Center for Strategic and International Studies

TRANSCRIPT

CSIS-Simon Chair in Political Economy

China's Digital Silk Road

EVENT DATE

Tuesday, February 5, 2019

TIME

10:30 a.m. EST

LOCATION

CSIS Headquarters, Washington, D.C.

FEATURING

Dr. Robert D. Atkinson
President, Information Technology and Innovation Foundation

Lieutenant General William C. Mayville, Jr (USA Ret.)
Former Vice Commander, U.S. Cyber Command

Emily Rauhala
Staff Writer, The Washington Post

Hirobumi Kayama
Special Advisor, Japan Ministry of Economy, Trade, and Industry

CSIS EXPERTS

Matthew P. Goodman
Senior Vice President; Simon Chair in Political Economy and Senior Adviser for Asian Economics, CSIS

Jonathan E. Hillman,
Senior Fellow and Director, Reconnecting Asia Project, CSIS

MODERATOR

Kate O'Keeffe,
Reporter, The Wall Street Journal

Transcript by superiortranscriptions.com

Matthew P. Goodman: Good morning, everyone. My name is Matthew Goodman. I hold the Simon Chair in political economy here at CSIS. Delighted to welcome you here to our humble abode for this event on the Digital Silk Road. We're delighted to have you. We're also delighted to have, as always, our big online audience. Nice to have you with us as well. Hope this isn't getting distorted because it's loud.

Matthew P. Goodman: So we are here to talk about the Digital Silk Road. And I'll introduce that in a second, and our – and our initial speakers, but let me just first do some administrative things. First, as usual, please turn off your phones, or at least mute them so they don't disturb the discussion. If we have any kind of security event, I'm your warden, or just follow me basically – obviously we can go down front, if that's appropriate, or there are emergency exits at either end here. There's an alley in the back. And the rally point is by National Geographic down on M Street. Unlikely, we've never had such a thing, so.

Matthew P. Goodman: And finally, let me thank our sponsors, JETRO, the Japan External Trade Organization, which has been a supporter of us for a long time, and really appreciate their support that enables us to do this kind of programming. And we really appreciate it.

Matthew P. Goodman: So, Digital Silk Road. This is, like, one of these terms that has just suddenly appeared out of nowhere in the last year or so. And now everybody is buzzing around it. And no one quite understands what it is. And so that's the point of today. We're going to try to understand a little bit more what we mean by the Digital Silk Road, and why it's important for the United States to be focused on it, and what we should be – how we should be potentially engaging or responding.

Matthew P. Goodman: You know, to the extent it's – you know, what's clear about it is that like much other hard infrastructure that's being built across the Eurasian supercontinent and beyond, part of the digital story is about laying down of fiber optic cables and satellites and other hard infrastructure that's supporting the information and communications technology business. But it's also – and included in that is the technology that underlies the – this telecommunications story, and particularly 5G, which we're going to hear about, I'm sure, today, and again has been in the news a lot. I'm sure that you all know something about that subject, but hopefully we'll delve into that a little bit more.

Matthew P. Goodman: You know, by – it's estimated in about five years about half the globe is going to be covered by 5G and over a billion people will actually be using 5G technology, maybe more. Nobody quite knows. So there's a lot at stake there. This story also, though, covers the notion of technology that's embedded in traditional infrastructure – roads, bridges, pipelines all have technology embedded in them. And I think that's also an important part of this story and I hope we touch on that as well. All of this provides a lot of opportunities. It presents risks. It produces a clear need for policy thought and discussion and policy responses. There are issues ranging from privacy, to security, to commercial opportunities as well, which is all part of this story. So we think it's an important story, and we're delighted that you think so enough to join us today. So we're glad you're here.

Matthew P. Goodman: CSIS has been doing a lot of work in this broad space. We have a project called Reconnecting Asia, which I think is advertised up here, which Jon Hillman is going to talk to in a minute. But we've been looking at this hard infrastructure story across the Eurasian supercontinent for the last two or three years and have this enormous database he'll talk to you about. We also are running, right now, a taskforce on global infrastructure, cochaired by former USTR Charlene Barshefsky, and former U.S. National Security Advisor Steve Hadley. We have a group of expert scholars, businesspeople and others who are looking at this story and what is at stake for the U.S., and how we should respond. So that's a big part of what we're doing. And stay tuned, we should – we're expecting to have a report out in mid-April. So please stay tuned for that.

Matthew P. Goodman: We're also doing related issues in digital – digital issues, digital governance. Actually, as we speak, there's an event downstairs on APEC and the digital governance. In the Simon Chair, we're going to be doing an event on March 4th on Whose Rules on digital governance, and the story around that. So I'm sure – and our colleagues, Jim Lewis and the technology program, does a lot of work in this space. And so CSIS is kind of all over this set of issues.

Matthew P. Goodman: So with the shameless advertising out of the way, I think my remaining duty is simply to introduce Kayama-san. Hirobumi Kayama is a senior advisor for Japan's ministry of economy, trade and industry. He's also director for JETRO in New York. He's been in the U.S. for many years, not just in this position but I was interested to see that he actually has an LLM from Columbia University and passed the bar in New York, which is an impressive thing to do. So we're delighted to have Kayama-san here to talk about a METI and JETRO perspective on this story, the Digital Silk Road.

Matthew P. Goodman: Kayama-san, please come on up. (Applause.)

Hirobumi Kayama: All right. So I have to turn the thing on. Yes. Good morning, everybody. And thank you very much for a very kind, you know, introduction of me, Matt.

Hirobumi Kayama: So today the – you know, on behalf of METI, Ministry of Economy, Trade and Industry, of the Japanese government, I'd like to share with you the METI perspectives on the Digital Silk Road initiative by China. I'd like to explore the potential U.S.-Japan collaboration on the digital aspect of Indo-Pacific strategy too. So in this sense, please look at this slide. Actually, this is an excerpt from the U.S.-China Economic International Security Review Commission 2018 annual report. We can categorize projects under the Chinese Digital Silk Road initiative into three. Number one, telecommunications infrastructure. Two, e-commerce offering. And number three, smart city projects.

Hirobumi Kayama: And today, assuming that hardware stuff is basically categorized into the first one, will be addressed by Jon's presentation and then following panel, so in this sense I'd like to focus on the second and the third pillars of the initiative, and stress the necessity and the urgency of public-private partnership among U.S. and Japan, given the technological leapfrogging situation in the emerging economies in Asia.

Hirobumi Kayama: Jerry Yang, cofounder of Yahoo, said in a recent interview, quote, "Southeast Asia enjoying high-speed growth resembles China 10-15 years ago. So-called digital leapfrogging, such as wide use of mobile phones or smartphones, without the

period of landline use develops more rapidly in Southeast Asia than in China," end of the quote. We have already seen that various types of digital leapfrogging in this region – such as e-commerce, riding hailing, e-payment. These and leapfrogging have dramatically changed ASEAN and Indian economies and societies.

Hirobumi Kayama: Look at this slide. People in the emerging economies of Asia are much more smartphone addicted than Americans and Japanese. Last year, the Indian smartphone sales surpassed the U.S. one. And Indian market becomes the second-largest market in the world. Besides the population, in these emerging economies have considerable optimism that new technologies offer more opportunities than risks. And more importantly relatively undeveloped infrastructure and then social systems have accelerated various efforts of problem-solving by digital technologies.

Hirobumi Kayama: For example, more than half population of Southeast Asia do not have bank account. And the public trust in the currency is not high. Due to these circumstances, e-payment service via smartphones have spread through Southeast Asia rapidly. In Thailand, 44 million people, around 60 percent of total population, have registered to prompt pay. This is an e-payment service promoted by the Thai central bank.

Hirobumi Kayama: Another instance of social program is traffic congestion. You might have experienced difficulties in grabbing a taxi in Southeast Asia. Ride-hailing service companies, such as Grab in Singapore or Go-Jek in Indonesia, have provided solutions to such circumstances. Grab, established in 2012, has increased its number of registered drivers from 100,000 in 2014 to 2.6 million drivers in 2018. That is 26 times as much. And in March 2018, Grab purchased Uber's Southeast Asian businesses.

Hirobumi Kayama: Now Grab is expanding its businesses – business domain to wider range of consumer and wholesale distribution and delivery services. Go-Jek, in Indonesia, has provided bike ride-sharing services in Indonesia, where you experience terrible traffic congestion. Now Go-Jek provides food delivery services, shopping agent services, and even cash accommodation services by bike drivers for consumers. Google invested in Go-Jek last year.

Hirobumi Kayama: As such, Asia is full of attractive and energetic entrepreneurs, with a belief that she or he can make the world a better place. We saw a rise of start-ups or sharing businesses in 2016 in China. And now we can see the same kind of boom in ASEAN and India. Those entrepreneurs have seized business opportunities by finding challenges that society or corporations faced and resolved the challenges with full use of digital technologies. In other words, Asia is hungry for technology. And facing with middle-income trap, even the governments in this region strongly advocating digital innovation as one of the pillars of their growth strategy.

Hirobumi Kayama: Now, many of my ASEAN friends admire China for its technologies, not the United States and Japan – nor Japan. This reminded me of an anecdote of Chinese culinary students in Tokyo. Recently, we have allowed top Chinese student to come and learn the Japanese food cooking in Tokyo. Almost all of them yearn after old days of China, because almost all Japanese still use paper currency and coins, and our menus at restaurants still written in paper, and they're unchanged frequently. So look at the Chinese big IT platforms activities. They take this rapid leapfrogging changes in Asia as new business opportunities and seize them ahead of us. While

Chinese government promotes Digital Silk Road initiative, Chinese private companies have taken the lead in materializing concrete projects.

Hirobumi Kayama: In addition to building telecommunications infrastructure, Chinese tech giants have accelerated their efforts of expanding e-commerce offerings and supplying smart-city projects. From leading Chinese companies – for the leading Chinese companies in digital space, such situation in emerging economies of Asia is just like what China had experienced before. And thus, they must be quite confident that those economies will eventually successfully develop digital economy, like China. Thus, Jack Ma, the founder of Alibaba, recently told, quote, "We think that e-commerce and the internet are a great opportunity in Asia. And we go to places with – countries with young people, countries that have lots of small and mid-sized companies, because big companies, they don't like – they don't need us," end of the quote.

Hirobumi Kayama: In fact, in last year Alibaba provided the city of Kuala Lumpur with its City Brain service for the smartization of Kuala Lumpur city. City Brain service uses big data and AI and Alibaba's cloud computing infrastructure, which is adopted by the city of Hangzhou, the hometown of Alibaba, city in China. This is the first case of these services being provided for foreign country.

Hirobumi Kayama: And then IT platform businesses in Asia have grown rapidly, and in Chinese IT platformers, based on various types of IT platform businesses in this region. In ASEAN, there are seven unicorns – such as Grab or Go-Jek – and they are competing each other. All of the seven unicorns are injected equity by Chinese tech giants, such as Alibaba, Tencent, and DD (ph). In India, there are also 12 unicorns, such as Flipkart, which Walmart acquired last May. Seven out of 12 unicorns have received Chinese tech giants' equity investment.

Hirobumi Kayama: Alibaba and Tencent provide various services covering various consumer life domains. These have given them outstanding opportunities and capabilities of collecting wide range of data. Funding power of Chinese entity is not the only strength of them any longer. The U.S. and Japan must face up to this reality. And we also have to note that the leapfrogging technologies in Asian emerging economies are not just copycat of U.S. or Chinese e-commerce businesses. Those technologies have developed in a manner which we had not even thought of, and a different environment, and different social settings.

Hirobumi Kayama: Indian company, OYO Rooms, established as a bargain hotel chain in 2013, has grown up to be one of the biggest hotel chains, with 450,000 rooms in total. Even the price sensitivity of the market – Indian market – the company hires more than 700 AI engineers and then changes its room charges 4,300 times a day. Taking advantage of the system, the company has fostered in the Indian market, the company plans to expand its businesses to China, U.K., as well as Japan. And I also would like to draw your attention to the fact that Grab and Go-Jek are now trying to play a key role in realizing inclusive growth or indigenous growth in their countries.

Hirobumi Kayama: For example, Go-Jek's business model itself facilitates income redistribution. From its customers, higher income layer, to drivers and small merchants, the lower income layer. Grab launched an accelerator which provides capital for startups business expansion and lets them use Grab's platforms for doing businesses. So we

have seen strong wants and wills in emerging economies in Asia, making me believe that for the United States and Japan providing funds, technologies, and market for such problem-solving businesses in Asia might be a new regional strategy as part of Indo-Pacific strategy.

Hirobumi Kayama: Recently you can see some Japanese companies which noticed such dynamism of digital businesses in Asia, found business opportunities there. For example, last year Toyota invested in Grab, and Aeon – one of the biggest distributors of Japan – launched a business collaboration with Go-Jek by linking its shopping malls and Go-Jek's delivery services. And even successful IT platformers in Asian emerging economies – such as Grab and Go-Jek, are advancing to a different stage where they need to introduce deep technologies of AI or IoT.

Hirobumi Kayama: We heard from one of the executives of those companies, quote, "We would like to avoid giving a handle of our nervous system," that is, AI, "to a big Asian nation. We feel scared of them taking data of our businesses by the nation," end of quote. So there are real needs in the emerging Asia for active participation of U.S. and Japanese companies in digital transformation, and their collaboration with local IT platformers. Such contribution to the regional growth is essential for building a free and open data distributions place in this region, with more – with about 600 million population in ASEAN, and 1.3 billion of India. Otherwise, a harmful digital protectionism, such as data localization, could spread around the region.

Hirobumi Kayama: And actually Prime Minister Abe launched a concept of data free flow with trust at the World Economic Forum in Davos. We believe that U.S. and Japan should work together in expanding our investment in Asian problem-solving digital businesses and facilitating free and open innovation in order to materialize this concept of data free flow with trust. So what the government could do in this area?

Hirobumi Kayama: As you already know, the U.S. and Japan agreed to collaborate on the digital aspect of Indo-Pacific strategy in addition to the infrastructure and energy aspects. As to the digital aspect, of course the security of next-generation telecommunications infrastructure – such as 5G networks or submarine cables – is one of the very important agenda of the U.S.-Japan cooperation. But at the same time, U.S.-Japan joint engagement in the problem-solving digital businesses in the emerging Asia is also essential.

Hirobumi Kayama: So needless to say, the private companies should play leading roles in these efforts. But simultaneously, governments should play effective roles in providing a sound environment where private companies can enjoy free and open innovation. The rapid expansion of the fourth industrial revolution has also rapidly increased speed of business cycle, size of businesses, and risks associated with them. Thus, we have to recognize the necessity of securing risk money for supporting rapid digital innovation in Asia, while avoiding harmful crowding out. In the United States, the BUILD Act will strengthen the risk money provision function for its private sector. In Japan, JBIC, Japan Bank for International Cooperation, has strengthened its equity financing function and contributed to accelerating digital innovation in Asia.

Hirobumi Kayama: The U.S. and Japan should pursue a further strengthening and effective coordination of such policy-based financing. Besides that, we have to undertake an international rulemaking regarding trade, e-commerce, investment, technology protection, privacy, infrastructure development, which can accommodate rapidly-

changing business environment caused by digitalization and globalization. The concept of data free flow with trust is one of the important pillars of this international rulemaking. At the same time, U.S. and Japan can work together in capacity-building efforts in the emerging Asia for proper implementation of those international rules.

Hirobumi Kayama: In conclusion, again, we are very much confident of the effectiveness of the U.S.-Japan Indo-Pacific strategy cooperation in the areas of energy and infrastructure. Now we have to expand such effective collaboration into the area of digital innovation in Asia. Thank you so much. (Applause.)

Jonathan E. Hillman: Good morning, everyone. I'm Jon Hillman, director of the Reconnecting Asia Project, which is what we keep advertising here. And I'd encourage you to check it out if you haven't already. For almost four years now, we've been mapping infrastructure across the Eurasian supercontinent, tracking not only China's Belt and Road, but also many of the other connectivity initiatives that are underway. And you can view a lot of the projects that we're tracking on our website, where we also have news and analysis. One of our recent reports was being handed out earlier. Hopefully you got a copy. And if not, it's on the website. It's called Influence and Infrastructure. And it basically tries to lay out the ways in which states use infrastructure projects to advance strategic objectives.

Jonathan E. Hillman: And while the report is intended to help serve as a guide for making sense of current developments, it draws from examples throughout history. And so what I'd like to do briefly this morning is share one of those examples for you. But let me start first by underscoring what's relatively new. And that's China's rise as a leading provider of infrastructure beyond its borders. So let's just, for a minute, consider one type of telecommunications infrastructure, which are submarine fiber optic cables. I feel like that doesn't get a lot of attention right now. We're all concentrated on wireless networks. But these are incredibly important. They carry the vast majority of international data. And a decade ago, Chinese companies were involved with just a handful of these cables. And those projects were almost exclusively in China, Taiwan, or Hong Kong.

Jonathan E. Hillman: And as you can see now, China's share is growing quite dramatically. It's a landing point – China's a landing point, owner, or supplier for 11.4 percent of these cables globally, and more than twice that – 24 percent – of planned cables. The share is, as you might expect, even higher in Asia. You know, almost 30 percent of existing cables and over half of planned cables. One of China's planned cables in Asia is a project maybe some of you have heard of. It has a clever acronym, which I'll let you figure out. And it went into production last October. When completed in 2020, it will become the shortest route for high-speed internet traffic between Asia and Africa. The cable will begin in Gwadar, which as some of you know is a key part of the China-Pakistan Economic Corridor, which is a flagship – probably the flagship corridor of China's Belt and Road.

Jonathan E. Hillman: And what's striking about this project, among other things, is how this cable and several others like it are literally retracing the steps of great powers that came before China. So a century and a half ago, Britain was wrapping the world with telegraph cables, including one through Gwadar on its way to India, which was Britain's prize colonial possession at the time. And while every historical comparison has its limits, I think this case illustrates how what begins as a

commercial contest can quickly become a strategic contest. And I think it's also worth noting these cables, while a bit slower, they were cutting-edge technology of the day.

Jonathan E. Hillman: So in 1865, sending a telegram from Britain to India took five to six days, and it involved up to 14 relay stations. At each of those relay stations, the message was received, decoded, and then physically transferred to someone else who coded the message and sent it onto the next relay system. And so this was, you know, quite difficult. Sometimes messages are arriving mangled. And sort of an international game of telephone, before the telephone. And it was quite expensive to play. A 20-word message cost the equivalent of around $800 today.

Jonathan E. Hillman: These early – these early communication infrastructure types were also plagued by design and operational challenges. In the telegraph's first few decades, there were no international standards and wires were being produced according to various specifications. Engineers were basically, though trial and error, still figuring out what materials were best for different climates, and how to protect wires against common threats, ships anchors, and stormy seas, and so on. The first cable to India was laid in two sections. And both failed, leading the British government dependent on a connection that ran through the Ottoman Empire, and that was therefore vulnerable to being monitored.

Jonathan E. Hillman: And frustrated by that experience, the British government decided to provide limited support for surveying new routes, for negotiating access, and for laying a set of strategic cables. In the meantime, Britain's global share of telegraph cables was expanding rapidly. And that was driven primarily by commercial motives. British firms had laid the first – the very first cables in the 1850s. And their innovative materials and techniques eventually dominated the market – so much so that Britain's largest telegraph company manufactured two-thirds of the cables used in the 19th century, and almost half thereafter. And 1896, Britain owned 24 of the world's 30 cable-laying ships. So this is an illustration of one of their – the very first cable-laying ships. But Britain owned 24 of 30 of them at the close of the century.

Jonathan E. Hillman: Eventually, though, strategic concerns took hold. At the close of the 19th century, the British government began developing a smaller system of cables that touched only Britain and its possessions. And this network of all red routes was actually largely opposed by some within the British government – the treasury – but they were essentially out-maneuvered by Britain's defense agencies, which as the historian Paul Kennedy has written, developed a virtual fetish for these routes. These investments had little commercial value, but they paid off in the coming years as competition among Europe's great powers escalated and finally spiraled out of control.

Jonathan E. Hillman: And so for German officials, the guns of August were followed by a deadly silence. On August 5th, 1914, a day after declaring war on Germany, Britain cut five of Germany's telegraph cables, which remained disabled for the duration of the war. And so Britain's advantages in that conflict stemmed not only from owning and operating infrastructure, but also the abilities of its companies and the international standards they set, and in monopolizing much of the expertise to lay and repair cables, that ensured that Britain's rivals were unable to do so themselves.

Jonathan E. Hillman: So I think the story could end there. And it would be something of a cautionary tale about how commerce can quickly turn into a strategic contest. But I think the real story is a little more complicated. And so there are at least two other dimensions that I think are worth pausing on, just in conclusion. One of those is that the telegraph was ultimately a double-edged sword for Britain. So it solidified Britain's control over its colonial territories initially, but then eventually these same infrastructure types undermined that control. British cables did not only carry colonial commands, but also potent ideas for change. Especially in India, nationalist movements used these tools in their fight for independence. And Britain's censors were unable to stem the flow of news and communication.

Jonathan E. Hillman: The other dimension that I think is worth pausing on is that the source of Britain's commercial success as a global hub for communications was due in large part to its openness. So during the global telegraph race, unlike most countries, Britain granted rights for landing cables on its territory without restrictions. So far from weakening its firms, it was this openness that helped turn London into the global communications and financial hub that it remains today.

Jonathan E. Hillman: So collectively, I think these experiences suggest that while communications infrastructure can offer strategic benefits, those benefits indeed come with some unintended consequences, especially for those who try to censor and control information flows. These experiences might also suggest that limited strategic investments could be worthwhile, but that it would be a mistake to allow strategic concerns to fully eclipse economic fundamentals, which often provide the longer-term, more lasting benefits.

Jonathan E. Hillman: And so as I mentioned at the beginning, every historical comparison has its limits. This report that we just put out is filled with examples. And I think that as new as many of today's developments are, including with much of the new technology, they're perhaps not entirely unprecedented. So I'd encourage you to visit our site, to check out the report, and to help – you know, help us make sense of these developments, let us know what you think. And with that, thank you and let me welcome our panel onto the stage. (Applause.)

Kate O'Keeffe: Hi. Good morning, everyone. I am Kate O'Keeffe. I'm a reporter with The Wall Street Journal, covering U.S.-China issues. And I'm going to be your moderator for this panel. And I'd like to quickly introduce our panelists. To my left, we have Robert Atkinson. Rob is the founder and president of the Information Technology and Innovation Foundation, which is a think tank focused on science and technology policy. we also have Emily Rauhala. Emily was, until September, the Washington Post China correspondent. And she's now based here in D.C. covering foreign affairs. And at the end, we have William Mayville. Bill is the former deputy commander of the U.S. Cyber Command and a former director of the Joint Staff. So hopefully we'll have a lot of interesting discussion for you.

Kate O'Keeffe: I'd like to get things started with a more general question that I hope, Rob, you'll be able to take the first stab at this one. My question is: What are the key components of China's Digital Silk Road plan? And what is Beijing hoping to accomplish with this plan?

Robert D. Atkinson: Sure. Well, thank you, Kate. And thank you. It's a pleasure to be here.

Robert D. Atkinson: So I think what you have to understand about this plan is China has a strategy. Xi Jinping has said that the strategy is to be the master of our own technologies. And by that, they mean they don't want to be dependent upon American, Japanese or European technologies. They want to make all of their own. And when I say all, I mean all. And so the second component of Chinese strategy is what they call the going out strategy. And this is the idea that the first phase of indigenous innovation, which is sort of early – a little bit before Made in China 2025 – was really to sort of gain market share at home. I think about it as kind of a protected aircraft carrier. You've got market share. Sort of kicked Google out. Now they've got Baidu and they don't really allow Amazon in. So they have this protected market.

Robert D. Atkinson: The next step is to go out and gain market share. They're not going to go out and gain market share in the U.S., for a couple of big – or Europe, or, frankly, Japan, for a couple of big reasons. Number one, the technologies aren't as good. They give you pretty good technology at a discount. That's kind of the – that's kind of the business model and the deal. And secondly, they're facing robust competitors in those home markets. And now, thirdly, as we're seeing the last year, they're facing a lot of distrust and security concerns, and all that. So the core sort of phase where China is right now is to gain market share in sort of third markets, if you will, particularly Southeast Asia and Africa. And that's really what the Digital Silk Road is all about. It's to basically give them help, but tie that help to selling from Chinese digital companies – Huawei, ZTE, Alibaba and the like.

Robert D. Atkinson: So at one level it's good, because those countries need better digital infrastructure and digital services. But on the other level, we have to understand what it is. It's a pure – it's a pretty clear industrial policy play for them to gain market share for their companies. And then once they have that, which by the way means that U.S. companies don't have that market share, then the next step after that would be to try to go out and try to, you know, gain market share in Europe, the U.S., and Japan.

Kate O'Keeffe: Thank you very much. Bill, can I go to you for some of the military implications of this strategy by China?

William C. Mayville: Sure. First, let me back up and just say that today the only superpower that is – great power that is capable of deploying military might globally is the United States. No one can produce the type of joint force that is – the U.S. military can do. Now, increasingly in the past 15 or 20 years, the means by which we've been able to do that has become even more reliant on industry. Today, we are heavily reliant on partnerships within key verticals such as energy, the transportation sector, information, and technology sectors. And so for our ability to deploy and project power from our space into another space, the way in which we move it and the way in which we sustain it is largely in concert with the powers that reside at the homeland. So the home game and the away game are merged.

William C. Mayville: What we see here with the Digital Silk Road that China is doing is attempting to create an alternative system that will compete with that. The global telecommunication infrastructure is intended to connect countries under a single technology standard. And what that does for China is it gets – allows them not only to get in front of the global economy that will be increasingly more digital, it will allow them to – in addition to tapping new markets, it also allows them to set the

technology standards, the priorities, and to dominate. It allows them to overpower competitors at its scale. It preys on smaller economies. It gives them the tools to keep them under check. It creates dependencies. It gains access to data. And we have to remember, it does that with companies that are subjected to and must comply with domestic Chinese law. So you have a revisionist power emerging that is challenging fundamentally the way in which we underwrite global security.

Kate O'Keeffe: OK. Thank you so much. I'm going to go to Emily now for some more specifics. So, Emily, I wanted to ask you: How do Chinese telecoms companies, like Huawei and ZTE, fit into this Digital Silk Road plan? And what impact could the recent U.S. indictments against Huawei have on the company, and on China's broader plans to try to dominate global 5G?

Emily Rauhala: Sure. Well, first of all, thanks for having me. My notes are my phone. I am a Millennial, but I'm not currently on Instagram, in case anyone's wondering. (Laughs.)

Emily Rauhala: I think it's a really important and complex question. The first thing is when we talk about the Digital Silk Road, what are we actually talking about? And there's two levels here, right? One is, you know, the specific elements of Chinese industrial policy, which are, you know, laid out in various plans and are part of the Belt and Road initiative. And the second level is one that both my co-panelists have referred to, which is this level of strategic competition. So it's operating both in specific, concrete ways, and in broader strategic ways. And I hope we can discuss both today.

Emily Rauhala: In terms of concrete, you know, business operations, I think what we're seeing is that the Belt and Road initiative has just thrown a ton of money into this space. And so for specific companies, like Huawei and also for others, this means that there's contracts to be filled. And whether that means building telecommunications infrastructure, 5G, providing services in various local economies, that's really how they fit into this picture. And of course, the exact relationship between those companies and the government is a subject of much current debate.

Emily Rauhala: At this broader strategic level, I think we really have seen with the recent developments in the Huawei case the extent to which the Chinese state is going to back companies that are part of this. So for instance, if a country were to arrest the CFO of a large Chinese telecommunications firm on charges related to alleged sanctions violations, we would see a very forceful response from the Chinese government.

Emily Rauhala: In terms of what the indictments mean for Huawei and more broadly for Chinese companies operating in this space, it's too soon to know exactly but I think it would be hard to find someone who would argue that this has been good news for Huawei or, indeed, for other Chinese telecommunications and tech firms. What we've seen over the last few months is this sort of effort – I think, U.S.-led effort, that's fair – to rally members of the Five Eyes intelligence-sharing network around sort of the U.S. position on Huawei as a potential security threat.

Emily Rauhala: Huawei has been saying for years – I think quite fairly – if you're going to say we're a security threat, show us the evidence. And what we saw at that press conference

two or one week ago, I forget, was really the first time that we've seen what the United States Department of Justice plans to try to prove in court. They have not been proven in court, but these sort of meaty details about sneaking into labs and stealing robotic arms – which are allegations that have not been proven in court – I think are going to have a big impact on public opinion, particularly among Five Eyes nations.

Emily Rauhala: I'm covering Canada right now. And certainly in Canada the cost of the government going ahead with Huawei and 5G has just gone way up. But I do think it's important to note that elsewhere in the world the company is doing really well. And a really interesting question for the United States, Japan and for Europe is, you know, despite the U.S. raising all these security concerns about Chinese telecommunication firms, they continue to dominate in many markets. And so a key question for the United States is why this company is still so attractive, and why its services are still being popular.

Emily Rauhala: Yeah. I'll leave it at that.

Kate O'Keeffe: Thanks. If any of the other panelists wanted to respond to any of the issues Emily just raised, feel free. And then I also have a follow-up question, which is: What do you guys think are the main potential security risks with Huawei? And is there actually anything at this point that Huawei or China could do to convince skeptics that the company is actually not a security risk? So maybe we'll start with you, Bill, on that.

William C. Mayville: I'm probably the wrong guy to start with – (laughter) – because my answer is absolutely nothing. ZTE, Huawei is in the same category, Kaspersky Labs, the risks are borne of surveillance, cyberattacks, cyber disruptions. And so I'm firmly in the camp of telling our partners and allies that if you want to remain interoperable with us, you have to participate in an alternate solution. And we need to partner with them to figure that out. And we need to extend that, because I think economically what it does is it robs competitiveness in other markets, and it prevents emerging economies opportunities to participate in the global community. So I think in every category we should push very hard against what Huawei, which is a state-run enterprise, is doing.

Robert D. Atkinson: I can sort of jump in on that.

Kate O'Keeffe: Yeah, please.

Robert D. Atkinson: So a couple things here. One is there's another issue here besides security, and that's sort of global market share. The U.S. used to be the world leader in telecom equipment. We had Western Electric, which became loosened, and now we don't, which is a serious problem. But we don't have one. And so it's an interesting thing because we don't have a dog in the fight from a sort of industrial policy or competitiveness challenge. The Europeans have that dog. And that's Ericsson and Nokia. But if you've – who are the two sort of dominant players, if you will, outside of China.

Robert D. Atkinson: But if you just look at Huawei, Nokia, Ericsson, Cisco, ZTE, they have 75 percent of the worldwide revenue in this area. But in the last three years, Huawei's market share has gone up 4 percentage points, all at the expense of Nokia and Ericsson.

Huawei's telecom revenue now is twice as – is a little bit larger than Nokia and Ericsson combined. So they're a big company. They're also a unique company in the sense of in the U.S. we tend to have these sort of verticals. We have companies that make ships, companies that make computers, and companies that make phones, and companies that make telecom equipment. Huawei is sort of the integrator. It makes everything. And it'll be interesting to see whether that model really works. It seems to work pretty well for them.

Robert D. Atkinson: So that's one issue. I mean, you could imagine a world in 10 years where you really don't have any other choices. Where you get Ericsson and Nokia, you know, at a much smaller share of themselves and can – because the capital costs of R&D are so high for this industry, you know, you have to have enough scale to be able to keep innovating. And maybe you get to a tipping point where you just can't do that anymore. So I think that's one issue.

Robert D. Atkinson: The second issue, on security. It's not so much, I think, whether you can prove that things are secure or not secure. It's that the emerging systems are harder to judge, particularly as we move to what are called software-defined networks. Networks in the past, the functionality was all hardwired in. And now we're moving to what's called software-defined networks. And from talking to experts, software-defined networks are just much more vulnerable. That's not the right way to put it. Software – it's harder to determine on software-defined networks whether they've been compromised or not.

Robert D. Atkinson: I think that's the key thing. I mean, if you think about your car, for example, if you have a relatively new car, like a Tesla. The software gets updated all the time. Well, how sure are you? So you've approved that first set of software. You've gone through every line of code. But now there's an upgrade. How sure are you that that upgrade is legitimate? And so I think that is raising some interesting and important questions. I'm not going to judge whether they are inherently unsafe or not. That's what people in the U.S. government do for a living. But it does raise certain issues.

Robert D. Atkinson: And then lastly, on the 5G itself, because of the network architecture and typology, does also raise other sorts of vulnerabilities that are sort of the 4G network don't raise. And so I think, again, that is one of the reasons why the Five Eyes are thinking much more about this than they were in a 4G world.

Emily Rauhala: As to whether anything could convince people that Huawei's now safe, if I was advising the company I would give them the following advice. I would say, you know, rigorously defend yourself in court – in U.S. court. There's clearly a demand in the United States for more information about this company's corporate governance structure, its operations, and its relationship with the government. I would encourage the company to provide that information. And I think the company's response to this whole case has been revealing. They have said, you know, we'll fight this in court. We abide by relevant laws.

Emily Rauhala: So this also has to do with the Chinese government response, which has in some ways been much more forceful and, in some ways, much more revealing than the corporate response. If the Chinese government wants companies to see Huawei as a neutral actor, it should consider, you know, how the arrest, detention of two Canadians on big security charges is playing internationally and, you know, the

impact that that's had among, you know, the West broadly, and other allies, including Japan, on the willingness to do business with these companies.

Kate O'Keeffe: Yeah. Actually, Emily, do you have any other insights into what sort of the everyday Canadian thinks about Huawei now? I mean, was Huawei really on the radar of Canadians until this extradition request?

Emily Rauhala: It was a little bit on the radar, because they sponsor Hockey Night in Canada, which is our – (laughter) – most popular television broadcast ever, historically and currently. So they've really made this very successful, frankly, push into Canada, certainly relative to other markets including the United States. Huawei's made investments, research partnerships with Canadian universities. You know, they sponsor hockey. If you're walking around Toronto, you see ads for Huawei phones.

Emily Rauhala: I don't think the average Canadian before this played out, other than a large number of, you know, Canadians of Chinese ancestry or with ties to China, really knew about their products, didn't know much about their phones. So their first real introduction to this question is, you know, the detention of these two Canadians on the ground in China in what is widely seen as retaliation for Meng's arrest in Vancouver.

Emily Rauhala: And prior to this whole incident, the Canadian government had said: We're coming in, and we're going to engage with China. We shouldn't be afraid of China. We want to do more trade with China. And now they're being forced by public opinion to walk that back. And, you know, if that's not a lesson for, you know, companies like this, and for the Chinese government, I'm not sure what is – although, they don't show any sign of wanting to back down on this case.

Kate O'Keeffe: Yeah, it's definitely a unique PR strategy. So, Rob, if I could just follow up on something you mentioned earlier. You mentioned Nokia and Ericsson, and the fact that the U.S. doesn't have, really, an equivalent to Huawei. I'm wondering what countries – what alternatives countries actually have if they don't want to use Huawei. I mean, are these two Nordic companies going to just supply the entire world's 5G? I mean, how does that actually realistically work?

Robert D. Atkinson: I should also mention, Samsung is an emerging player in the 5G marketplace. And they're investing a lot and have, you know, very – what seem like good offering as well. So I don't – absolutely, Ericsson, Nokia, Samsung. There's no reason they couldn't supply the world market with 5G. They just build more factories. It's not hard to do. I think the question, I think, is much more about we up here – and, by the way, this isn't just about telecom equipment, as the other speakers alluded to. It's about e-commerce, search, a whole wide variety of new ICT business models. And generally the U.S. and Europe have not been very aggressive in that space, in that region. They really have sort of let Huawei and these other companies go out there and just take it.

Robert D. Atkinson: I mean, Huawei's an incredibly sophisticated company when they go to these places – Kazakhstan or these other countries. They go there, and they build relationships. They even have, like, scholarships for high school kids, or college kids to come to Beijing. I mean, they're very sophisticated. And I don't see American and European companies with the same level of response. And so at one level, we're getting what we deserve, because we're not doing it. And secondly, I think our foreign aid policy

– and particularly Europe, but also the U.S. – where are we? I mean, you know, you can say that the Chinese are putting, you know, unfair amounts of money in there, but they are putting a lot of money into that. And where are we? Why isn't AID or OPIC or the European Development Bank – why aren't they putting a massive, massive effort in there?

Robert D. Atkinson: And then secondly, tying it to commercial advantage. I mean, I know you're not supposed to say that in Washington. We're all supposed to be totally altruistic and helping them and nothing for ourselves. I don't think that world is real anymore. The Chinese have shown that's not real. And so if we're going to give them aid for telecom, they need to buy our equipment. And we don't seem to be doing that. And so at one level I'm not surprised that Huawei, ZTE and these other companies are making such important advances, because they're sort of pushing against an open door.

Kate O'Keeffe: That's a really good point. I guess we can give Huawei maybe a little break for a second. (Laughter.) And I have a question about another aspect of the Digital Silk Road, which is actually the very popular message app WeChat. And I wanted to ask you, Emily, what role does this app play in the broader Digital Silk Road plan? And also, what do you make of reports that the Chinese government is actually able to censor WeChat, well beyond China's borders?

Emily Rauhala: Thanks. I think understanding WeChat is really important, both in terms of, you know, the day-to-day use of the internet and also this broader question of strategy, and multipolarity, and how we think about the internet going forward. WeChat, as I'm sure most folks in this room know, is the Chinese messaging app. But it's sort of evolved into an entire online ecosystem. And it's hard to overstate just how popular it is. Whereas, in the United States, lots of people are using a variety of different apps. In the United – or, sorry – in China, almost everyone is using WeChat, from little kids to, you know, I've interviewed 79-year-olds who are doing all their online shopping on WeChat.

Emily Rauhala: And when we used to think about the Chinese internet, going back 2009, 2010, even further along, we used to think, OK, well, China's now developing an intranet. In 2009, the government sort of famously turned off the internet in the northwest after unrest. And that was sort of the framework we were using to understand the internet in China. What WeChat's sort of worldwide popularity among Chinese speakers in the Chinese diaspora and others has taught us, is that the walls of this sort of new Chinese online commercial, social, cultural ecosystem are much more blurry.

Emily Rauhala: To give one example, recently in a Canadian political race in British Columbia, on the west coast, a candidate was sort of forced to resign from the race after posting a Chinese language comment on WeChat that a lot of people thought was sort of racially divisive. And so this idea of different conversations happening in different online ecosystems I think is really critical to understanding. Another example: I've been reporting on the crackdown and mass internment of ethnic Turkic Muslims in China's Xinjiang province. And when we interview families of people who are currently in those camps, one of the most common things they say is their WeChat messages to their loved ones are either being intercepted, completely censored, and/or they are getting threatening messages on WeChat. So in really practical

ways, and in sort of really big-picture ways, it's changing how we understand China's online environment.

Kate O'Keeffe: Thank you very much. I wanted to know if any of the other panelists wanted to flag any other companies or specific technologies that are important for us to sort of keep an eye on as we're assessing the Digital Silk Road plans. And if I could throw that to you, Bill, please.

William C. Mayville: Yeah. Well, sure. The BDS navigation system is problematic, particularly when China's already demonstrated a willingness to militarize space. The sensors, the enhanced guidance, the dual use of this, in addition to everything it's doing in the cyber domain is problematic. I think anything that enhances, if you will – I don't know if this is the correct framework or not – but allowing China to have digital sovereignty in the region is problematic. I think we have to look at what enables and say: Why is that? And is that good for all of us? We have yet to see, but the promise of AI – 5G, AI. I'm concerned about when the infrastructure's in place, and then you see the introduction of internet application platforms and digital services, that kind of soft penetration.

William C. Mayville: So I think that it's what all happens downstream and how does this modernize – how does the modernization further enhance the grip of China in certain regions and across the globe. And my fundamental premise is that China is unfit to own large chunks of the world's communication infrastructure, and given its extensive surveillance, given its censorship, given the fact that it has for years been stealing property – intellectual property. You know, I just – it's just wholly problematic. So you know, I start with an inherent distrust of this actor. And I question the motivations behind all of its modernization because of this, you know, thing that I – you know, where I just think that they have demonstrated that they are willing to use this for the betterment of China, and not necessarily when it's not convenient for them to look at how this really impacts access to the global commons.

Robert D. Atkinson: So I think I would agree with what the lieutenant general said. I think 5G is going to be probably the most important one. I think there's a lot of sort of unwarranted paranoia about this. You know, whether they do well in 5G or not doesn't mean that we're not going to have 5G in the U.S. We will have 5G in the U.S. no matter what. The benefits of 5G are in the application space. And so we can buy Ericsson, Samsung, or Cisco equipment. It doesn't really matter. And we'll do well in 5G. So when everybody says China's winning the 5G race, I think they're missing part of the point. The point of 5G is just we're going to have a better network. And highly unlikely it's going to be a Chinese network at this point in time.

Robert D. Atkinson: I think in other areas, biometrics. The Chinese are going great guns in biometrics, particularly facial recognition. You can say what you want about facial recognition, but I believe facial recognition is going to be a very important technology going forward. It's going to make our lives a lot easier and better. But it's a complicated and expensive technology to develop. And the Chinese could gain global market share in that, and really, you know, be the sort of default provider in that space. And then lastly AI. AI – one of the key things that AI depends upon is data. And the Chinese have no compunctions about enabling large amounts of data to be collected.

Robert D. Atkinson: So I think those are the big things. I do want to argue, though, that I think we tend to, again, overly panic about some of this. When China goes and uses the Digital Silk Road, and there are incentives in other packages to convince some country in Southeast Asia to buy their equipment or to buy their cameras, or whatever they buy, it's important to recognize that the country that has those cameras or equipment is setting the rules and setting the law.

Robert D. Atkinson: It's not like China saying: We'll only – we'll only sell you Huawei telecom equipment, but you have to agree to spy on your citizens. China fundamentally doesn't care about that. They just want to sell the stuff. I mean, it's just – it's a commercial transaction. They spy on their citizens at home, but they're going to leave those decisions about surveillance and privacy and all those others things – those really are left up to the countries that are buying this stuff. And as far as I can tell, there doesn't appear to be any sort of arm-twisting based upon that we're giving you money and so you have to do that.

Robert D. Atkinson: What I think is more problematic is that countries are looking at China and going: Well, I like that model. I get to control my citizens. I'm going to do that too. But you have to remember, that's different than China sort of imposing that model on them. The problem is, I think that China is just something that a lot of countries not emulate, largely because, I think, of a failure of the U.S. to push back adequately to say that our system is better and gets you better innovation. But so I think it's – you know, those countries are still in play, in my way of looking at it. You know, we can influence them, and we should try to.

Kate O'Keeffe: Just a quick follow up. So you mentioned that you think there's a lot of undue panic, and that, you know, countries who are using Huawei equipment are able to sort of set their own rules. I think that is a controversial view. There are certainly some out there who believe that Huawei has backdoor access to its equipment. So I was wondering what you think about that. Do you think that's just fearmongering? Or is that a legitimate concern?

Robert D. Atkinson: Well, that's a different issue. Whether they do or whether they don't, I don't know. But that's not setting the rules. They're not – let's say – let's just say, for the sake of argument, that they have a backdoor. The government that they're selling this to, or the country they're selling it to, might have rules that say you cannot use backdoors, you cannot spy. So they're not forcing the country to change the rules. If they have a backdoor, that's something they would be doing surreptitiously, not in direct partnership with the government of a country, necessarily.

Emily Rauhala: I think I broadly agree. But this question of the long arm of the Chinese state, I think I agree that they're not saying: Buy our telecommunications equipment and then you have to spy on your citizens. But this sort of broader use of defining China's national state security across borders I think is really significant. In recent years, you know, I covered the case of a Swedish national abducted from his vacation house in Thailand and renditioned, mysteriously, to China. Then he shows up and says, you know, I kidnapped myself and took myself to China. I'm paraphrasing, but – and I think we're going to see this kind of – this kind of action in the digital space. And we already are seeing it in real ways among – in diaspora communities and among critics of the Chinese government. So I think that's – to me, that's where that plays in. But I agree broadly with what you said.

Emily Rauhala: One other point I wanted to make was that in the United States the response to all this is really being led by the security and intelligence community, which is very important, because I think it's very clear that there are real security and intelligence considerations here. But when we're talking about something as broad and as personal as the internet and how we interact online, from a strategic perspective the United States and its allies need to think about how and why people use the internet. I'll use myself as an embarrassing example. I know that WeChat is surveilled and censored. I've, you know, shown in small Chinese villages and had people waiting for me there, because I discussed plans on WeChat. I know it's dangerous. I know it's not secure. And yet, it's still on my phone. I do have a phone without it, for the record. (Laughs.)

Emily Rauhala: But what is the United States, what are other allies, offering as – product-wise – as a sort of alternative to this? If Huawei's telecommunication networks work really well and they're affordable, if their internet ecosystem, if Alibaba, if WeChat are really great internet experiences, people are going to use them, especially at a time when faith in U.S. technology is at, like, negative 10 billion. When I say to people, oh, you know, what about WeChat, it's surveilled? And they're like, I'm on Facebook. Whether that's fair or not, the current perception is that there's on some level an equivalence when it comes to using the internet. And I think strategically one consideration is, what is the response to that?

Robert D. Atkinson: So it's not equivalent. And the idea that people think it's equivalent – I know – (coughs) – I know you're not saying they think that, but the fact that anybody in the U.S. could think they're equivalent tells you they don't know what they're thinking about. Facebook does not sell its data to advertisers. When you advertise on Facebook, you don't get to know that it was you that saw my ad. I get to know – all I get to know on – and I'm not defending Facebook, per se, but they're so much mythology that's gotten in the last year of this tech-lash and this demonization. The business model is to match customers to ads anonymously.

Robert D. Atkinson: Secondly, Facebook, and every American internet company, does everything possible to resist the U.S. federal government from getting into their networks. Now, they obey the law. And if worst comes to worst, you know, push comes to shove, they will do it if there's a legitimate court order. But every single one of those companies has a big legal department. And all they do is they push back against the U.S. government, trying to get inside their – you know, with court orders to get inside their network, because they want to protect that. That was that whole Apple case with the encryption.

Robert D. Atkinson: Chinese companies do not do that. Anytime a Chinese company were to raise one little iota of complaint, they would be completely taken down. I always remember this meeting I had – and I won't say which company it was. It was a pretty major Chinese internet company in Beijing. And we're in there, a group of us. And I asked this guy a question. And, you know, some question about the government, or something. And he says, well, I'm really not allowed to answer that. Let me turn it over to the Communist Party official for him to answer. Can you imagine going out to Microsoft and saying, hey, what do you guys think about the federal privacy rules? I'm sorry, we can't answer that. Let me turn it over to the Department of Justice official. (Laughs.) So it really is completely different.

Robert D. Atkinson: And part of that I think get to this other point. I think we're really making – we're going to look back on this in 10 years and go: What in God's name were we thinking? Because the Chinese government is not attacking its tech champions. It's doing the opposite. It's doing everything possible to prop up its tech champions. What are we doing? We're demonizing these companies. We're bringing bogus privacy cases against them, sometimes not all the time. We're threatening antitrust cases against them. The Chinese government knows that the way they're going to win this is not by breaking up their platforms and their dominant players. It's to build them up. And we're going in the exact opposite direction, I would argue. And it's going to make it harder for us to project our soft power throughout the world, if we do that.

William C. Mayville: Yeah, I have a couple of thoughts on that. I struggle to understand, despite China's economic growth, this one-party system, how it survives promoting multinational capitalism. I struggled to understand that. I think there's an impending catastrophe between the state and the state's economy, unmet expectations of its middle class, global competition, unable to provide alternatives to the free-trade system developed by democratic nations. And if it has, when that moment comes, laid the infrastructure in place, and it goes unchecked, I think we find ourselves in a very difficult position to project power, to provide an alternate response.

William C. Mayville: And the difficulty we have here is cyber in general has enabled new forms of power – principally economic and political power. And we haven't yet come to terms with that. To the extent that it has application in terms of the traditional forms of military power, what we're really finding is that given that cyber today doesn't really generate anything more than temporal and limited concessions – that's what it's able to produce for military – there's no knock-out punch, it really means that for the defense – for military, you're on the defense. And what we have right now strategically is because of new forms of political and principally economic power, a way in which other nations and China in particular can compete with the current world order below the threshold of what would trigger a more serious response.

William C. Mayville: And we're not – we aren't in that space. The first briefer I thought did a great job on the number of folks that don't have banking accounts in the world. I think it's – like, the number in my head is like 2.2 billion today don't have banking accounts. And I could be off on that. What have we done to contribute to that? Well, just look at our de-risking operations as a result of our Patriot Act and war on terror. And what you find today is because of anti-money laundering regimes, and CFT requirements, and know your customer requirements. And the penalties after the fact to the institutions that allow a breach to happen has put a dampening effect on the financial markets. And we're not penetrating. And we are – this area, we're not penetrating the United States, we're not penetrating in the – in the global markets. And so what we do is we cede human terrain to these alternate choices.

William C. Mayville: So, yes, it is true that China is out there, and others are out there. But we are doing things in the physical world that made sense at the time that we developed them, that I think we have to rethink and ask ourselves going forward: Does this really – how do we need to adjust these various regimes so that we don't necessarily create new unintended problems.

Kate O'Keeffe: OK, thanks. I wanted to move onto the topic of data localization. Sounds boring, but it's actually very interesting. And, Rob, I was wondering if you could tell us how

you think China's requirement that companies store data within its border fits into this Digital Silk Road plan.

Robert D. Atkinson: Well, you know, data localization is a big, big deal. My colleague Nigel Corey is here, who leads our work at ITIF on that. If you're interested in sort of looking at the best work, I'd encourage you to look at Nigel's work at ITIF.org. We just issued a report last Monday called – I think it was, the Ten Worse Innovation Mercantilist Practices of 2018. (Laughter.) Really riveting. (Laughter.) But this year, China was, what, two or three, Nigel? Two. So two of the worst practices were from China, and they're both related to this.

Robert D. Atkinson: So the Chinese have this policy that says you have to store data – any data generated in China has to be stored in China. And they use this essentially bogus argument that if somehow data leaves China it's not private. Well, first of all, they really don't have a privacy regime anywhere, so it's probably more private if it goes to another country because they have better privacy. But the point being, it's a bogus excuse to essentially do data protectionism. And the reason they do that is they want to have the data centers and cloud computing and others kinds of – and other kinds of technologies, they want them to be in China. They don't want them to be out of China.

Robert D. Atkinson: So, for example, when you look at a company like Amazon Web Services, which is the largest cloud computing provider in the world, Amazon is not allowed under Chinese rules to go in and open up a cloud computing business. Yet, Alibaba is allowed to come into the U.S. and open up a cloud computing business. Amazon can't do – AWS can't do that. And they have to partner with a company – a Chinese company. And they have to have the servers – the center – the servers in there. And they have to give them proprietary technology.

Robert D. Atkinson: So I don't – as I said, I think that the Chinese – this is, to me, a completely unfair trade practice. We should bring a WTO case against it and we should force them to stop. I also am encouraged by Prime Minister Abe's leadership in this. Japan now is really – the U.S. is not the leader as much as we should be. But Japan has emerged as the leader now in trying to craft a new trade regime around open and cross-border data flows, which I think is going to be very critical going forward. China's going to be the big opponent of that, although recently they said they wanted to be part of that agreement, which is, I think, a mistake, initially, because they're not going to live up to it.

Robert D. Atkinson: And then the last point I'll just make on that is I think that they're not – they're not imposing this regime when they go into these countries. They're not saying: If you want to buy our equipment and get our aid, you have to have data localization. But they're encouraging it. They go to these countries, like Indonesia. I mean, Indonesia is close to being as bad as China when it comes to data localization. They have two new policies, I believe, in that space.

Robert D. Atkinson: And they're looking and going: Hmm. We want to grow our tech economy. We want to have all these companies. We want to have data centers. Let's just do what China did. And so, again, I think we are not doing a very good job of articulating what the costs are on that. We wrote a report last year where we looked at what the costs are economically to data center localization to domestic companies that have to live under that regime. And they're quite significant. But we don't really

promulgate that information adequately enough and go engage our allies and other partners to let them know that.

Kate O'Keeffe: Did anyone else have comments on that, or should we move to our final question? No? OK. (Laughs.) And so, right. I think we'll just do one last question for all the panelists to respond to, and then we'll move into the audience Q&A. So please get your questions ready. So I guess my final question for you guys is, broadly, how do you think the U.S. and its allies should respond to China's Digital Silk Road plan? And just a sort of prediction question, where do you see all this shaking out in the next 10 years? I think you already said, you know, we're going to be kicking ourselves, but if you want to expand on that.

Robert D. Atkinson: Well, I look at the world in a pretty Manichean way, or a zero-sum way, I guess. It's somebody gains market share, or we gain market share. It's not like the pie is fixed. I mean, it's not like the pie – the pie is fixed. The Chinese either get it or we get it – or the Japanese get it, or the Chinese get it. And so I think we should fight for every scrap of global market share in advanced technology industries. So when people say, oh, Google shouldn't go into China because they censor, fine. We'll let the Chinese companies have all that market share and get none of that revenue coming back to the U.S. to support U.S. companies. I think that's a major, major mistake.

Robert D. Atkinson: I mean, to me, this is largely about commercial competition because if we lose that competition – innovation industries are different. They're not like a call center. If you lose all your call centers and you want to bring them back, you can open them up in a couple of days. Just throw a bunch of servers in, a bunch of headphones, and train people on how to read a script. But if you lose your AI, if your lose your telecom equipment, if you lose advanced industries you just don't get them back. And the only way to ever get them is to do what China did, which is steal the technology and massively subsidize it.

Robert D. Atkinson: So I think that's really the main lesson, is we should just fight for every scrap of that. And that means – I agree with what we just did recently, where we put more money into OPIC. I think that was a good idea. But we still don't have an Ex-Im Bank that's functioning the way it should function. We don't have aid policies that are anywhere near sizable enough. We don't tie them to these kinds of things. So there's an awful lot we could do. I don't think – I don't think in 10 years it's a default that the Chinese are going to dominate that region from a digital perspective. But I think if we don't change course then, yes, I believe they will dominate.

Emily Rauhala: I think certainly the security response and the – what's happening in U.S. courts right now is an important part of this whole issue. As someone mentioned earlier, the United States right now is very focused on this being strictly a legal matter and not a matter of great power competition. I understand why they're saying that. I think it very clearly is a matter of strategic competition and spheres of influences. And so the thinking within policy communities needs to reflect that.

Emily Rauhala: Also, I touched on this earlier, by the best response from the U.S. and allies is to offer alternatives that are excellent. People don't use the internet based on who provides their network services. People chose the internet based on what is fun and useful and speedy. And the best thing that U.S. tech could do right now is, you know, clean its own act up and tell its own story better, so that people are going to

want to – going to want to choose to use products that are made here, or elsewhere, as opposed to Chinese products.

Emily Rauhala: And the fact is, China's engineering right now is awesome. Like, there's so much happening. There's so many apps that are amazing. The online experience is amazing. And this – the whole vibrancy of this market is lost in the – in the U.S. conversation about this. So I think going forward the U.S. and allies really need to work on providing an alternative that people want to use.

William C. Mayville: Yeah, I very much agree with what Rob and what Emily just said. In terms of economic, I think we need to have a meet and compete. We have great products. We have better products. Our system of business is underwritten by laws that the international community agree with. So an investment in a partnership with us is one that is dependable for you, should you have challenges down the road. I just think that we need to deploy that. But I also think we need to think, you know, innovatively here about how we want to protect our market advantage.

William C. Mayville: And for those – you know, as Rob said earlier – China goes into new areas and does, you know, wonderful things, such as offering scholarships and working with the community. But they also do bribes. They also work in nefarious ways, and they work outside the norms to maintain a foothold and then to exploit a competitive advantage. And I think that needs to be called out through tariffs and subsidies, and import quotas, and whatever it's going to take to address that, so as we are deploying our products and our – and enabling the reach of our economic reach, I think likewise we have to be attuned to where China exercises things that fall outside, you know, international norms, and clearly in violation of the way in which we would like all nations, including ourselves, to behave. And we need to put pressure on that.

William C. Mayville: I also would ask that we – I think another area that we need – and this is tangential to extending the reach – the economic reach of the West – is we need to go back and look at the political – how cyber – and this environment has enabled new forms of political power. And I don't think we in the West have done a very good job of challenging, as a way of policy if you will, political warfare in the sense that, you know, there's a lot that we could be doing to market our capabilities, to identify and make known where there are rules-breakers, and to provide feedback to countries that don't – that block that, so that – so that in addition to extending the reach of the economic arm, we are also using the political arm to help create expectations of behavior, and use that as a way to put pressure for those that seek to – mainly China and others – that seek to do something that I think disserves the global community.

Kate O'Keeffe: Thanks. I would like to add one serious deficiency with the Chinese internet, though, is people can't read our stories. (Laughter.) Which I know you very-well know.

Kate O'Keeffe: So thank you so much to all the panelists for your comments. And I think we'd like to move to the Q&A now. Please wait for the microphone to get to you. And then please identify yourselves before speaking, and then ask a question as opposed to making a statement, if possible. Thank you.

Kate O'Keeffe: Sorry, where are the mic, actually? Oh, they're there. Oh, OK. (Laughter.) Sorry. This woman in red, please. (Laughs.) That's a good idea, to wear red to a panel. (Laughter.)

Q: Thank you very much. Mariam Baksh from Inside Cybersecurity.

Q: My question is for the retired lieutenant general. There is a couple – not a preamble, but just a couple of notes. So you mentioned the defensive position – the inherently defensive position we find ourselves in, given the sort of intangible nature of the cyber realm. And then you also mention that our fate is sort of tied to the practices of private industry. I wonder how you feel about requiring private companies to institute those cyber best practices, versus, like, voluntary – having it be on a voluntary basis. Actually crafting regulations for patching or other sorts of best practices like that.

William C. Mayville: And let me make sure I understand the question, the idea that we would raise the standards of performance to meet baseline cybersecurity requirements?

Q: Yes. To the extent that you or somebody else would determine that, baseline. Yes. You use a tricky word, "standard." Because that standard is sometimes seen as something that people can do but shouldn't – don't have to do. I'm speaking specifically about regulations. But if you're saying that regulations might equal a raising of the standard, that would be noteworthy.

William C. Mayville: Yeah. Let me start. And, Rob, if I could ask you to help me with this. You know, I think I understand, which is – look, I do think there needs to be standards. And I do think that we need to, as part of our – if anything, not – to bring greater assurances to the trust envelope that I think is often lacking. And I think to the extent that we can promote that with partners and allies in the international community, and in partnership with the business community in the various verticals that are already in this space, I think that's a good thing. I think that would be – that's an example of where I think we can lead. That's the sort of thing that I think is exactly what we should do. I think there's a leadership component to that.

Robert D. Atkinson: Well, I think one place to start, there have been a number of stories in the last few months about how the Chinese have gotten virtually all of the data and plans and IP for major weapons systems, including submarines and fighter jets. And they got them not from the OEMs, but they got them from the suppliers. And I read something – I'm not going to get the number right – but a significant share of DOD suppliers are not using state-of-the-art cybersecurity practices. And why DOD allows this to happen? Maybe there are reasons for that, but to me, if I was running DOD, I'd say: You got, you know, six months to fix it, or else, and we're going to buy from some other supplier. I mean, these are pretty vulnerable systems. And it's not rocket science. I mean, you can make systems that are pretty secure. Or you can do stupid things, like have your password be "password." So. (Laughter.)

William C. Mayville: On that point, there was a GAO report that came out in October of '18 that said that it found that DOD's weapon system acquisition program for future weapon systems – about a $1.7 trillion portfolio – was deemed by them to be at significant risk to cyber threats. And the reason it was is for years and decades services who make the requirements and do RDT&E work on the part of businesses, were not – failed to heed the warning and to bake in those requirements. And so today, if you're to

believe the report. And I think there's – I think DOD would respond that it's not exactly that bad, but somewhere in the middle. If you were to look at that, and you say, well, why is that? Because we just didn't have standards in the acquisition process that you must build to.

William C. Mayville: And they can't – they can't be debated. You either do it or you don't do it. And if you don't do it, you don't get the contract. And we don't have those sorts of things in place. And I'm confident we'll redress all the problems that were identified in the report, but it's going to cost us more than it cost the current program right now. That's not right.

Kate O'Keeffe: OK. Can we get the mics to this gentleman in this block here, with the purplish shirt? Thanks.

Q: Hi. My name is Dr. Aqab Malik. I'm a Fulbright scholar currently at the Sigur Center, Elliott School.

Q: I'm going to follow on from what Emily said right at the end, when you were doing the session, and talking about the strategic power play between the U.S. and China, and the rise of China in that respect. I'm writing about this, so I'm particularly interested in this. So given that if we look at the Chinese perception of the way the world is – I mean, that's how you're going to be able to really fathom about how they're rising, what they're doing, and why they're blocking everything. That we can significantly say that Chinese companies are a strategic threat then. And because China's blocking access into their market space, especially in the digital realm, would we ever be doing that in the West? I mean, I'm a Brit, so I've got to consider that part.

Q: But in the U.S. as well. And given that's the case, over the last couple of decades, but especially in the last 15 years, the U.S., particularly, has lost a lot of access to future technology resources – for example, rare earth minerals. Afghanistan being one of those which you occupied for a long time and is still doing so. And the find in rare earth minerals there, to be exploited, which the Chinese are actively seeking access to. So given that this is the scenario of the next few years and the decades to come, and this is a significant power play by the Chinese, and this is just one aspect of that to compete in the strategic realm, what are the consequences or the potential likelihood of blocking complete access to Chinese companies in the U.S. as well? Will that actually occur or not? Because you're going to get it either way. Does that make sense? (Off mic.)

Robert D. Atkinson: Well, look, it's a little bit like somebody's punching you in the face and you say, geez, if I punch you in the face I've started the fight. I mean, you look for example – and I'm going to get the name of the company wrong – but it's – the semiconductor company. It's basically a DRAM company, a memory company, in China that's bankrolled completely by the Chinese Integrated Circuit Fund, $100 billion fund. They got about –

Kate O'Keeffe: Are you talking about Jinhua?

Robert D. Atkinson: Pardon?

Kate O'Keeffe: Jinhua?

Robert D. Atkinson: Not Jinhua, the smaller group. Fujian, I think.

Kate O'Keeffe: Fujian Jinhua, yeah.

Robert D. Atkinson: Yeah, Fujian Jinhua, yeah. Thank you. So they got, like, $3 billion or $3 ½ billion to build this ginormous DRAM factory. And the way they got their technology is they stole it. They bribed people who – in Taiwan to steal Micron technology. Luckily, they were caught. And the Trump administration did this very clever thing – like, one of the best things they've done, in my view, in this space – is they basically cut off their ability to buy the equipment that you need to make these things, these chips, because we have – we have enough. That's an area where we do have enough market power and we can do that. And the company announced two weeks ago they were going bankrupt. It was going to go bankrupt and close in April. And the quote I had in the paper was, "it proves that crime doesn't pay."

Robert D. Atkinson: So when – in my view, when the Chinese – when you have pretty clear evidence that the Chinese are doing that, we should – we should lock our markets, when you have clear evidence. There was a case in the paper last week about a company, I don't remember their name, but they make essentially push to talk radios that the police use, and other first responders. Pretty clear evidence that they stole that technology from Motorola. And we blocked sort of the phone – we blocked, like, the 2.0 phone that stole it, but we're letting in the 3.0 phone. I mean, it's like, look, in my view if you – if it's pretty clear evidence, you know, beyond a preponderance of a doubt that you have stolen American technology, you should not get access to our markets. And eventually the Chinese companies will figure out that there is a price to pay for this kind of behavior.

Robert D. Atkinson: This kind of behavior, by the way, is rampant. I mean, it's not just, like, an occasional thing. And somebody – there was a quote today by somebody, oh, it doesn't matter that they stole Tappy, the thing for T-Mobile, the little finger thing. (Laughs.) Sure, if that's all it is. But it's not. It's much, much more sophisticated. And so I'm not worried about that. I think at some point you have to send the Chinese a message that's says crime does not pay, and you're going to have to pay the price for it. And the Europeans and the Japanese, to me, have to align with us to do that as well.

Kate O'Keeffe: Just to clarify. Sir, were you also talking about, you know, would the U.S. block Chinese companies from, like, coming into the U.S. and selling their products there? Was that also part of your question? Because if so, I just wanted to say that I think we have seen that in some cases, with CFIUS, the Committee on Foreign Investment in the U.S., where they've moved to block certain attempts by Chinese entities to expand their business operations here due to national security reasons. And one of those companies is certainly a key player in this Digital Silk Road, which is a financial, you know, part of Alibaba. When they tried to buy MoneyGram, that transaction was stopped due to these types of concerns. So, I mean, it wasn't the type of blocking of market access that I think we're seeing China engage in. But it was, I guess, a U.S. form of that.

Kate O'Keeffe: Sorry, we'll go – can we go to this gentleman in the very front here?

Q: Thank you. Chris Macrae, Norman Macrae Foundation.

Q: I wanted to challenge something that I thought I heard Robert say 15 minutes ago, which I think was that all trade is a zero-sum game. I want to start from a sustainability goals perspective of, you know, progress for the human lot. As far as I'm concerned, all progress for the human lot, from the sort of bottom up, is potentially win-win. So I've studied and worked Bangladesh. I've been over there 15 times. And if, for example, women who 40 years ago had no life because they were dying at 35 because the health was so bad, and everything are, you know, surviving to 65 and building last mile health from the village up, that's a win-win-win for everyone.

Q: So I think there's a really big problem – because if you look only at GDPs, you're not looking at education. Or you're not looking intergenerational things which multiply value, which are relevant to all the sustainability goals at their deepest. That's the thing I'd like some clarity on, because it seems to me if we only look at things from the top down and say everything is a zero-sum game then, OK, you know, we're never going to achieve any sustainability progress, and no one is ever going to trust anyone who uses only those models.

Robert D. Atkinson: Well, just to be clear, I didn't say everything is a zero-sum game. I said global competition in technology industries is largely a zero-sum game. Nor do I believe that the sort of Silk Road – Digital Silk Road efforts are, you know, probably pretty good. I mean, these countries need these technologies and the Chinese are providing them. My complaint with the Chinese is not really about Digital Silk Road. It's about this set of unfair mercantilist practices that underly that or underpin that. I will say one last thing on sustainability, if you look at the U.N. 20 – I think it's 20 – Sustainable Development Goals, growing GDP and productivity is not one of them. I'll tell you the most important thing for somebody in India. It's more money. You know, Indian GDP per capita is abysmal. It's super, super low. It's about 12 percent or 13 percent of U.S. GDP. The single most important thing we could do to help India would be to help them to grow their GDP.

Robert D. Atkinson: So, I think it's – I get that there are other things that are also important but dismissing GDP growth when you're super poor I think is just consigning people to poverty. So I actually would argue that GDP growth is probably the most important thing we can do in the emerging markets to help them get a better life.

Kate O'Keeffe: OK. So we're coming up on the last sort of 10 to 15 minutes. So maybe we can take three questions at once and then the panelists can sort of respond that way. So how about this gentleman here, this gentleman here, and – oh, no. There's so many more people. (Laughs.) And I guess this gentleman here in the purple tie. I'm trying to, like, geographically distribute.

Q: Hi. I would like to thank all the panelists for all your insights. Two very short questions.

Q: One is to follow up on Kate's earlier remark on CFIUS, which is both in the CFIUS expansion and then last year's – and the EU's position to come up with a framework for investments screening, both mention that national security grounds for blocking or reviewing certain transactions, mergers and acquisitions. My question is, in the age when conventional manufacturing is increasingly integrated into the digital space, how do we define national security? And is our government the best

agents to actually make this definition, instead of leaving it to the market to sort out?

Q: And the second question is, I think earlier last month Deutsche Telekom come out with a paper basically cautioning governments in Europe that disallowing and banning Huawei equipment from the 5G network in Europe is going to severely hinder the ability of a European company to roll out 5G technologies across the continent, and in turn would hinder the progress of digital technology on the entire continent. So my question is, if, you know, we have decided collectively that Huawei is such a security threat that we're banning it from the whole market, you know, what are the alternatives? You know, should governments take the lead? And how should it be done? Is it a government-driven effort, or should it be public-private partnership, or something like that?

Kate O'Keeffe: OK, thanks. And then the second question. Oh, right. Sorry, can we have a microphone here? Sorry. (Laughs.)

Q: Thank you for choosing me, even though I'm wearing all black today. But my name is Michael Armao and I run a market risk analysis firm.

Q: And my question in the commercial sense dovetails on two comments, one that I've heard from General Mayville and one that I heard from Dr. Atkinson. With respect to some systemic issues that U.S. and European companies run into when selling their wares in this Digital Silk Road area – for example, dealing with companies who euphemistically say, well, U.S. companies don't want to sell to us, which basically means they don't want to pay underneath the table. So most U.S. executives don't want to go to jail for violating the Foreign Corrupt Practices Act. A certain number of European companies, most companies, have an equivalent. The British do, I know.

Q: So with that being said, you have then Dr. Atkinson's comment about taking Chinese companies to the WTO, with the current administration's disdain for the WTO, as exemplified by, for example, not even wanting to name judges to the appellate division. What would the panel's take be on dealing with these systemic issues and the current political environment for us to be able to represent companies in that area? Thank you.

Kate O'Keeffe: OK. Thanks. And the third question, please. Thank you.

Q: Hi. Thank you. And thank you for calling on bipartisan purple on State of the Union day. (Laughter.) Bill Hederman from University of Pennsylvania.

Q: I was wondering if we could talk a moment about China's Silk Road, et cetera, in Venezuela. It seems like this is a place where we're going to have some of these practices move from theory to problems really quickly. I'd just be interested in your insights on that.

Kate O'Keeffe: Thank you. Those are all great questions. Maybe, Emily, can we start with you? And if you – if there's one you want to respond to, or we can throw it to the –

Emily Rauhala: What was the first question?

Kate O'Keeffe: So, well – so the first question was about should countries be in charge of determining national security priorities or should that be left to the private sector? And I think sort of inherently given it's national security it would have to be determined by the government. But I'm sure companies would love it if that weren't the case – (laughs) – because they could probably make a lot more money. And, yeah, anything else you wanted to add.

Emily Rauhala: Sure. On that, I'll just say briefly, you know, do I think governments do a good job of abusing the term national security? Absolutely. China does it. The United States has done it. But in terms of leaving it to the market, I'll come back to an earlier point I made earlier, which is people – including and particularly me – are really stupid. And – (laughs) – we all when it comes to tech make lazy decisions and often act against our best interests – particularly our security and privacy interests. So as imperfect as it is, I don't – I don't see market as the best mediator of security, because we've seen all the time that people make very poor decisions. But, of course, governments can abuse national security. And that's something that's a really key issue for both sides here.

Kate O'Keeffe: And then we – the two other main questions are about the WTO and Venezuela. So did either of you want to respond to those?

Robert D. Atkinson: So I can do the WTO. I don't know anything about what we're doing in Venezuela. I think – I don't think the administration is as down on the WTO as you might think. I mean, Dennis Shea, who's the U.S. ambassador to the WTO, is doing a really excellent job. Lighthizer signed on to at least one case as part of the – actually, I think a maybe a couple. So I wouldn't say it's not an avenue. In our view, it should be a stronger avenue. And I think the administration should push, along with our European allies, for serious WTO reform. The administration is right that the WTO really doesn't work right. There's a really good paper by Mark Wu, who used to be at USTR and now at Harvard Business School – or, Harvard Law, on the failure of the WTO when it comes to China. I think he's absolutely right. But you don't want to throw away the bathwater.

Robert D. Atkinson: I don't know enough about Foreign Corrupt Practices law to say whether that could be something under the WTO jurisdiction if you were to reform the WTO. It's an intriguing idea that I think we all ought to look at. But I will say that, you know, we are competing with one hand tied behind our back when other – when our competitors can put a big bribe under the table. A lot easier for them to get the contract than us. You know, I don't know what to do about that, but I think it's naïve for us to say we're going to be the beacon of light and goodness and somehow that's going to accrue to our commercial advantage. There are lots of cases where it's not going to accrue. It's going to accrue to our competitors, who don't have to live by those rules. So whether you can figure out a way to get more of a global regime on that and get these countries part of it, I don't know – I don't know the answer to that. But it seems like an area we should move forward on.

Kate O'Keeffe: Did you want to talk about Venezuela, or?

William C. Mayville: I'll try, because it's a great question. It's happening in our backyard right now, and we have been for too long ignoring these issues, and in particular Venezuela. So here's – let me be a little bit of a futurist with where I think we could be going as a government. So let's think about the human catastrophe that is Venezuela. And we

will – no doubt we should lead the effort to address and redress the humanitarian crisis that is there now. But then on the heels of that, why are we looking at development differently instead of it – in the way that I remember it in my days in Iraq and Afghanistan?

William C. Mayville: Why aren't we looking at how we can partner with industry to promote local entrepreneurism? Why aren't we exploring ways in which we could, for example, create fiat-based global chains, tokenize things locally. There's ways to do that. You get an anchor bank. You get a – you get a blockchain online banking system. You deploy it the way you would deploy – the way, say, USAID would deploy aid. You think about it strategically. But now what you're trying to do is to foster entrepreneurial spirit. And you empower that by extending that technology? I stretched a little bit, but that's the sort of creative things that I think we have to think about deploying in the future. So it's – I clumsily addressed Venezuela, but I tried.

William C. Mayville: On CFIUS, I absolutely believe it is the role and responsibility of government to be a leader here. I think no other force can do that. And I think this is precisely what government is supposed to be doing. I do accept, however, the observation that today the technology moves too fast for policy to government, and that it's very, very difficult to assess the risk forward. But none – those two reasons aren't justification to find some alternative system. And I think we are caught flat-footed here. I think there are new partnerships. There's a way to inform that process. But I think it's absolutely something that government should do.

Kate O'Keeffe: Thanks. And just one last quick – super-quick thing on Venezuela. I assume that you may have been referring to the blockbuster Reuter's report last year about how ZTE was working with Venezuela to track its own citizens. And that really is such a fantastic story that if you're interested in this issue you probably read it, or if you haven't I would recommend it. And I was heartened to see that there were requests from senators here for the U.S. government to probe that issue, because I think – as you pointed out – that really is sort of an example of some of the worst fears that people have about China exporting this model of digitization around the world. So thank you for flagging that.

Kate O'Keeffe: And thank you, everyone, for coming to this event. And I hope you have a great lunch. And I release you. (Laughs.) Thanks. Bye. (Applause.)

(END)