the Internet of Things, okay, I assume the Internet of--they call it that because it's all of these things that are going to be attached to the Internet--right. I just want a kind of a working definition or what's the alternative, the Internet of Nothing, you know, No Thing? I just didn't know.

So, yeah, if you could answer the other question, I'd appreciate it.

DR. MULVENON: So the real dilemma, sir, is that the Internet of Things is relatively easy to identify now. It's all the gizmos you can get at the Apple store, the cameras, the ring, doorbell systems where you can sort of talk to people even though you're 3,000 miles away and they think you're home, and that sort of thing.

I think the real dilemma is going to be over time that those devices like the immersive networking environment under 5G are going to disappear into the walls. And we're increasingly going to live in a world in which we have what's called ubiquitous networking, where it's less, you know, less device oriented and instead is more immersive.

And so it's going to be harder to say this particular gizmo did this to me because it's going to be part of a mesh, and that's one of the words that's often used with 5G is a "mesh" as a better way of thinking about how all these things connect to each other.

I would just come back, you know, swinging for the fence, which is to say that since the spirit of the day is looking at how China has actually successfully combined state industrial planning with regulation, with large-scale subsidy and investment, to actually leap ahead on many areas that we would like to do like high speed trains, hypersonic glide vehicles, you know, whatever your flavor of the day is, to really relook this issue and to not caricature the issue of U.S. government participation in a national 5G initiative.

And what was lost, for instance, in the Axios report about this was that, in fact, the U.S. government was just going to build out the middle layer of the 5G, and the commercial companies were going to have to build out the more expensive but more lucrative upper and lower layers of 5G, and all the U.S. government was going to be doing was going to be involved in basically like the Eisenhower interstate system building the interstates.

They weren't building the Sheetz and the gas stations and the Starbucks and everything else that were on all the off-ramps. Those were being provided by commercial, but no commercial company felt that they had the MO, or the juice, to be able to actually build out the backbone, and so that's a more sophisticated way of looking at a proposal that was I think very sort of silly in the way it was criticized.

But it is precisely the function of government to be looking at not only mandating the standards for that kind of infrastructure, but then providing the tax incentives and everything else that would go along with facilitating that kind of infrastructure.

That's one of the things the Chinese government does really well, and just because the Chinese government does it doesn't mean necessarily that we have to throw it out the window.

COMMISSIONER TALENT: You're right. This whole issue reeks of externalities, doesn't it?

DR. MULVENON: Yeah.

COMMISSIONER TALENT: I mean that the market is not going to deal with.

DR. MULVENON: Right.

MS. BISCEGLIE: So I think, yes, we're a big fan of the national strategy. I personally don't think, you're not that far from having something that's useful and usable. I think the implementation will take a little while, but I also think that if you were to look at what you have, whether it be, as I mentioned, Circular A-130, which already talked about having a government-wide shared service to look at this. If you look at the Wolf provision, that's in law.

I think the more that you tie regulation to money so the agencies can't get their money unless they're actually adhering to these principles, I think that's really important. So OMB, OFPP, I think you have some real key players that are already participating, and it's just a matter

of somebody saying, yes, this is important to them because it seems to constantly be getting shuffled into something that's less prioritized.

COMMISSIONER TALENT: That would be a possibility because you could do that in the appropriations bills. If you could identify best practices that you were requiring them to follow.

MS. BISCEGLIE: Yeah. So if you look at the Wolf provision, which we wrote about in the report and we're happy to follow up with the Commission on, they actually--that's exactly what it is, it's tied to the appropriations.

And the same thing with the Management Act. You know before you give them any piece of this $500 million, ask them to come up with their supply chain risk program and then have them do some sort of routine, whether it be quarterly or whether it be annually, which is probably easier, so we're not asking them to constantly do reporting.

But some sort of check-in that doesn't just say do they have a supply chain risk management plan, but what did they find? Because what that's going to do, it's actually going to build a best practices library for the government because then they'll start sharing across agencies, and then you'll start getting into awareness and real time alerting and other things that are really needed.

You'll also build the knowledge base of the sub-tier concerns, which you brought up earlier, because it's not--the way that we acquire in the government, we have socioeconomic set-asides, we use a lot of value resellers, we don't necessarily know who the company is when we're doing a contract through a GSA or through whatever other mechanism because they have somebody in front of them, whether it be a small business, whether it be, as I mentioned, some sort of a distributor or a value added reseller.

So I think that there are some real easy procedural things that you can bank on and put it against appropriations. I think you have some of the building stones already in place to capitalize on.

MR. FERRANTE: So I know you asked for one recommendation, and I have one recommendation, but it has three parts.

[Laughter.]

HEARING CO-CHAIR WESSEL: Six subparts.

[Laughter.]

MR. FERRANTE: Cybersecurity threats are everywhere and evolving everyday. Every single day if not every hour. And so we, the United States, we cannot operate in a bubble. We have to realize the fact that this is a global Internet, a global interconnection of machines, and we need to work with our friends and adversaries around the globe to set standards, set standard, acceptable standards of use--cybersecurity; cyber norms. Okay.

And I think we're in a great position to develop a strategy here in the United States, a comprehensive strategy, and then take that strategy globally, and set the standards for our friends and, again, our enemies to have these difficult conversations and set these cyber norms.

The second part is here domestically I think we can do a lot to support our major Internet service providers. Our major Internet service providers in the end are the conduit for this data and these threats to the homes of the American people. And there is no reason why my mother should not be able to fire up her laptop and Facetime with her grandchildren across the country without having to worry about a state-sponsored actor hacking her computer or a financially motivated actor stealing her credit card information.

We need to do better to protect American people and the end-user. The ISPs have insights into this malicious cyber activity in very large volumes. We need to make sure that they have the resources they need to identify these threats and stop these threats before they enter the homes of the American people.

And last, but certainly not least, which is probably the most important recommendation, it's to educate the American people. They need to understand these risks and be able to identify them before they come into their home.

Again, what I said earlier, I think this is the tip of the iceberg. As more and more of these devices are coming into American homes, we need to make sure we do our part to educate American people what they're inviting into their homes.

Thank you.

HEARING CO-CHAIR WORTZEL: We're at the point where we said we were going to do closing remarks. So mine is thank you very much.

These last three comments and Senator Talent's great question may be the three recommendations we get out of this hearing. I thought that was superb, and I'll turn to Commissioner Wessel.

HEARING CO-CHAIR WESSEL: Rather than asking a question, I will make a comment, and first of which, thank you each for all of your work today and all that you've done over time.

Second, to be egocentric for the Commission, the Wolf provisions you're talking about were actually recommendations made by this Commission and the work of this Commission with Mr. Wolf and his able staff who worked so hard not only on that but on DFAR reform. You may recall that the C4ISR depot in New Jersey was using Chinese equipment because there was no ability of the procurement officials to limit, to look at acquisition provenance unless it was something on the munitions list, as I recall, and C4ISR is not on the munitions list.

The other quick comment is you talk about norms and the desire to have international standards, et cetera, all of which I think we want, but I still have a real problem with that in the sense that, as you'll recall, when President Xi and President Obama signed an MOU on cyber espionage, it was an easy deal to reach.

The Chinese agreed they would not engage in cyber espionage for economic gain. I'm sure they laughed their heads off because for them economics and national security are the same thing. So, you know, there may have been a slight drop in the number of intrusions here in the U.S., but the targeting improved dramatically.

So, you know, we're talking past each other at times when it comes to the Chinese and maybe others as to what we mean, and, again, we're about to face, you know, we're in the process of 5G rollout, we have the IoT, and we're still talking about all-of-government and other things when, you know, I think we got to run at light speed and we're not doing that. We're still taking baby steps.

So with that, we will adjourn until April 8; is that correct?

HEARING CO-CHAIR WORTZEL: Fifth.

HEARING CO-CHAIR WESSEL: April 5. I apologize. Thank you all. Thank our staff for all their help in preparing today's hearing, and we stand adjourned.

[Whereupon, at 12:53 p.m., the hearing was adjourned.]

STATEMENT FOR THE RECORD OF DR. HEATH TARBERT, ASSISTANT SECRETARY FOR INTERNATIONAL MARKETS AND INVESTMENT POLICY, U.S. DEPARTMENT OF TREASURY

TESTIMONY OF THE HONORABLE HEATH P. TARBERT
Assistant Secretary of the Treasury
Before the U.S.-China Economic & Security Review Commission
"China, the United States, and Next Generation Connectivity"
March 8, 2018

Chairman Cleveland, Vice Chairman Bartholomew, and distinguished Members of the Commission, thank you for the opportunity to submit written testimony on the potential effects of next-generation connected devices and networks on U.S. economic and national security interests. We appreciate the Commission's recognition of emerging technologies—including fifth-generation wireless (5G) and Internet-of-Things (IoT)—as a key driver of America's economic future and your thoughtful consideration of the potential national security implications of a broader shift toward these new technologies. In addition, we are grateful for the Commission's longstanding support of the Committee on Foreign Investment in the United States (CFIUS), and specifically for your recommendations on how to strengthen and modernize CFIUS. A number of your recommendations are reflected in the Foreign Investment Risk Review Modernization Act (FIRRMA), S. 2098, 115th Cong. (2017), which the Administration has endorsed.

Economic and National Security Implications of 5G and IoT

We believe the rollout of 5G and IoT technologies will involve a growing convergence of know-how and platforms across companies, industries, and countries. These innovations also promise to push us toward enhanced connectivity at the global, national, and individual levels. The potential for enhanced interconnection across users, greater interoperability across platforms, and deeper convergence of 5G and IoT know-how with other breakthrough technologies—such as block chain, robotics, and artificial intelligence—will stretch beyond the traditional realm of what we think of today as communications infrastructure, likely touching almost every aspect of our economy. There are both economic and national security dimensions—opportunities as well as challenges—inherent in these new developments.

The potential significance and breadth of 5G and IoT technologies are generating questions about the best role for government to play not just to address general privacy interests, but also to address vital national security interests. Given the promise that these new breakthroughs offer to our economy and quality of life, it is in our interest to allow these businesses the freedom to seek market opportunities and sources of growth. However, given the potential national security interests at stake, it is important for us to be able to mitigate potential vulnerabilities that could emerge in this new environment.

A key element of U.S. success will be the modernization of our national security-related trade and investment tools to ensure U.S. agility in embracing opportunities while addressing potential risks. As you know from my recent testimony before the U.S. Senate Committee on Banking, Housing, and Urban Affairs, my top priority as Assistant Secretary of the Treasury is ensuring that CFIUS has the tools and resources it needs to

perform the critical national security functions that Congress intended it to.[1] FIRRMA—a bill introduced with broad, bipartisan support—is designed to provide CFIUS with the tools it needs to meet the challenges of today and those likely to arise in the future, including in emerging technologies—the topic before the Commission today. Passage of FIRRMA would enable CFIUS to protect our national security and strengthen America's longstanding open investment policy that fosters innovation and economic growth.

On behalf of the Treasury Department, I want to express our appreciation to the Commission for its early and active support of legislative proposals to update the CFIUS statute to address current and evolving security risks. We share the Commission's view on the importance of expanding CFIUS's ability to review investments in certain U.S.-based start-ups, joint ventures, and other similar arrangements. These types of corporate structures are frequently used in emerging technology sectors—including sectors related to 5G and IoT, such as semiconductors, sensors, and software—and can involve the transfer of sensitive U.S. assets, know-how, and capabilities to foreign actors that merit close scrutiny by CFIUS to mitigate potential U.S. national security risks. We also appreciate the Commission's emphasis on the importance of critical technologies and infrastructure to U.S. national security. Emerging technologies and know-how, including those associated with 5G and IoT, contribute to a broader innovation ecosystem and communications architecture with wide-ranging applications, the ramifications of which often stretch beyond one particular company or technology.

Importance of Foreign Investment in the United States

From the early days of our Republic, the United States has been a leading destination for investors, entrepreneurs, and innovators. In his famous *Report on the Subject of Manufactures*, Alexander Hamilton argued that foreign capital was not something to be feared or viewed as a rival to domestic investment, but was instead a "precious acquisition" in fostering our economic growth.[2] Throughout the nineteenth and twentieth centuries, capital from abroad funded the construction of America from our railways to our city skylines, while at the same time helping make such innovations as the automobile a reality.[3]

Today, the United States is an international leader in emerging technologies and a magnet for global research and development, including foreign capital to support these efforts. Foreign investment plays an important role in U.S. innovation and in developing specific emerging technologies in the United States, just as it has contributed to other important U.S. sectors historically. From Main Street to Wall Street to Silicon Valley, foreign investment has also brought significant benefits to American workers and their families in the form of economic growth and well-paid jobs. As Secretary Mnuchin—echoing his

[1] *See Nomination Hearing Before the S. Comm. on Banking, Housing, and Urban Affairs*, 115th Cong. (May 16, 2017) (testimony of Dr. Heath P. Tarbert).
[2] Alexander Hamilton, *Report on the Subject of Manufactures* (Dec. 5, 1791), *available at* https://founders.archives.gov/documents/Hamilton/01-10-02-0001-0007.
[3] *See* Mira Wilkins, *The History of Foreign Investment in the United States to 1914* (Harvard Univ. Press 1999).

predecessor, Secretary Hamilton—has observed, "we recognize the profound economic benefits of foreign investment" today and place the utmost value on having "industrious and entrepreneurial foreign investors" continue to invest, grow, and innovate in the United States.[4]

Evolution of CFIUS

Despite its many benefits, we are equally cognizant that foreign investment is not always benign. At several junctures in our history we have moved to address specific national security risks generated by the foreign policy context of the time, while aiming to maintain an overall open investment posture.

On the eve of America's entry into World War I, concerned by German acquisitions in our chemical sector and other war-related industries,[5] Congress passed the Trading with the Enemy Act, giving the President broad power to block investments during times of war and national emergency.[6]

Later, in the 1970s, the oil shock that made OPEC countries wealthy led to concern that petrodollars might be used to purchase key U.S. assets. In 1975, President Ford issued an Executive Order creating CFIUS to monitor and report on foreign investments, but with no power to stop those posing national security threats.[7]

Then in the 1980s, a growing number of Japanese acquisitions motivated Congress to pass the Exon-Florio Amendment in 1988.[8] For the first time, the President could block the foreign acquisition of a U.S. company or order divestment where the transaction posed a threat to national security without first declaring an emergency. That law added a new Section 721 to the Defense Production Act of 1950, which remains the statutory cornerstone of CFIUS today.

---

[4] Steven T. Mnuchin, Secretary, Dep't of the Treasury, SelectUSA Investment Summit Welcome Address (June 20, 2017).

[5] Edward M. Graham & David M. Marchick, Institute for Int'l Economics, *U.S. Nat'l Security & Foreign Direct Investment* 4-8 (2006). Prior to America's entry into World War I, it was revealed that the German government made a number of concealed investments into the United States, including establishment of the Bridgeport Projectile Company which "was in business merely to keep America's leading munitions producers too busy to fill genuine orders for the weapons the French and British so desperately needed." Ernest Wittenberg, *The Thrifty Spy on the Sixth Avenue El*, American Heritage (Dec. 1965), *available at* http://www.americanheritage.com/content/thrifty-spy-sixth-avenue-el. The company placed an order for five million pounds of gunpowder and two million shell cases "with the intention of simply storing them." *Id.* The plot was revealed when a German spy inadvertently left his briefcase containing the incriminating documents on a New York City train, with the documents being returned to the custody of the Treasury Department. *Id.*

[6] 50 U.S.C. § 4305. TWEA, originally passed in 1917, empowered the President to "investigate, regulate, direct and compel, nullify, void, prevent or prohibit, any acquisition holding, withholding, use, transfer, withdrawal, transportation, importation or exportation of, or dealing in, or exercising any right, power, or privilege with respect to, or transactions involving, any property in which any foreign country or a national thereof has any interest." *Id.* § 4305(b)(1)(B).

[7] Exec. Order 11,858, 40 F.R. 20,263 (May 7, 1975).

[8] Pub. L. 100-418, Title V, § 5021, 102 Stat. 1107 (1988).

Subsequently, in 1992, Congress passed the Byrd Amendment, which requires CFIUS to undertake an investigation whenever two criteria are met: (1) the acquirer is controlled by or acting on behalf of a foreign government; and (2) the acquisition results in control of a person engaged in interstate commerce in the United States that could threaten our national security.[9] In the years that followed, it became evident that CFIUS and Congress did not share the same view on when a 45-day investigation period was discretionary rather than mandatory, a rift that was more clearly exposed in the wake of the Dubai Ports World controversy. In order to instill greater procedural rigor and accountability into CFIUS's process, Congress enacted the Foreign Investment and National Security Act of 2007 (FINSA), which formally established CFIUS by statute and codified its current structure and processes.[10]

Now, more than a decade after FINSA and three decades after Exon-Florio, we find ourselves at another historic inflection point. New developments in the current geopolitical climate—including the significant uptick in strategic investments by some foreign governments and the growing role of technology in the economy and in national defense—call again for an updating of CFIUS to allow for closer scrutiny of the potential national security risks associated with foreign investment in U.S. emerging technologies. The national security landscape as it relates to foreign investment has been shifting over the past several years in ways that have eclipsed the magnitude of any other shift in CFIUS's 40-year history. Nowhere is that shift more evident than in the caseload CFIUS now faces.

The new challenges that CFIUS is confronting arise from a number of different factors. First, the ways some foreign governments are using investments—particularly those in emerging technologies—to meet strategic objectives, are generating concerns about the potential U.S. national security ramifications of acquisitions, including in sectors that might not have been considered sensitive in the past. Second, increasingly complex transaction structures—in some cases designed to dilute the appearance of government involvement or even to skirt CFIUS authorities—have become more common. Third, growing U.S. reliance on globalized supply chains in which there are newly forming concentrations of control, poses particular risks. Fourth, with the growing role of technology in national defense, CFIUS faces new national security risks posed by technologies that have current and potential future defense applications; military capabilities are rapidly building on top of commercial innovations. And fifth, the digital, data-driven economy—a trend likely to accelerate and intensify with the introduction of 5G and IoT technologies—has created national security vulnerabilities never before seen. Today, the acquisition of a Silicon Valley start-up may raise just as serious concerns from a national security perspective as the acquisition of a defense or aerospace company, CFIUS's traditional area of focus.

CFIUS's exposure to such complex and challenging cases has allowed it to play a critical role in protecting against threats to national security. At the same time, however, this has highlighted gaps in our jurisdictional authorities—particularly in sectors such as

[9] Pub. L. 102-484, 106 Stat. 2315 (1992).
[10] Pub. L. 110-49, 121 Stat. 246 (2007).

emerging technologies. We continue to be made aware of transactions we lack the jurisdiction to review but which pose similar national security concerns to those already before CFIUS. These gaps are widening as threat actors see such transaction forms as an effective means to acquire leading edge capabilities rapidly without being subject to national security-based regulatory restrictions. The problem lies in part in the fact that CFIUS's jurisdictional grant is now 30 years old, originating with the Exon-Florio Amendment and maintained in FINSA. Under current law, CFIUS has authority to review only those mergers, acquisitions, and takeovers that result in foreign "control" of a "U.S. business." That made sense in the 1980s and even in the first decade of this century. But in recent years, the foreign investment landscape has changed significantly, with non-controlling investments and joint ventures becoming ever more popular.

Consequently, certain transactions—such as investments that are not passive, but simultaneously do not convey "control" in a U.S. business—that CFIUS has identified as presenting a national security risk nonetheless remain outside our purview. These types of venture capital deals are particularly widespread within the emerging technology sector. Similarly, CFIUS is also aware that some parties may be deliberately structuring their transactions to come just below the control threshold to avoid CFIUS review, while others are moving critical technology and associated expertise from a U.S. business to offshore joint ventures. We see joint ventures and licensing arrangements of concern, for example, in emerging technologies, including subsectors that support 5G, IoT, artificial intelligence, medical technologies, microelectronics, robotics, and semiconductors, to name a few. While we recognize there can and should be space for creative deal-making, purposeful attempts to evade CFIUS review put our country's national security at risk. Finally, we regularly contend with gaps that likely never should have existed at all, such as the statutory loophole that allows purchases of businesses located in close proximity to sensitive military sites to be reviewed by CFIUS, but not purchases of vacant land. These gaps can lead to disparate outcomes in transactions presenting identical national security threats.

Support for FIRRMA

The Administration endorses FIRRMA because it embraces four pillars critical for CFIUS modernization. First, FIRRMA expands the scope of transactions potentially reviewable by CFIUS, including certain non-passive, non-controlling investments, transfer of sensitive capabilities of U.S. businesses through arrangements such as joint ventures, real estate purchases near sensitive military sites, and transactions structured to evade CFIUS review. The reasons for these changes are twofold: (1) they will close gaps in CFIUS's authorities by expanding the types of transactions subject to CFIUS review; and (2) they will give CFIUS greater ability to prevent parties from restructuring their transactions to avoid or evade CFIUS review when the aspects of the transaction that pose critical national security concerns remain.

Second, FIRRMA empowers CFIUS to refine its procedures to ensure the process is tailored, efficient, and effective. Under FIRRMA, CFIUS is authorized to exclude certain non-controlling transactions that would otherwise be covered by the expanded authority.

Such exclusions could be based on whether the foreign investors are from a country that meets specified criteria, such as having a national security review process for foreign investment.

FIRRMA also allows CFIUS to identify specific types of contributions by technology, sector, subsector, transaction type, or other transaction characteristics that warrant review—effectively excluding those that do not. Additionally, CFIUS can define circumstances in which certain transactions can be excluded because other provisions of law—like export controls—are determined to be adequate to address any national security concerns. Only where existing authorities cannot resolve the risk will CFIUS step in to act. Emerging technologies is likely to be one of those areas where there are gaps and CFIUS will continue to have an important role as the last line of defense.

Third, FIRRMA recognizes that our own national security is linked to the security of our closest allies, who face similar threats. In light of increasingly globalized supply chains, it is essential to our national security that our allies maintain robust and effective national security review processes to vet foreign investments into their countries. As noted above, FIRRMA gives CFIUS the discretion to exempt certain transactions from review involving parties from certain countries based on such factors as the nature of the U.S. strategic relationship with the country and the nature of the other country's process to review the national security implications of foreign investment. FIRRMA will also enhance collaboration with our allies and partners by allowing information-sharing, subject to appropriate controls, for national security purposes with domestic or foreign governments.

Fourth, FIRRMA requires an assessment of the resources necessary for CFIUS to fulfill its critical mission. FIRRMA would establish for the first time a "CFIUS Fund," which would be authorized to receive appropriations. Under FIRRMA, these monies are intended to cover work on reviews, investigations, and other CFIUS activities. FIRRMA also authorizes CFIUS to assess and collect fees, which we would anticipate would be set by regulation at a level that does not affect the economics of any given transaction. Finally, FIRRMA grants the Secretary of the Treasury, as CFIUS chairperson, the authority to transfer funding from the CFIUS Fund to any member agencies to address evolving needs in executing requirements of the bill. This approach would enhance the ability of agencies to work together on national security issues.

***

In sum, I appreciate the Commission's support for modernizing and strengthening CFIUS to address current and future national security risks. In that regard, I am hopeful that FIRRMA will continue to move forward on a bipartisan, bicameral basis. It is our aim that, with these enhanced authorities, the United States will be best positioned to embrace the promise of emerging technologies, including those associated with 5G and IoT. Thank you.