Hudson Institute

Competing Perspectives:
How Does the U.S. Maintain a Competitive Edge in 5G?

- Dr. Nadia Schadlow, *Senior Fellow, Hudson Institute; former U.S. Deputy National Security Advisor for Strategy*
- Dr. Rob Spalding, *Senior Fellow, Hudson Institute; former Senior Director for Strategic Planning, U.S. National Security Council*
- Harold Furchtgott-Roth, *Director, Center for the Economics of the Internet, Hudson Institute; former FCC Commissioner*

Hudson Institute, Washington D.C. Headquarters
1201 Pennsylvania Avenue, N.W., Suite 400
Washington, DC 20004
March 26th, 2019

TRANSCRIPT

Please note: This transcript is based off a recording and mistranslations may appear in text. A video of the event is available: https://www.hudson.org/events/1667-competing-perspectives-how-does-the-u-s-maintain-a-competitive-edge-in-5-g-32019

NADIA SCHADLOW: Good morning, everyone. Thank you for coming this morning. It's my first 5G event at Hudson. So I thought today I will introduce the speakers and then essentially moderate a discussion. Our speakers are both experts on 5G-related issues. We have a series of questions that we can talk about, and then I'm happy to take questions from the audience toward the end, and we will end promptly at 11:00. So thank you. So first, I'll introduce Harold Furchtgott-Roth and then Rob Spalding.

Harold is the director of the Center for the Economics of the Internet at the Hudson Institute here. Prior to this, he's done many things in his career. He was a visiting fellow at AEI. He wrote a book called “A Tough Act To Follow?" about the difficulties of implementing the Telecommunications Act of 1996. And from 1997 through 2001, he was commissioner of the Federal Communications Commission, the FCC. In that capacity, he served on the Joint Board on Universal Service, and he's one of the few economists to have served as a federal regulatory commissioner and the only one to have served on the FCC.

Rob Spalding is a friend of mine. We worked together on the National Security Council. He's a retired brigadier general in the Air Force and has also done many things in his career; among them, I will just highlight a few. He was a key person in drafting and helping to draft the National Security Strategy of the Trump administration. He speaks fluent Chinese and spent time in China as an Air Force officer. You were the DATT, right?

ROBERT SPALDING: Mmm hmm.

SCHADLOW: Right. He's also a skilled combat leader. He had - he led the 509th Operations Group, the only - the nation's only B-2 stealth bomber unit. And he's done a lot, so I'm really happy to have him here today. So I thought I would begin the discussion a little bit with talking about 5G in a general sense. I really learned a lot about the topic when I was working on the National Security Council and, specifically, helping to draft the National Security Strategy. We actually have some language in there on 5G, thanks to Rob and others. As many of you know, who've looked at the strategy, a key feature of it is its discussion of the nature of the competition out there - the military, political and economic competitions taking place, all accelerated by technology.

This is a theme of the document and a theme of the Trump administration. And 5G is really part of that landscape of the competition, what's happening there, both economically because it will be so important to our future economy and also from a national security perspective. So I think in some ways it really is a litmus test for kind of understanding how the country is going to think about this competition over the near to medium term. I mean, it's happening now. So why don't we start with Harold to start a little bit - your perspective on 5G - kind of to paint the landscape and the picture, and then we'll go to Rob. There are different views, and the Hudson is a place where diverse views can and should be debated. So there are different views on how the United States should best tackle the 5G challenge, and I think we'll hear some of those today.

HAROLD FURCHTGOTT-ROTH: Well, thank you, Nadia, and thank you for organizing this session today. It's a great honor to be here with you and Rob. 5G is a type of wireless technology. Once every five years or so, there's a new generation of wireless technology - 1G, 2G, 3G, 4G - sounds a little bit like a Dr. Seuss book. 5G is the next generation, and unlike the prior generations - which you could come up with a very specific definition of exactly what the capabilities were, which bands of spectrum it could operate on, exactly what its technical characteristics look like - 5G is going to be a little different. It won't be limited to specific bands. It will operate in a lot of different bands, very often in combinations of bands of spectrum.

We could think - you can think about it in a few different characteristics. One is speed - it's going to be substantially faster than current speed; latency - the time lapse between sending a signal and receiving a signal is going to be shortened a great deal; and capacity - the amount of information that can flow is going to be substantially greater than today. The current plans - a lot of wireless carriers plan to deploy 5G technology in the next year or two. Some countries, such as China, have already deployed a great deal of 5G technology. And it has become one of the central points of tension, if you will, between the United States and China over the past couple of years, I would say. China has made 5G technology one of its strategic initiatives, at the central government level, and they've been very successful at it. It is something where the central planning of China has been able to insinuate China into 5G in ways that did not exist in prior generations of wireless technology. And the issue - I think we'll be discussing some today - is, is this something that the United States, as a government, should respond to in some way, and if so, what should that response look like?

SCHADLOW: Exactly. Perfect opening. Rob - a perspective also on how 5G not only will change our economy maybe in some specific ways but also the implications for national security.

SPALDING: As you know, we discuss the importance of the information domain in the National Security Strategy and really 5G is at the heart of how the information domain is changing. I got my first modem, and I got on the Internet in 1995, I think. You know, 2007, with the introduction of the iPhone, was a time that, you know, the Internet really moved from, you know, being stuck on the computer to your mobile device. I think this evolution of wireless - in bringing the Internet together with artificial intelligence, machine learning, big data and machines - is going to be a fundamental change in our lives, primarily because we're not going to see very much change in terms of how our mobile devices perform, but certainly, we're going to see a whole bunch of machines that start to show up outside our door that are doing things for us in a very beneficial way.

So when you look at it in terms of the national security perspective - Europe dominated 2G, 3G; U.S. dominated 4G; and the Chinese essentially decided that they're going to dominate 5G. Well, when you build out most of the world's infrastructure, and you realize that most of the traffic is going to migrate to these wireless networks, then you have enormous power to do surveillance, you have enormous power to use the machines that are connected in ways that aren't intended by their owners, and you have a huge ability, specifically with big data and artificial intelligence, to begin to influence populations. And we saw that in the 2016 election, we continue to see it both from the Russians and the Chinese, and as the National Endowment for Democracy and the Hoover Institution demonstrated, there is enormous influence going on in the world today. And that was with, you know, 4G technology. You know, imagine what that will be like when there is such pervasive amount of data and understanding and the ability to implement that at a very fine level - it's staggering.

SCHADLOW: I want to talk a little bit about the relationship - just as some of you in the audience might be as new to 5G as I am - but the relationship between the infrastructure of 5G and then what runs through it and who produces the infrastructure and some of the nature of the landscape there, in terms of American companies, Chinese companies, because not everyone might be familiar with that, and it's an important component to what we've seen in the news.

FURCHTGOTT-ROTH: Most of us are familiar with different manufacturers of handsets. I happen to have an Apple; some people have Samsung. There are a variety of manufacturers of handsets. The handsets don't really talk to each other very much. Mostly traffic goes - actually, 85 percent of traffic goes through Wi-Fi; well, I can talk about that separately. A lot of the discussion has to do more with the cellular networks. And today, there are essentially four manufacturers that have complete suites of network equipment, and those would be Huawei from China, Samsung from Korea, Ericsson from Sweden, Nokia from Finland. There are other companies, such as Cisco, that have some parts of the suites of network equipment. There are other companies that license technology that's used in network equipment, whether it's Qualcomm, Intel, others. But in terms of major manufacturers - actually, Cisco is a partial manufacturer - but most of the manufacturers are not American. Huawei, on the other hand, is the - has staked out a position in 5G. They have deployed hundreds of thousands of base stations in China and in other parts of the world. There are contracts for Huawei equipment in dozens of countries around the world. So that's on the network equipment side.

And the landscape is - in part, one of the questions is, how many companies can survive in the market for 5G network equipment? In the past, if you go back 20 years ago, there were probably a dozen different manufacturers for wireless network equipment. Some of those companies - most of those companies don't exist anymore; they've gone out of business, or they've consolidated in some way. As technology has advanced, the importance of economies of scale in the manufacture of this equipment has become more important. The number of viable companies has probably shrunk. And I think one of the questions right now is, how many companies can survive in a 5G network world? And then going forward, you know, again, every - approximately every five years or so there's a new generation of wireless technology. And what is the future for the manufacturing of network equipment in the wireless space?

SCHADLOW: Rob, do you want to comment a little bit?

SPALDING: Yeah. The bottom line is we've ceded our ability to manufacture microelectronics, which if you consider - you know, if you had a potential adversary and you were going to allow them to manufacture all your weapons of war, that might be - put you in a certainly challenging position. As we've said, the information domain is the most important domain in the 21st century. Data is a strategic resource. And to the extent that you allow the hardware that carries that data to be manufactured in a totalitarian state that has values and principles that are inimical to yours, you're essentially putting yourself at their whims.

FURCHTGOTT-ROTH: I would note that we've done very little manufacturing of electronic equipment in this space probably for 20 years in the United States. Most electronic manufacturing in the world today goes on in China - and some of it by Chinese-owned firms, a lot of it by non-Chinese firms. And that transition to manufacturing in China has been going on for quite a while now. It does present problems that Rob knows, but this is not a new problem and not unique to 5G, I would say.

SCHADLOW: So what are some of the alternatives now to change - what alternatives do we have in front of us to change course or to shape the landscape in a way that's favorable to U.S. interests or at least not harmful? And then, second, I think we need to talk about the role of allies and partners and other states and how their decisions today are likely to impact us. Rob, do you want to...

SPALDING: Yeah. So just remember when you came into the White House. The discussion at that point was - economic security and national security are completely separate things. Like, we don't consider them even to be on the same planet. The NEC does its thing, and the NSC does its thing. That's not the final conclusion we came to in the national security strategy. Economic security actually underpins national security. And so the idea that you can cede everything that you do in your economy to the market does not necessarily bode well for a future where market forces are essentially being undermined consistently by players that don't abide by fair rules. So I mean, it is a fair question, how many players can the market and the industry sustain? But a far more important question is, how do we prevail in a world where there's such, you know, a complete disavowal of any of the international rules when it comes to industry. And so it's not a mistake that microelectronic manufacturing went away in the United States. That, you know - I would contend - was part of a deliberate strategy. It wasn't just business. It was - there was definitely - other than market forces going on, I believe that there is a national strategy in China around telecommunications, specifically dominating telecommunications, not for a market-based decision, not for solely an economic decision. It's a national decision, and it provides enormous power in a world where we're so connected.

FURCHTGOTT-ROTH: Look. I agree with that. I think the - at the end of the day, I think the important thing for the United States, though, is we are a free market country. We are a country in which new technologies have evolved in a free market society. And I'd say the wireless industry is maybe the greatest example of that. The wireless industry developed not because of government interference but precisely by the absence of government interference. For much of the past 30 years, the wireless industry has been the least regulated industry in the United States. For the prior 30 years, from the late 1940s to the late 1980s in fact, it was government regulation that prevented the development of wireless technologies in the United States. I - the way that the United States has developed well in wireless technology has been with a very light touch of government regulation, and I think that's probably the best path forward. China presents, I think, the exact opposite approach, which is heavy central government planning, heavy central government regulation, and that's a way that may work for China. I'm just not sure that that's the best approach for the United States.

SCHADLOW: There are security issues, though. I think one - you know, one of the issues that I've grappled with is, how do you impress upon the private sector and, I would say, the wireless industry specifically, also, the importance of security, where they just haven't emphasized it? In their spending, in their business plans, it's not an issue of importance to them. And so it seems that one key way forward is somehow to develop a shared consciousness as - I like that term. General McChrystal used it in his book a shared consciousness of the problem by the - by, in this case, the wireless industry. But even more broadly, that seems to be an important first step because - well, the technical experts will know. But 4G is not a secure system, right? It's very, very vulnerable in many ways. And so that also leads to some of the implications for national security and the military and DOD's thinking about 5G. So could you comment on how you get the private sector to understand the problem set in a different way and does that matter? And then too, Rob, if you could go into a little bit more of how DOD is seeing 5G.

SPALDING: Yeah. I think - look. We're at an inflection point in history in terms of where technology impacts are our everyday lives. I would agree that at one point we were dominant in wireless. I think we've lost that. In fact, the Chinese have accelerated past us. Today I think we're 62nd in terms of wireless speed in the world. We're about fifth most expensive - in other words, five - six times the cost of what somebody pays in Hong Kong for connection, five times of what they pay in Stockholm. Thirty-four million Americans don't have access to broadband, you know, unless you want to define it at the incredibly low speeds that the FCC is currently defining it as - not only that but even the wireless companies themselves don't actually think of themselves as wireless companies. The CEO of AT&T was here last week talking about his competitors. Who did he call his competitors? Disney. Last time I checked, Disney wasn't a network company. They're an entertainment company. So there has been a change in the business models within the wireless companies. They've basically stagnated on the customers they have.

Their business models have transitioned to - let's increase revenue per customer. Let's do that by being content creators and content owners and content distributors. It's not about building the network. The AT&T CEO, the Verizon CEO, the T-Mobile CEO does not get up every single morning and think about - how do I secure - how do I protect the American people? Thinks about, how do I increase revenue for my shareholders? That's their fiduciary responsibility. There is a role for government in thinking about what we've called the most important domain in the 21st century - how we protect Americans' data? If you go around today, does anybody in this room expect that anything that they do is actually secured from either a state actor or just a regular hacker, you know, in their basement? No. Everybody's basically became - become used to the fact that we essentially have no freedoms when it comes to the digital space. There is an obligation to design that in the technology. Now, we've allowed it to develop organically in democracies to the point where it actually threatens democracies now. And so with the introduction of 5G, that's only going to accelerate. You know, rather than 10,000 devices per - you know, within the square mile of this location, you're going to have 3 million. And it's going to be far more pervasive in terms of what the data aggregators know about you and how they can influence your lives. Today it's Amazon. It's Google. It's Facebook. Tomorrow it's going to Baidu, Ali Baba, Tencent and the Chinese Communist Party.

FURCHTGOTT-ROTH: Well, let me note a couple things. One is Huawei technology is not in the networks of the major wireless carriers in the United States and has not been there for several years now. When Sprint acquired Clearwire in 2013, one of the conditions of the acquisition was to get rid of Huawei equipment. The concern was potential security problems with the Huawei equipment, not necessarily collection of information as much as just how reliable and how easily hacked the equipment was. There's growing concern that Huawei equipment in both the United States and in many other countries around the world - I think Rob raises a good point about the difference between different types of equipment and the type of security we think we have with the information that we have. And that is something that's been going on with all levels of wireless technology. It's not new to 5G that the sense of how secure your information is - who is looking at it, whether it's state actors or government actors or frankly commercial companies that simply use the information that you have - it's something that's been going on for quite some time.

The last point Rob made is also probably the most important. As important as - are the actual networks in wireless services, the even more important services are the online services that ride on top of them. The largest corporations in the world - Amazon, Facebook, Google, Microsoft, Apple; Apple's maybe a little different - but the others, they're not actually based on network equipment, they're not actually based on providing direct wireless services; they are the services that ride on top of them. And today, those corporations, the largest ones in the world, tend to be American corporations. There is a generation of parallel companies in China that look an awful lot like the American companies, and they're doing very well in many parts of the world - much larger potential than actually just providing the basic communications services.

SPALDING: Yeah. To answer your question on DOD, DOD is still - you know, I would say if you're occupied with lethality, is there a primary goal? I would say, in the information domain, there's a lot you can do to undermine democracies without getting lethal. And there is an obligation for them to begin to think differently about the world. I mean, it was clear in the National Security Strategy - we need to think differently about the future, particularly as it relates to artificial intelligence, the use of data and how pervasive that gets injected into our societies. DOD can't wait until essentially they're - the society's been undermined beneath them, before they begin to think about what's their role in defending the population?

SCHADLOW: It's a completely - it's an - interesting in terms of thinking about the nature of Homeland Security, right? And it's a different approach - you know, thinking about...

SPALDING: Well, you think about why militaries were developed in the first place; they were developed to protect populations from being coerced by other nations. Well, when you can actually go right into the heart of the society and begin to undermine it from within, then, you know, the nature of how you defend that - really, you have to think differently about that.

SCHADLOW: Well, there are about 58 countries now that have already agreed to incorporate Chinese hardware into their systems. Are things proceeding in a way that's inexorable? I mean, are there decision points in the future? And I think that that's important actually for a place like Hudson and other think tanks as well to think about - are there key decision points in the future which can be shaped - right? - where both the private sector needs to be thinking about that in a strategic way? DOD - the role of working bilaterally with allies and partners on this problem set - is this a multilateral problem set, where we need to create new fora to deal with this in the near term? Any thoughts?

FURCHTGOTT-ROTH: Well, you're right - a great many carriers around the world have signed contracts or released letters of intent with Huawei to use their equipment. I'm not sure how much these are DOD issues as other types of issues. Wireless carriers around the world are private companies. They're private companies even in China and even in North Korea. The wireless carrier there is - North Korean government couldn't possibly do that, so they brought in some private company to handle their wireless services. And these wireless companies are exactly what Rob said - the CEOs of the companies have fiduciary responsibilities to make money for their shareholders. They wake up in the morning; they're less concerned about security than they are about profitability. And the wireless carriers, typically, they do contracting the way all businesses do; they'll send out an RFP, they'll get various proposals. And Huawei has been - and they'll get proposals probably from Samsung, Nokia, Ericsson, maybe some other companies as well. Huawei has been very low on costs. And then they've been also able to put together packages of financing, either directly from Huawei or from the Chinese government, that have been incredibly attractive, not just in developing countries but in European countries as well. And the combination of a low cost and very attractive financing has been very difficult to - for the other companies to compete with. Is that something that - I don't really have a...

SCHADLOW: Yeah.

FURCHTGOTT-ROTH: ...Silver-bullet answer for you. There has been some growing resistance, though, on the security side. National intelligence services in various countries, particularly in Europe, have been very concerned. They've expressed those concerns to their national governments. But at the end of the day, a lot of - these are private companies making these decisions. And the relationship between national governments and the private carriers about how those decisions are made is going to vary country by country.

SPALDING: Yeah, and I think allies and partners are looking for America to lead. It's not - you know, it can't be just no way, Huawei. It's got to - what is our strategy to lead the free world in this 21st century where information dominance is absolutely critical to maintaining your freedoms. That's something that our allies and partners are asking. So if you just come to them and say, hey, well, we don't want you install Huawei. OK, well, what's your plan? I don't think that's a winning strategy. I would note that, you know, President Eisenhower built a highway system that was ostensibly made for national security reasons. It was connected to our Air Force bases. But I would venture to say that most of us enjoy the lives we do today because of the trucking system that goes along that highway system that was built ostensibly for national security reasons. So let's go back to the space race. We engineered most of our - we taught most of our scientists based on federal grants for them to go get engineering degrees to work on the space program. Most of our technology that we've been living the fat - off the fat of for the last 40 years was actually created by a lot of the U.S. investment during the Cold War. So it is not - it would not be the first time that national security actually injected lifeblood into the innovation system of this country.

SCHADLOW: Open it up soon for questions, so start thinking. And then I'm going to put my friend Chris Walker on the spot too, back (laughter) - because he's done a lot of work on this at NED. So - and I'm - be interested in some of your comments. Going to ask one more question specifically about spectrum and 5G, Internet of things, military national security and spectrum availability for the military. Do you want to comment on that a little bit, Rob? Because that's also an important part of this.

SPALDING: Yeah. I think the spectrum problem's overblown. Look, I don't agree that probably the best way is to auction off spectrum, then let companies sit on that and not use it. So - and that's been going on quite a bit. I would say that with 5G in terms of how you can do network slicing, how you can do - use multiple spectrums, as Harold was talking about, there's an opportunity here for rethink the way - to rethink the way we use spectrum. I don't know. I don't have an answer from a policy perspective in terms of should, you know, DOD give up its spectrum. I know DOD has been harmed in the past by having to give up spectrum that they thought that they needed for their mission, so I'm not going to speak about that. What I will say is we put men on the moon. We did awesome things. We can figure the spectrum deal out. And it doesn't have to be the companies calling the shots. We can put a lot of smart people in the room and say, how do we divide the spectrum in a way that benefits American people?

SCHADLOW: Rob, would you be satisfied or would you feel a little bit better if companies, even if a few out there, indicated that they recognized the urgency of this problem set, that they have a role in protecting democracy and the landscape which they have emerged from - right? - essentially.

SPALDING: Yeah.

SCHADLOW: So is it possible, or is that too...

SPALDING: I don't think it's possible. And that's primarily because of the way they've managed their companies. They're - most of them are heavily laden with debt. They have enormous 4G investments that they have to take care of. So they're - right now, they're just not in a position to move in a way that the nation needs to move strategically. Now, could they come up with a game plan to perhaps join forces and do something for the country? I think they could. But, you know, it - they're not going to do that without some kind of incentive in the system for them to do so. Right now, they have a responsibility. This is the way our system designed. Like it or not, we have free markets, and we have democratic principles. And they go together, and they work together. Unfortunately, sometimes it doesn't work to get us out of a situation that we're in. That's why we had things like the national highway system. That's why we had the space race. There are times when we need to think differently about how we do things. But, you know, it's going to take leadership from government saying, this is what we need. And it can't be just, hey, AT&T, we need you to do this, because how would they be incentivized to do so in the current system? They're not.

SCHADLOW: Right. So at the very least, we need a clear sense of what kinds of incentives need to exist.

SPALDING: Right.

SCHADLOW: …Like, the nuts and bolts of that. And again, that would be - that's not something that we can - the three of us can develop on this panel this morning. But it is something that can be done. Harold?

FURCHTGOTT-ROTH: Let me just make a couple points. One, I do think the 5G plans of American wireless carriers are being constrained by spectrum availability. It's just been - there's a lot of spectrum in the pipeline coming from the government to get to the FCC to be licensed off. And there a lot - there's a lot of spectrum that will eventually be used for 5G that's in that pipeline. Second, keep in minds that, at least specifically on Huawei, there is no Huawei equipment in the wireless networks of the major American carriers, and there hasn't been for years. You mentioned Randall Stephenson, the CEO of AT&T. He gave a speech last week on this Huawei issue. And I'm not sure he would - what he said was very consistent with what we've been saying up here. So it's not that the American wireless carriers are somehow unaware of security issues.

But Rob does make a good point. The - at the end of the day, that is not their primary objective. Their primary objective is to have a profitable business. The types of security - the types of wireless networks that are available throughout the world are frankly - they're frankly, let's say - because there are only a handful of manufacturers of network equipment. So it's not that there are some place in the world some types of secure networks that wireless carriers here simply aren't buying because they don't want to. It's the same network equipment that's available everywhere. It's the same network equipment that is vulnerable to security lapses, to breaches. And I think what Rob is getting at, really, is that we may need to think about ways of developing more secure networks. And where that is taking place, both on the military side and on the corporate side of the United States, is what are called private networks. Public networks are inherently unsecure. And it's coming up with what I would call private networks that do not connect as clearly to the rest of the Internet that are ways that you have much more secure communications.

SPALDING: Yeah. And I've lived this for 27 years in there as an Air Force officer, both as a consumer - so I was subject to, you know, the bad connectivity out in the hinterland because guess what? That's where our bases are. But I'll let you consider this. While they're not in the - Huawei and ZTE is not in the main carriers, it is in the rural carriers. Guess where the rural carriers are? They're where our military bases are. So we've got Huawei and ZTE equipment surrounding our military bases, surrounding our missile fields. You know, so think about in terms of the intelligence collection capability that gives, you know, the Chinese. It's - we just haven't thought deeply enough about this problem. We are so focused - and I'm speaking now, a former member of Department of Defense - we are so focused on the away fight, we've completely lost sight of what's happening here at home.

SCHADLOW: Well, on that happy note, clearly I think that we're seeing that 5G, to go to the beginning of the discussion, is a litmus test in a sense for how we're dealing with these new challenges and how democracies need new operating models to compete against authoritarian state actors. And we don't have the models yet. We haven't deployed them, and we need to do more thinking about them. And we need to do it quickly, actually. This is not a long-term problem set. It's something that, as we started the discussion, it's happening now. And decisions are being made now that will have long-term implications. So I'll open it up to discussion. There's a gentleman there. And then I'll ask - Chris, are you OK with saying a few comments about NED's work? And then we'll go round the room. If you could also say where you're from or your name, please.

DAVID WINKS: David Winks with AcquSight. In your earlier comment, it seemed that the value of data about people's life patterns is what drives a lot of the business models for Google and Alibaba. With that data, is there a concern with the recent changes in the Chinese laws requiring Chinese companies to cooperate with Chinese intelligence that somehow they would use that data to do the same sort of composite scoring on Americans that is being done in their own country?

SPALDING: Well, if you take - four of the largest banks in the world are Chinese - you take Alibaba, Baidu and Tencent, take all the consumer electronic manufacturing, you combine all that up, and you say, hey, if those gain dominance not only in China but also abroad, that gives them enormous power to move the needle. Now, you can - today, you can - China, because of its huge market pool, can influence U.S. corporations to do things they want, like fire their employees that say things about China that they don't like. Imagine a future where, you know, your products all of a sudden are - you notice that they're more expensive, and you notice that, you know, your kid didn't get into a certain school. That is a future that I see coming as multinational corporations lose their state kind of allegiance because of, you know, globalization and the internet. But you have an entire society of 1.4 billion led by 80 million that actually directs the entire corporate structure of the country towards a specific end, and that end is basically suppression of speech, suppression of religion and oppression wherever it meets into Chinese domestic law. In other words, Chinese domestic law always, in every case, in every jurisdiction, trumps international law.

SCHADLOW: Chris, do you want to...

CHRISTOPHER WALKER: So thank you, Nadia. Chris Walker at the National Endowment for Democracy. And really, thank you to the speakers. This has been incredibly thoughtful and illuminating discussion on a very complex topic. I think what I would say is the - it sounds to me like the 5G network discussion is of a piece with the larger challenges that have emerged in recent years. And I'd put it this way. We've had what I think is unanticipated systems competition. In this case, with China, which has a state-driven approach to the world, it sidelines nongovernmental actors. It seeks to control expression. And it brings all of the instruments of the state, which are quite formidable, to this end. At the same time, we have enormous systems integration and intersection in ways that were really unimaginable during the Cold War, just in the depth of the intersection of technology, media, information more generally, culture, education. You can go down the list. And I don't think we really reckoned with this. And we kind of sleepwalked into it, and now we're in the middle of it. And the 5G may be the most acute aspect of this. And I think the discussion also reflects that there are no simple solutions.

I think what I and my colleagues have focused on is what all dimensions of democratic societies can do to respond to this, not just at the official level, but also our nongovernmental sectors thinking these things through and coming up with better approaches. I guess one question I would pose on this count - and I think either Nadia or Rob alluded to this - we've looked at developments both in places like sub-Saharan Africa and Latin America. And there, there are any number of countries that only have Huawei and ZTE operating within these systems, some of them young democracies, open systems. They now control the technical chokepoints. They've also invested hundreds of millions of dollars into media content through CGTN and Xinhua Radio China International and so forth. So you have both the technical infrastructure and, to a large degree, the kind of media content infrastructure with, at a minimum, a privileged hand by a power that doesn't respect free expression and seeks to suppress it. So I just wonder in the - you know, in the larger picture, when we think about allies around the world in open societies, what we should be doing in the near- to mid-term to make sure that they don't get so far into this - they're probably up to their waist now, heading towards their neck - how we extract them, in a sense, from what is, I think, a pretty tough predicament for their own systems integrity.

SCHADLOW: Thanks, Chris. Do Harold or Rob - do you want to comment?

SPALDING: Well, we spend $800 billion a year on defense. So this would seem to be one area where we could spend a little bit of that money on. I agree we're not going to get much with leverage. Huawei has a great strategy. They are proceeding on that strategy. I think they're fully supported by the Chinese state. And so to expect that, you know, we can blunt that just by going around and having, you know, diplomatic discussions - I don't think that's - it's just not - it's not feasible. It's not possible. It needs a more coherent strategy with regards to, you know, what is a vision for the future? And then we actually have to put resources toward it. We have to put minds toward it. We have to put money toward it. And we have to think about it in a very thoughtful way and then go out and do it.

SCHADLOW: Thanks, Rob. There was a lady - yes, up front. Yes.

LI YUNG: Thank you. Thank you for your presentation. My name's Li Yung (ph). It's very important about high-tech. And I think, for the past several decades, the high-tech is really improve a lot. But I think on the other hand, if you think about United States, everything is going backward to what I am concerned because productivity is not based on what they can improve to improve the people's well-being or security. Instead, it's a profit over people. And it's our (ph) government hiring people. A revolving door is basically - is used unfair, just on a (unintelligible) method to reduce the productivity of high-tech or improve that hacking or spam. The whole thing is turned really upside down. So I just wondering, you - how do you ask a government really insist on the productivity rather than a lot of things that is going backward? You can hire people (unintelligible). It's fine. But problem is that you see the people, let's pry (ph), then go to change the people data or go to change your government employment data and then ask the people who are capable to do things to become unemployed. You see a lot of people unemployment on a street, and they are so unhappy about our government. So can you do something about it to see just how much they'd work on fixing the spam and hacking?

SCHADLOW: I think we - yeah. We can do a quick answer to the - that's a - maybe a broader question. But do you want to comment, just briefly? I mean, I think, essentially, we're talking about technology and changing our manufacturing base. But I think...

YUNG: I think the technology there, but government are not doing that. They are not hiring people to do the right thing on the right direction (ph). Instead, they're going the backward.

SCHADLOW: Thank you.

YUNG: So...

FURCHTGOTT-ROTH: Thank you.

YUNG: Just, of course, it will cost a lot, but economy benefit.

SPALDING: So I mean, one of the things that - the way I would answer that is - and this is in the National Security Strategy, and we thought about it - you know, the idea that democratic principles and free market principles go together is enshrined in the Atlantic Charter. It's in the U.N. Charter. It's in the same system that was conceived of after World War II. And what we've allowed here is a mix of free market principles and totalitarianism to kind of seep in and kind of corrupt some of that really close-knit tie between democratic principles and free market principles. For the most part, our allies and partners - our democratic allies and partners - abide by the international rules of the road. We don't have problems with trade. They're 85 to 90 percent compliant with the Container Security Initiative, for example. I would say that China currently - the data shows 20 percent compliant. I would say they're probably not compliant at all. So it's - to the extent that we want to actually put those two together - democratic principles and free market principles - that I think you'll start to unleash some of the innovation that we've lost because we've allowed it to be corrupted.

SCHADLOW: Thank you. Next question. In the back - you, in the black shirt, right here - thanks - lady. And then I'll - sorry. I'll get you next.

DIANE KATZ: Thank you. I'm Diane Katz with the Heritage Foundation. Many of these discussions focus on hardware. And obviously, that's not where the U.S. strength is. But I don't hear as much discussion about our ability to defend and protect through software, which is where we do, you know, surpass others. And yet, the U.S.'s own government IT system is a mess. And so I'd like to hear from the panelists why we're not putting more focus - you know, rather than on the, you know, boxes - Huawei boxes - rather than on the defense through software.

SCHADLOW: That's a good question. And I think also, then, the relationship between hardware, though, and security - right? - because I think early in the conversation, there was an effort to talk about that.

FURCHTGOTT-ROTH: Let me make a couple points. One, when we speak of the network equipment - network equipment really is, largely, software. So, yes, there is a physical Huawei box. But the real intelligence is in software, both inside the box but really at a network operating system. So a lot of this is software-driven. But you're right. The United States really is not a hardware manufacturing - we don't have a lot of hardware manufacturing that goes on in the United States. We are a software-driven company. We have lots of wonderful software-oriented companies in the United States, whether it's Microsoft or Oracle or any number of other companies that are software companies. And they are very important companies. And a lot of the Internet is going towards cloud computing, in which - the United States is, today, one of the leading sources of technology on cloud computing around the world, which raises a whole set of other security issues related to that as well. But you - please don't leave the conference thinking that there's no attention being given to software issues.

SPALDING: Yeah. And I would say, you have to look at the entire thing. It's a hardware layer. There's a software layer. There's a data governance model. All of those contribute to - and then there's a network switch. All of those contribute to the vulnerabilities that we have today. So you can't just go after any one. I will say that the CPU environments - it's a poor design, from a security perspective. It's really not something that can be secured. It wasn't designed to be secure. It was designed for speed. So everything that we've had, in terms of our - the evolution of our systems, have been designed for speed and connectivity, openness. OK? So going back and then trying to go back through that data governance model, software stack and hardware layer, and secure it - it's a failed endeavor. So you have to go back and you have to rethink the entire ecosystem and how we would have a different way of looking at it. Now, do we manufacture most of the hardware in the world? No, but we're actually pretty good at designing new hardware that can meet some of those criteria. So you know, my suggestion would be, we design it and then we begin to think about a coherent system that actually looks at all those areas and tries to come up with a foundation for our future that's secure.

SCHADLOW: That's what you talked about, too, in some of your writing - building it in...

SPALDING: Yep.

SCHADLOW: ...The security. Thank you. And then, yes, you had a question up here, up front?

KIM HART: Thank you. To follow up on that point about the different layers of the Internet - sorry. I'm Kim Hart from Axios. I have heard some people speculate that if we're looking at the challenges that you've all - that you've been elaborating on this morning and looking at both how - the data governance, how data is flowing across borders, the hardware itself, as well as the sophistication of software and how it all works together with the cloud. Is there a world in which, maybe not technically speaking but sort of geopolitically, we're looking - we're going to end up with maybe more of a fractured Internet, whereas an internet that is currently very broad and connects the entire world will be more determined by - the borders of which will be more determined by sovereign players than it is today, and is that good or bad?

FURCHTGOTT-ROTH: We're there already. We're there already. China is pretty much a closed Internet system. The Internet systems in other totalitarian states are very closed as well. It's possible and used a lot, unfortunately, for governments around the world to have chokepoints on information entering and leaving their country. And the concept of the Internet as this global information highway has developed into a global information toll road with checkpoints at different places. I guess I'm a bit of an idealist. I think it would be better if we had the global information highway rather than just a lot of chokepoints.

SPALDING: Yeah, and I think, you know, there is a country that's building a global information highway, and that's China; it's called the Belt and Road Initiative. There's a land component. There's a sea component. There's a digital component. It's called the Digital Belt and Road. And so, you know, they - now I think Huawei has built out 50 percent of the undersea cables. When you add in all the dominance around the world in 5G, and they're running fiber in all these countries that they're putting infrastructure projects in. You know, there - so there is a coherent system coming together; it's a system that's based on sovereignty, it's based on suppression of speech, it's based on, you know, controlling what you do in the digital world. And so, you know, the answer is, are we going to stand up and have an alternative view, and then how do we convince Democratic allies and partners to adopt that view in a way that preserves our collective freedoms?

SCHADLOW: And I think to add - I mean, the irony of some of this also is that some of the money being raised for these initiatives are being raised on - you know, Western capital markets.

SPALDING: Right, our retirement funds.

SCHADLOW: So there's also a whole - you know, a whole other element as well, but that also gives you...

SPALDING: Brilliant.

SCHADLOW: ...An example of opportunities in which, you know, even understanding the nature of those relationships is a first step toward perhaps changing things or at least understanding where...

SPALDING: Yeah, and you probably didn't know you're invested in your own impression.

SCHADLOW: In the back, the gentleman - red tie.

GEORGE FOLSOM: Thank you. My name is George Folsom, Institute for Political Risk Management Studies. We all saw the Bloomberg articles regarding Super Micro. And the technology press excused it, said that it actually didn't happen. There's a Ph.D. information technologist, by the name Weaver, at the University of California at Berkeley, however, who said that indeed, it actually could have happened. And from his perspective, what needs to happen is a relocation of what he characterized as the trusted base of our information technology infrastructure back to being manufactured in the United States. He actually advocated repatriation of if, not the entire - in other words, you wouldn't be cutting China out from the entire supply chain but just repatriating your trusted base. Do you all have an opinion about that?

FURCHTGOTT-ROTH: Well, there have been initiatives, and there is one right now on security supply chain. And it's a difficult problem in a lot of ways. You can't just relocate manufacturing bases that are largely based in China now and relocate them somewhere else. Having said that, there are things that we can do at the margin, and we do have - at the margin, we do have some forms of manufacturing capability for certain things. But for large-scale things, for mass market devices, I think it's going to be very difficult to move that anywhere but low-cost manufacturing locations.

SPALDING: Yeah, I think if democracy has made a concerted effort to focus on this as an issue, there is enough market pull both in the United States and the rest of the free world - the EU and all of our democratic allies and partners in Asia - to actually create enough of a market to, you know, rethink our supply chain for secure microelectronics. So this is, you know, basically, the government - the free governments of the world basically taking a hands-off approach to where they get their hardware. They can - we could come together and say, hey, we're going to build this capability, and we're going to protect it, too, because it's important to us as democracies. You know, there is an element to be said. We're not talking here about centrally controlled economies; what you're talking about is focus on an area that's extremely important to our future and saying, we're going to have a say in this. You know, there's numerous examples where, you know, U.S. manufacturers in one industry or another have faced enormous competition from a manufacturer abroad that was bound and determined to destroy their market share in the U.S. I'll tell you - give you one that's going on right now - rail manufacturer in the U.S. The Chinese basically blew out the Australians. There is no rail manufacturers in Australia anymore; they're all Chinese. And the same thing's happening here to our own system. Now, they're doing that in an industry where, you know, there's 50 percent utilization of their current manufacturing space. So tell me what business model actually makes sense in investing in that market, unless you just intend to wipe it out.

FURCHTGOTT-ROTH: Let me illustrate some of the challenges, though. You take a handset. There are roughly a thousand different components in here - roughly a thousand - probably 700 are manufactured in China by a lot of different companies. So the security to supply chain is not just one company. It's not just one manufacturing company, it's not just two manufacturing companies; it's hundreds of different manufacturing companies. And right now a lot of that manufacturing base is in China and kind of - it's one thing to relocate one company or one line of business, maybe two, but to relocate hundreds, it's very difficult. And at the end of the day, you're still going to be dependent on a lot of components coming from China.

FURCHTGOTT-ROTH: OK, the gentleman in the red sweater. And then...

AUDIENCE MEMBER: Africa seems to be in the receiving end. We - most countries use 3G, and Chinese companies seems to be everywhere. I wanted you to make some comment about Africa and the influence of the Chinese, and if the U.S. are trying to do something. I was born in Cameroon, and if you - not long ago, because of protests and the president cut the Internet in a particular region for several months, and he was able to do that because the Chinese are very much involved in the country. So if you can make some comment about Africa. Thank you.

SCHADLOW: I think that, you know, the National Security Strategy did actually acknowledge that Africa is an arena of geopolitical competition. It raised the issue up as an important one. There's bipartisan support for understanding how this competition is unfolding. The BUILD Act, for instance, is a small step toward addressing - at least trying to address some of the One Belt, One Road issues in terms of providing American businesses with opportunities to do more investments in the infrastructure. So at the very least, I think there's a growing awareness, which, again, is a first step toward the problem. That doesn't mean we're actually solving it right now or working, you know, toward the concrete solutions that we need to. But I think, also, a first step is getting key African states to understand that they're a key part of this, too, and they're going to be making choices. But to Rob's point, we want to be able to provide them with alternatives, right?

SPALDING: Yeah, and I would say, you know, our former colleagues at the NSC absolutely get your point. And our focus on this - I would say the federal bureaucracy is probably the biggest ship with the smallest rudder in the history of mankind. And so national security said - strategy said we need to go in a different direction, and it's going to take departments and agencies a while to figure that out, and you're going to see in the coming decade or two decades, I would imagine, a whole series of legislation that comes out addressing this issue, a whole shift in the way we do foreign policy, we do diplomacy, we do informational exchanges, we do economic engagements. So, you know, I would characterize - we've got - you know, if - we have this bipolar personality in the federal government. We've got this really strong guy. He goes out and fights a lot. And then this other guy that's got the diplomacy, economic and informational, portfolio; he's kind of been asleep at the wheel, and he's been eating too many Cheetos. We need to get him exercising and out there, you know. And it doesn't help when we're constantly increasing our military arm, and we're not increasing our diplomatic informational and economic expertise. And so we need to get that guy off the couch and exercising and out there.

SCHADLOW: Harold?

FURCHTGOTT-ROTH: Amen. Sounds good to me.

(LAUGHTER)

SCHADLOW: No Cheetos. OK. I had - yeah, the lady in the back. OK.

AUDIENCE MEMBER: I'm working for a business around here in D.C. I just want to mention, in the beginning, that there's actually the world's first 6G summit taking place in Finland at the moment, in Finnish Arctic, actually. But my question - usually, the biggest threat to cybersecurity and other securities is the end user - so we all, human beings. So I would like to ask about your views. What kind of emphasis, or is there a need to put more emphasis on how to probably raise awareness or skills of the end users also, in regarding 5G and cybersecurity in 5G era. Thank you.

SPALDING: That's actually a great question. I'd like to take that on. So when you come out of your door each day, do you take it upon yourself to defend yourself? Are you basically protecting your neighborhood? Do you ensure that everybody else follows the traffic rules? That's essentially what each individual faces in the digital space today, right? They're on their own. And all I'm saying is the government does have a role into making sure that, you know, you can step out in a digital world that you can feel safe in.

SCHADLOW: And what that structure looks like. Harold.

FURCHTGOTT-ROTH: Look. I think you're right. There are a lot of threats related to cybersecurity. Some of them have to do with the end user. Some of them have to do with the network itself and the ease of sabotaging it. I frankly think that's the greatest concern with network security, is potential for sabotage. I'm less concerned about it for collection of information because there's massive collection of information on all networks in the world today. But the end user - and we've seen this. We see lots of - there are a lot of bad actors in the world. There are a lot of people who can easily be bribed to become bad actors. And that's just part of human nature, and that's not going to change, unfortunately. The way in which individuals use the Internet and just the blind acceptance that everything's going to be all right - I think that's a very big problem. We tend to, I think, probably put too much information on the Internet that a lot of times we later come to regret.

SPALDING: Yeah, and when we were working on this in the White House, you know, and I talked - spoke to a lot of engineers that build networks for a living, you know, I remember one particular meeting went almost two hours. And, you know, it's very hard for us to imagine a different kind of world than we live in today because this is the world we grew up in. But if you could imagine what that world would look like, that's what we need to build. And it was about two hours into this conversation when one of the engineers says, but we don't build networks that way. And I said, that's exactly the point.

SCHADLOW: And to your point, can we ask more of the private sector to start giving us some of those options and expectations that they have a role to play in this too? When you get into a car, you have certain expectations that the car is going to be built in a certain way so that you can, you know, there's - in a similar way, I don't know the exact answer, but I think it's a question that individuals can ask more and more and should get answers on.

SPALDING: Yeah, and how many times has an American been told, that's impossible, and they've gone out and done it?

SCHADLOW: So we had the lady in the green right up here. And then I'll get to you.

AUDIENCE MEMBER: So our topic today is competing perspective, but I'm wondering whether the panel would talk about cooperation. As you mentioned, like, a cell phone might involve hundreds of companies that needs cooperation. So firstly, is 5G cooperation between U.S. and China - is completely off the table in the foreseeable future? And secondly, will U.S. be OK for China to cooperate with other countries - especially, you know, U.S. allies? Based on recent trips of Secretary Pompeo, it doesn't seems like the U.S. is OK with that. So I'm wondering how the panel think about it. Thanks.

SCHADLOW: Thank you. Harold.

FURCHTGOTT-ROTH: I'm not quite sure I fully understood the question. But...

SCHADLOW: Is there room for cooperation, I think...

FURCHTGOTT-ROTH: Oh, is there room for cooperation?

SCHADLOW: ...In creating a 5G network and the role of - you know, how we think about cooperation, the U.S. and China in this endeavor?

FURCHTGOTT-ROTH: Look. I imagine there are discussions going on between the State Department and the Chinese Foreign Ministry all the time on a wide range of issues. Cooperation is always possible. I don't think we're there yet. I'm not privy to those conversations, so I just don't know. I mean, for now - for - really, for years, Huawei equipment has been banned from the major networks. Rob makes a good point. There is Huawei equipment in some of the smaller carriers out in rural America.

SCHADLOW: Rob.

SPALDING: Yeah, I would say until there is an effort to change this increasingly - increasing need to restrict speech, freedom of religion, and oppression in the People's Republic of China, that the idea that we would cooperate on something so foundational to our future success is really - you know, in my mind, it's a non-starter.

SCHADLOW: OK. First, yeah. There are two questions here, so.

AUDIENCE MEMBER: My question is, if you think about Huawei, they sign so many contracts with countries around the world that they have very kind of a successful business model or - that is supported by Chinese government. They supported - they created such of national champions by supporting them financially or even diplomatically. But for United States, how can we have a - some other strategy that can really trump this kind of business model or - (laughter)?

SCHADLOW: Yeah, I think that that's sort of what we're trying to raise in general at the panel. And we see sort of - not competing viewpoints, actually, 'cause I think you're - (laughter) in some - we're struggling, I think, with identifying the model.

SPALDING: We need a public-private kind of model that actually plays to our strengths, right? You know, today, businesses are incentivized to do what they do by our set of rules and laws in this country and by the way the federal government spends its money. We can change. Those can be changed. It's only to imagine for us to reset the landscape in terms of, what are the incentives? How do we spend our money? What do we want companies to make profit doing? They have to make a profit. That's the way our system works. And so how do we want to incentivize them to make that profit?

SCHADLOW: Harold.

FURCHTGOTT-ROTH: One thing that's different in this area than in something else - let's say, airlines or agricultural equipment - the firms that are competing for the contracts around the world typically are not American companies - Cisco, to some extent. But largely speaking, the major network equipment manufacturers are not American companies. And so it's not that we have a national champion in the same way that China has a national champion. But the countries that do have - that are not China are - it's Finland, it's Sweden, it's Korea. These are very important countries, but they're not - these are not the global influence countries, if you will. And so those countries probably do have their own system of trying to help their companies. But it's - for the US, it's a very different situation. It's not that we go in and sort of say, well, we're going to use OPAC and all kinds of government subsidies to help them. Well, wait a minute. No, that's - they're not our companies anyway.

SPALDING: Yeah, and if, you know, China came in and said, hey, we're going to buy Boeing, we're going to take it all back to China, we'd say, whoa, hold on a second. We want to have Boeing as a prime military contractor. So I mean, it's just - it is - you have to relook, in this country, what is the value of industrial policy? And how can it be done in a way that actually continues to promote our free market principles, but also protects the kind of key industries that we need for the 21st century?

SCHADLOW: And I would just say, I mean, I see Rob's point earlier on about American leadership. But this is not just an American issue.

SPALDING: Yep.

SCHADLOW: Right? I mean, this is - I mean, there's no reason why our allies and partners in Europe can't be at the forefront, helping to develop some solutions to these problem sets. And you know, why isn't that happening? Or to what degree is that happening, right? I think there was another question up here.

AUDIENCE MEMBER: I think that the approach we should take regarding privacy depends on what kind of level of threat - what level of threat regarding the 5G. And I think the threat of China has been underestimated for a long time in - especially in the United States. So I wonder, what is the ultimate goal or destination for China regarding 5Gs? So I don't know your perspective on China's purpose. So why they are moving so rapidly ahead to 5G issues? Thank you.

SPALDING: Yeah. I think, you know, just for me, personally, leave aside what China is and what the Communist Party wants to do. That really shouldn't concern us so much. Who do we want to be as a nation? I think preservation of the republic is probably paramount in everything that we think about going forward. It should be, how do we preserve our freedoms? How do we preserve the kind of society that we want to live in? We can answer those questions without looking at any other country. We can just look to ourselves. And we have everything that we need. And when we do that, we can look to all those countries around the world that's - that actually agree with the way, you know, we want to live.

SCHADLOW: Harold.

FURCHTGOTT-ROTH: I would say, from an economic perspective, that wireless technology has been one of the greatest innovations, probably in the history of humanity. It has literally helped bring communications to billions of people who, until 20 years ago, had no way of communicating beyond how far they could speak by voice. It has been profoundly important to the development of society in the past 20 years. And it's been very important to United States. Lots of - speak to young people today. What do they want to do? They want to go into high-tech. They want to go into startups. They want to develop some app. They want to do something related to this new industry called high-tech in the wireless sector. And that's all been a good thing. And we want to be sure that that remains in a competitive environment, in an environment in which Americans can play a meaningful role and an environment in which this new technology continues to evolve in a useful direction.

SCHADLOW: I think we have time for one or two more questions. The gentleman in the back.

AUDIENCE MEMBER: Harold, you talked about national champions, but earlier on, you mentioned that there were a lot of American companies that verged out or went out of business.

FURCHTGOTT-ROTH: Yeah.

AUDIENCE MEMBER: What can we learn from the experience - well, Nortel wasn't an American company. It was Canadian.

FURCHTGOTT-ROTH: Canadian. Yeah.

AUDIENCE MEMBER: Lucent. What...

FURCHTGOTT-ROTH: Lucent. Yes.

AUDIENCE MEMBER:...Can we tell about - what can we learn from the experience of American companies over the last 20 years in this sector? It wasn't Chinese that drove them out of business.

FURCHTGOTT-ROTH: No. Exactly. It's - look. Competition is - competition is mean and nasty. And it is not something that you can rest on your laurels. And you just always have to be efficient and looking for new ideas. And so we've gone from a situation where 20 - the business history of high-tech over the past 30 years is littered with the corpses of bankrupt companies that used to be at the cutting edge. And today, they're just gone. Competition has been great because what is happening at the same time is technology has just raced ahead. And the companies that don't, that cannot innovate and cannot do better are not going to make it. And these companies have also operated in a largely unregulated environment without a lot of government interference. And that's been a good thing. And in the United States, we have migrated to certain sectors where we are really, really good. And those tend to be software and customer interface, advertising, marketing - the Googles, Amazons of the world. We're really good at that. And we haven't been quite as good at kind of the manufacturing side of things.

SPALDING: Yeah. The only caveat I'd add to that is there hasn't been a lot of U.S. government intervention. There's been plenty of Chinese government intervention. So let's say that you go out and have a football game, and you bring eleven players and you're playing by the rules. And all of a sudden, the team that comes out puts 22 players out there. How are you going to deal with that? Where's the referee to actually make sure that we have 11 players on both sides and one team's not, you know, basically violating all the rules? Essentially, you can't say there has been zero government intervention. There's been huge government intervention. It just hasn't come from the U.S. government.

AUDIENCE MEMBER:...Before China became an important player. So that's, as Harold said, that's the normal competitive process that seems to have painted ourselves into a corner. But that's...

SPALDING: And I would say the Trump administration says, great, let's have competition. Let's have fair competition, where you bring 11 players and I bring 11 players. Let's don't let you bring 22 players in and then I bring 11.

SCHADLOW: I think also it's worth thinking about - and I don't know the answer to this question, but - where is the innovation, and the young engineers in Silicon Valley, where are they putting their efforts? Right? What kinds of technologies - technologies to make my life easier as a consumer, or technologies that affect some of these core areas that we're talking about? And I don't know the answer to that completely, but I think it's worth considering.

SPALDING: And I think 5G is going to be, actually, one of those great spurs for innovation in the United States, as long as we get it right. And there's kids that are going to come up with ideas that we haven't even thought of on the basis of this, you know, nationwide, secure 5G network. But if it doesn't get built, or if it gets built, you know, in a way where we're actually no longer sort of a technology leader, well, then we're left picking up all the pieces that everybody else designs.

SCHADLOW: So I think we're about time to end. We do have time for one final question, but - OK. Gentleman up front.

AUDIENCE MEMBER: Have we considered modifying the EIS contract, which the government uses to buy telecom services, to include things like supply chain security as part of that contract?

SCHADLOW: I think there are some changes in that area. Right?

SPALDING: They're talking about it.

SCHADLOW: Yeah. So thank you very much for coming. We see this, really, as the start of a conversation. I think it was a good start to a conversation. There are clearly several other areas that we can work on building on this, and I hope to see you in the future. Thank you.

(APPLAUSE)