Center for Strategic and International Studies

TRANSCRIPT

Debate: "Should the United States Severely Restrict Huawei's Business?"

EVENT DATE

Friday, June 28, 2019

TIME

10:30 a.m. EDT

LOCATION

2nd Floor, CSIS Headquarters, Washington, D.C.

FEATURING

The Yes Team:

Martijn Rasser,

Senior Fellow, Technology and National Security Program, Center for a New American Security

Dan David,

Founder, Wolfpack Research LLC

The No Team:

Paul Triolo,

Practice Head, Geo-Technology, Eurasia Group

Erin Ennis,

Senior Vice President, U.S.-China Business Council

CSIS Experts:

Scott Kennedy,

Senior Adviser, Freeman Chair in China Studies and Director, Project on Chinese Business and Political Economy, CSIS

Transcript By
Superior Transcriptions LLC
www.superiortranscriptions.com

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Scott Kennedy: Well, good morning. Welcome to CSIS. I'm Scott Kennedy. I'm a senior adviser in the Freeman Chair in China Studies here, and I'm also your safety officer for today. There's lots of folks here, and if there is any kind of issue or any type of challenge I'll try to give you advice and protect you. You'll be able to go out one of these exits on either side. You'll go down the stairs, come out the sides of the building, and we'll meet across the street, and then the losing team will buy a round for everybody. (Laughter.) That's not going to happen. We're going to have a great event today, no issues whatsoever.

And in fact, this is the week of debates. The Democratic Party had two debates that touched lightly on China. We're going to take, instead, a head-on approach to the most urgent issue facing U.S.-China relations, which is "Should the United States severely restrict Huawei's business?" Let me briefly explain why CSIS is hosting this debate, introduce the two teams, explain the format and the rules, and get you, the audience, involved right away.

So why do we need this debate? Well, on May 15th the president issued an executive order prohibiting the purchase or use of any communications technologies produced by entities controlled by a foreign adversary and likely to create undue risk of sabotage of U.S. communications systems or catastrophic effects to U.S. infrastructure. This executive order is clearly aimed at Huawei; and comes on top of the National Defense Authorization Act, which already placed a ban on federal government funds being used to purchase Huawei equipment. Also on May 15th the Commerce Department added Huawei and 68 of its subsidiaries to the entities list, which prohibits American companies from providing components and services to Huawei. Four days later the Commerce Department issued a temporary general license allowing U.S. firms to provide support for existing businesses, and that temporary general license is set to expire on August 19th. Beyond this, the U.S. government has advised other governments around the world not to buy Huawei 5G equipment and some of them have taken steps similar to those in the executive order. So we're having this debate, first of all, because the U.S. has tried to start to severely restrict Huawei's business.

Second question, though, is, why should we care, and why do we need a debate? Well, these actions indicate that the U.S. faces an unprecedented national security risk. Americans have a vague idea of these risks, but they're largely unknown outside the government because a lot of the information that's based on identifying these risks are classified. Secondly, U.S. components are so important to Huawei that these steps put Huawei's existence in doubt. Huawei is by far China's most successful high-tech company, and at the same time American companies do billions of dollars of business with Huawei and Huawei is one of the world's largest telecom firms with business in 170 countries, and these steps could affect the stability of the networks that Huawei supports. Even more important, these actions are being taken in the broader context of an increasingly tense relationship, potentially part of a larger strategy vis-à-vis China, and possibly involving economic disengagement. And so these actions affect the interests of other countries as well, including American allies and friends.

Now, raising these facts is not to argue for or against the administration's actions. But these are highly consequential steps, and in a democracy we should have a robust discussion about the risks we face and the strengths and weaknesses of different courses of actions. That's why we're having today's debate.

I'd like you all now – as audience members, you found on your seats when you arrived these iClickers. I don't have one up here, but you all have one on your seat, and we want

you to vote now. And hopefully you'll see – behind me you'll see the question: "Should the U.S. severely restrict Huawei's business?" And so you turn on your clicker first and then you choose A or B, and we want to see what your views are just as we – before we get started with the debate itself. All right. So – all right, so we've got something – roughly 53 to 47 (percent). We'll come back to that. So that's important to know. So we have a relatively even, divided split here to begin with.

But now we're going to turn things over to the professionals, and we have two fantastic teams. Let me introduce both of them very briefly. You have brochures where their longer bios are contained.

First of all, on the yes team, Martijn Rasser. He is a senior fellow in the Technology and National Security Program at the Center for a New American Security. Prior to joining CNAS, Martijn had a distinguished career in the intelligence community and more recently in the investment world.

His partner is Dan David, who is the founder of Wolfpack Research, an investigative and due diligence firm. He is also the co-founder of the investment research firm GeoInvesting, and he has been extremely active in trying to highlight the risks facing the United States and investors.

On the no team we have Erin Ennis, who has been at the U.S.-China Business Council since 2005, and since 2015 has been their senior vice president directing their government affairs and advocacy work. She previously worked at the U.S. Trade Representative and in the U.S. Senate.

Her partner is Paul Triolo, who is the practice head of geo-technology at the Eurasia Group. Previously he worked for over 25 years in the U.S. government, focusing primarily on China's rise as a high-tech power.

The format for today's debate is straightforward. First of all both sides are going to make opening statements, first with the yes team and then the no team, and then they will make – offer rebuttals, six minutes each. And then we're going to have question time, kind of like the U.K., and we'll allow each side to ask questions of the other side and have each – give each team 10 minutes. They'll then make closing statements of five minutes each, and the yes team will get to decide whether they want to go first again or whether they want to defer to the no team, and we'll ask just before then.

The basic rules is that you can use the time however you want – divided separately 10 minutes, zero, five, five, whatever you prefer. If you want to stand and dance, you can stand and dance. If you don't want to dance because there's a lot of people watching, then don't dance. There will be a stopwatch on the side that identifies where we are and keep us relatively on time. This isn't a congressional hearing so we're going to give a little bit of flexibility, but for the most part we'd like both teams to feel that it's a fair use of time. And then we're also going to, finally, maintain as much decorum as possible, because even though these are very significant issues, potentially strong opinions on both sides, it's important that we have as cordial a conversation as possible.

So, with all of those preliminaries out of the way, I'm going to turn things over to the yes team for their opening statement. And you all have 10 minutes.

Martijn Rasser: Great. Thank you, Scott.

Good morning, everyone. It's great to see so many people here.

So the question is, should the U.S. act to restrain Huawei's business activities? Dan and I will show that that answer is a clear yes. U.S. actions to date – placing export controls of critical U.S. technology, banning Huawei from our domestic networks, and encouraging our allies and partners to do the same – is justified and it's necessary.

So why does this matter? Scott alluded to this already: The stakes are great. The Chinese government's geopolitical objectives and Huawei's commercial activities are fully intertwined. Huawei is an extension of the Chinese state. By championing Huawei, China seeks to gain expansive control over next-generation wireless communications networks known as 5G. 5G will enable advanced military communication and situational awareness, autonomous vehicles, smart cities, the Internet of Things. 5G will be the backbone of the global internet economy. It is the driver of the next Industrial Revolution. 5G will touch everything that you and I do. We cannot have a geopolitical rival, a near-peer revisionist power, a potential U.S. adversary control the technological foundation for the modern economy. The risk of service disruption to critical infrastructure, unfettered cyber espionage – this threat is real and it's unacceptable. It is also a severe danger to the security of our allies and partners. Ultimately, global security is at risk.

This is why the decision to exclude Huawei from U.S. networks and to deny them critical technologies is fair and it is just. Make no mistake, in doing so we will make some sacrifices. 5G rollouts may take longer. Some U.S. firms will lose revenue. This, however, is a price worth paying as a nation. What's important is that we do 5G right, not fast. We must ensure we have a secure and trusted telecommunications network to support transformative economic growth. We need to safeguard our military's ability to operate at will around the world.

I want you to remember this is not a partisan issue. It's a core national security concern. It has broad bipartisan agreement. And the fundamental concerns over Huawei's technology and its relationship with the Chinese state goes back decades. It was the Bush and Obama administrations that set up the process that we're putting in motion today.

Furthermore, this is not a unilateral American concern. In fact, it's the Australians who, during a 5G wargame exercise, really catalyzed the actions that we're discussing today. The Australian government determined that Huawei technology posed unacceptable risks to its critical infrastructure and was a conduit for espionage. The U.K. government soon thereafter released a report citing rampant security violations in Huawei's software. This provided the momentum for U.S. actions. While some pundits will have you believe there is widespread disagreement with our allies and partners, there is, in fact, very little daylight between us. The main difference is how we choose to address the problem. We believe, Dan and I, that the U.S. course of action is the best option at this point.

Dan, the floor is yours.

Dan David: Thank you, Martin. Thank you, Scott. Thank you, CSIS, for having me here today.

I am simply here as a concerned citizen, and I appreciate the opportunity to speak to you about my experience over the last 12 years of doing on-the-ground due diligence in China. What we have found are the two Chinas, I like to call it: the people of China,

who are open to us, supportive of us, honest in helping us do the right things; and the government of China and the corporations of China. And these are our experiences, only some of them. We have exposed over a dozen China-based frauds, delisting $15 billion worth of market cap just from my firm alone as a part of a greater, yet untold multibillion – hundred-billion-dollar fraud in progress being perpetrated on financial markets all over the world. And we understand that the fraud that we catch is nowhere near the fraud in total. Now, I always feel it's important to point out that it's not illegal in China to steal from an American citizen. So we have $1.4 trillion in market cap here now today, which has grown by about a trillion dollars since 2008, and none of the China-based CEOs are legally accountable in the countries in which they live. So the fraud continues.

Our first China fraud – one of the first China frauds that we exposed cost us $300 in due diligence. We spent $300. It was about an $800 million market cap company, and about two hours after we released our findings they crashed. A(n) investment bank had the same due diligence we had three months prior to us and chose not to expose it, bury it, and raise $90 million from U.S. investors one month prior to us exposing that. Those investors were wiped out.

We have on multiple occasions found China-based CEOs just one day disappear. We ask, where are they? Did somebody call the police? They say, who do you think took them? When are they going to be back? Maybe 30 days, maybe 60 days, maybe 90 days; you'll hear something. But that happens in China. CEOs can be just picked up and taken, and you don't hear back from them for some time.

We have been sued several times for hundreds of millions of dollars defending our right to free speech by U.S. law firms. Yeah, there's always a U.S. law firm involved. You can bet on that. And that's really what happens here, right? Our court systems are just, and they're taken advantage of. Our free press is just, and it's taken advantage of. And there's always a lawyer willing to help here in the United States. And the companies that have sued us all lost and were delisted, went bankrupt; investors were wiped out.

I have been hacked and subjected to denial-of-service attacks more times than I can count. The last time was Monday. Thanks for inviting me here today, Scott. I'm sure it had nothing to do with it. (Laughter.) I treat these denial-of-service attacks like OSHA incidents now: it's been 44 days since my last attack. But they do happen way too often.

The FBI called me this year just to inform me that I was under surveillance from China – to which I said, no shit, welcome to the party. (Laughter.) And I'm not talking about some field office or regional office; I'm saying they flew in – I can't tell you where they flew in from, but they flew in and spent two days in my office going through my systems. That was not an easy thing for me to agree to, but in the end not a hard decision either.

Our investigators in China, China nationals, are some of the most honest and moral, brave people you'll ever want to meet, fighting for integrity and justice. And for this, they have been threatened countless times, beaten, run off the road, pistol-whipped, arrested, prosecuted for criminal defamation – that's right, criminal defamation. So if you say something about a company they don't like, they can put you in jail. And in this case the offended company was allowed to have their attorney stand with the prosecutor and prosecute this investigator, who was given two years in jail. He published nothing. He said nothing. But he worked for an American who did publish, and for that he got two years in jail. For brevity's sake I won't tell you about the awful conditions that he had to endure, but they were objectively awful and worse than you can imagine. Kun

(ph) suffers from PTSD to this day, and we suffer from the decision that put him in that situation. He swears that he has no regrets, but I do have regrets.

One of our investigators took it upon himself, so fed up with the police corruption – if you can believe this – to wear a wire and an undercover camera to his own police interrogation, where the police were telling him that if he didn't give false testimony against people he worked with they would make up charges against him. I'm happy to say that we smuggled Michael (sp) out of China. And after five long years just two months ago Michael (sp) was granted asylum here in the United States, in no small part due to the video we were able to smuggle out with Michael (sp).

Now, how does this relate? These companies I'm talking about are inconsequential to the government of China. They mean nothing. And this is what you can go through doing basic due diligence that we take for granted here. Had these been SOEs – state-owned enterprises – we're talking serious jail time, big time trouble. If we were talking about Huawei, that's a game-changer. That's freedom over. That's life over. And that doesn't mean and I'm not saying that Huawei's a bad company; not at all. That's saying that's how important Huawei is to China. There is no looking into Huawei for somebody like us or the average person doing your due diligence in China. That can't happen. That is their national champion. And that's a problem.

Scott Kennedy: Hey, Dan, I think we're going to pause right there. Thank you both for your opening statement.

Dan David: There's no timer.

Scott Kennedy: Yeah, we're – there was. It's on the right side. Sorry.

Dan David: Oh.

Scott Kennedy: No worries at all. I'm going to thank you both for that.

We've added a few more seats so folks who are in the back should be able to find seats along the sides or up in the front.

We're now going to turn to the no team. And you have now 10 minutes.

Paul Triolo: Thank you, Scott. And I think your timing in putting this together was very appropriate, as this issue is also being discussed, I think, in Osaka this week.

So I think let me just quickly get – note to Dan that all those attacks that you were experiencing, none of them probably traversed Huawei equipment. I just want to make that point.

So I think what I'd like to do is discuss – drag us back to sort of the issue of – at hand here, which is what is the response – what is the policy response to this issue around – the issues around Huawei. And I think you could probably put the question better as, you know, should the U.S. government kill Huawei, for example? So this is – this is the quote that Steve Bannon has used, that it's more important to kill Huawei than even – than to have a trade deal. So I think that's one quote that I'll point out.

The other one is Theresa May's quote following her Cabinet discussions around whether to allow Huawei into U.K. networks. And she said, we're going to listen to our experts. And I think that's a really – another really important quote.

So I think when we look at this issue, I think there's really three issues that have become entwined with the Huawei issue that need to be resolved to try to find some middle ground. So I think Erin and I are coming at this from – very much from an industry point of view. We're not defending Huawei's business practices. We're looking at this issue as trying to find a middle ground that balances the risks to national security and also looks at the broader industry and economic issues around suppliers and customers that have come up just within the last month since the entity list order was – entity list was issued on May 15th.

I think it's important to note that there are – there are three main issues that we see that have been caught up in the broader relationship, so I think – and need to be resolved before there's a way forward here.

So the first one, of course, is the law enforcement issue around Huawei that led to the arrest of Meng Wanzhou and the specific issue of violation of Iran sanctions. And in that case, I think that's a fairly easy issue to resolve. We saw – we saw what happened in the case of ZTE, where a deal was arranged and the company paid a fine, agreed to discipline its executives, and that issue was addressed. We saw – we saw this happen last year. Even after they had violated the original agreement, a solution was found to that – to that – the issue of ZTE and the entity list.

But the problem is that there are two other big issues that have been – that are at play here. One is the issue of subsidies and fair competition and market access. And so there's a lot of concern, of course, that Huawei has received subsidies from the Chinese government, and this has led to its dominance in 5G network supply globally. And so that issue, I think, has to be also addressed if there's a – if there's a middle ground to be found in this – on this issue.

And then, of course, the third issue is the national security issue, which Martijn raised. I think in that – in that case I think the U.K. approach has been very instructive, and we can talk more about that. But I think that – I call that the mature approach. They have at least – almost 10 years of experience in reviewing Huawei's source code, they've looked very carefully at Huawei business practices, and they believe that they can handle the national security problem, the security of 5G supply chains. And that's what led to Theresa May's statement that we'll listen to our experts on that, and that's really important.

So I think if we look at, then, at – just specifically at the industry issues around this, which really have come to the fore in the last few weeks and I think which we have focused very much on, the sort of direct impact of the entity listing on both Huawei's customers and on its suppliers, I think that's really the – one of the issues that hasn't really been discussed in much – in much detail and needs to be understood. So on the – on the customer side, of course, there is the issue of 500 million smartphones out there that will need to continue to be patched and upgraded. The temporary general license allows that, but that's going to be an ongoing problem. That's actually a cybersecurity problem. Those phones will need to be supported going forward, a huge issue.

And then I think the key thing is the infrastructure side of Huawei's business, and Scott alluded to this. The problem then is also the issue of supporting all the equipment that's already out there in terms of software and upgrades. And then the actual cost, potentially, of carriers having to rip out and replace equipment if this order stands because this is really – this issue has really thrust particularly Europe into this – into a really difficult decision around supply chains. And if they can't count on Huawei equipment being upgradable for 5G, they're looking at facing considerable costs in ripping out that equipment. And GSMA, the industry group, did a – did a scenario planning, and they came up with this figure of $62 billion just for Europe. We think that's probably high, but it illustrates that the costs of this decision being – going forward and not being rolled back means that carriers around the world, not just in Europe, are facing huge costs and then a delay, as some mentioned here – Martijn mentioned earlier. GSMA estimated 18 months, and probably that's conservative. So the cost on the – on the infrastructure side is huge.

On the supplier side, though, I think is really where our comments will probably be more relevant, and that is that U.S. industry, and particularly the semiconductor industry, is very concerned about two things. One is the potential for this action and other actions against Chinese companies to lead China to – Chinese companies to view U.S. suppliers are unreliable. And this would mean over time that Chinese companies would be designing out U.S. semiconductors, for example, and this is a huge issue for U.S. industry because this gets to their ability over time to derive revenue from the China market, and to invest that in R&D, and to innovate. And so, ironically, this is viewed as a national security problem from the supplier side because their ability to continue to innovate and drive development in the semiconductor industry is under threat here.

And then, finally, the standards process. This is another issue. So the TGL allows U.S. companies to engage in the standards process, particularly the 5G process, but the concern is that over time this could – this ability of U.S. companies to lead in standards-setting could also be eroded.

So those two issues, I think, are things we need to explore more. But I think the bottom line is this is a complex issue, a nuanced issue, and understanding where industry is on this is required to fully understand the issue.

And then the search for a middle ground here I think is what we're really after here. We're not saying that there's no issues with Huawei, but we're saying there needs to be a very careful, nuanced, and middle ground found to resolve the problem.

Erin Ennis: Let me just add a few points from the general business community perspective on this.

Among the reasons why the U.S. economy has been as strong and resilient as it has been at least through the 20th century and into the 21st is that we have found a way to balance our national security interest with our commercial interest. If you overly-weight one of those two issues over the other, there are unintended consequences not just to having too much of a military interest trying to drive what our commercial interests are, but also on the other end having too little attention to where those national security issues are.

Now, when you deal with these issues from a trade and commercial perspective, there's really two things that you have to keep in mind. The first one is, frankly, the golden rule of trade policy: Do unto foreign companies as you would have foreign governments do unto your own companies. If we single out individual companies without providing

sufficient evidence about what the concerns are, based either on a national security concern that maybe we civilians can't know, then we should assume and we will see that American companies are similarly targeted overseas. Now, that is something that I think we should not stand for. We should accept the fact that it is possible to provide sufficient evidence of where the problems are and to craft punishments that fit the crimes that are identified in those areas.

The second issue that I would make is kind of a corollary to this, and that is that when we do these things the U.S. needs to rely on a strong rule of law to deal with them. We shouldn't be adopting approaches to technology that are not clear, that are vague, that make it difficult for companies to, once they've been designed as violating the law, to address the problems and come back from it. If a company violates the U.S. law, it absolutely should be prosecuted through the appropriate means, If necessary, controls on the products that it has access to from the U.S. market should absolutely be limited. But U.S. companies need to be given the opportunity to be able to comply with these issues.

In the instance of the case against Huawei, American companies were given very little time to comply. And it has led to chaos in terms of how these things are implemented. If the threat is so high that we must immediately keep the products out of the market, then why is it that we're allowing products that have 20 percent of Huawei's components still into the market under the de minimis rules? And the specific case, in this one, we really do need to have sufficient evidence to address these cases. And it just simply hasn't happened. And, frankly, this is one of those instances where we, I think, are about to provide Newton's third law of motion – for every action there will be an equal and opposite reaction. And it will be against American companies.

Now, I will note that I think we also need to be doing these things in alliance with our trading partners. We could develop the best technology in the world, but if we attempt to cut off our market to China's, or American companies to the components that we need, we are going to be the proud owners of the best Betamax technology in a world that uses VHS. China is the largest market in the world for American companies, and it probably will be so for at least the next 10 years. The actions that undermine American companies' ability to compete in that market, and to compete globally, will harm our economy and, again, throw that balance out of whack against national security and commercial interests.

Let me close by making one last point. And that is: Huawei needs to do better. The fact is that Huawei has very legitimate trust and transparency issues, and there are real questions about the security of the products that it provides. If it wants to be accepted as a global leader, it has got to hold itself to the highest standard on these issues, but its actions will have to speak louder than the words that it's given today.

Scott Kennedy: Thank you both. I think both teams have set out very clear views about the question. Really appreciate you doing that. I think we have a great framework. Now we're going to turn to the rebuttal section. We're going to allow the yes team six minutes for rebuttal.

Martijn Rasser: All right. Thank you.

Paul, first I wanted to just point out the GSMA figures you cited. They did not disclose what their methodology for the calculation was. So I'm not sure that's the best figure to throw out. Also, Ericsson disagreed with the rip and replace argument that GSMA made. So in terms of Theresa May listening to her experts, in fact, she is not. Again, like I said

earlier, you know, the British government determined, and I quote, that they found "serious and systematic defects in Huawei's software engineering and cybersecurity competence." Theresa May's own defense minister was so concerned about this that he purportedly leaked and was promptly fired for doing so. The fact that he's willing to sacrifice his very substantial job for this is a sign that there's a lot of concern among high-ranking British officials that is not being listened to.

In terms of the smoking gun that you were referring to, to insufficient evidence, I already mentioned the Australian and the U.K. examples. The African Union has accused Huawei of enable espionage – a five-year long espionage effort against their systems. And just a few days ago, we learned in press reporting that a U.S. cybersecurity firm determined that Huawei's software is riddled with vulnerabilities to a much greater degree than any other competitor out there.

On subsidies they're orders of magnitude larger than anything any Western country could hope to receive. We're talking of hundreds of millions of dollars in unrestricted loans, unconditional grants, bonuses for top engineers. In addition to that, they get sweetheart deals on land, real estate, to retain employees. What this enables Huawei to do is plow money into R&D that they would otherwise not be able to afford – this just giving them an edge – and also able to heavily undercut the competition around the world. It's not a level playing field.

So, Dan?

Dan David: Paul, I didn't quite hear what you said when I was finished speaking. Was it that none of the things that happened to any of the people I worked with happened on Huawei equipment?

Paul Triolo: Yeah, likely happened. I said that was probably most likely, mmm hmm.

Dan David: That's objectively untrue. And I'm sure you didn't mean it that way, but, like, these are very serious things that happened to people that I know. And I don't blame Huawei. Again, their equipment is ubiquitous. Of course it's being used. Just like it's being used against the Uighurs, right? Why wouldn't it be? It's surveillance equipment. You need it in that 5G/4G technology. You're going to need it in everything. It doesn't necessarily make them bad, but China needs their equipment for everything.

I think, you know, our rebuttal here is that they've made our point. There are problems with this relationship. I mean, they've said it. There are legitimate trust issues. There are legitimate transparency issues. There are legitimate rule of law issues that need to be solved. Guess what? They're not solved. (Laughs.) And they going to be solved today? No. Are they going to be solved as we're rolling out 5G? No, because, guess what? We're rolling out 5G. So these issues are not solved. And as we draw them out, we're going to work on legal reform. We're going to work on IP theft. We're going to work on legitimate trust issues. We're going to work on closing these security loopholes. Just let us be part of this infrastructure. We're down the road and it's too late.

It seems like this argument continues to center around we're too entangled, so let's just go further. We're just – you know, we just – we can't stop now. And if we keep getting the answer no, we're just going to have to continue to go further and hope that we can negotiate our way out of this. But we're not negotiating our way out of this. The legal reforms in China are not getting better, they're getting worse. The authoritarian rule's

not getting better. It's getting worse. So I don't know how we're going to expect this to get better before 5G becomes the reality.

And I don't accept that the rest of the world is going to become more innovative than the United States. I don't agree with Vladimir Putin on anything, but one thing. The thing he admires most about the United States, we are the innovators of the world, and always have been. We had our Sputnik moment and we went to the moon. They beat us to space; we went to the moon. I reject the notion that if we get into a competition we will lose. Maybe we need to take a jab to the face before we take our supply chain back. So it's either that or we have a rule of law and a cooperation that says: What's good for you is good for me. What's good for me is good for you. We want that kind of relationship where we take care of each other, not take advantage of each other. That's all we're asking for. And nobody here is saying that's the relationship we have. So they've really made our point for us.

Scott Kennedy: Terrific. Thanks so much.

The no team, six minutes.

Paul Triolo: OK. So on the –on the GSMA figures, agreed that they're probably too high. But one of the challenges here is nobody really knows how to make those calculations, because this situation has never happened before. So they're probably a little high, but they're probably within the ballpark. I think the key part of that is the delay – the 18-month delay period. And that's probably accurate, from discussions I've had with many carriers and other industry folks. So I think we can quibble over the number, but whatever the cost is it's high of actually have to rip and replace equipment, and change carriers, and train engineers, and basically abandon all capex plans that were in place.

On the – on the issue about the U.K. government, I think it's a little more complicated than you've outlined here. The U.K. government decision that Theresa May mentioned was based on two studies. One was a study by her national cybersecurity center, backed by GCHQ, which came to the conclusion, again, that – and it's – I can make – I can give you references here – that the supply chain issue and the securities around 5G was manageable. In fact, when GCHQ and the NCSC set up the review center for Huawei software, they started with the assumption that the Chinese government could order Huawei to do something.

And they felt that that was a manageable problem because 5G security does not rest solely on the vendor. The vendor is actually a small part of the security posture for 5G, which is multilayered. The carriers have a huge role in this. They have huge visibility on the network. They have a say in all aspects of network maintenance and software updates. So the U.K. approach was based on a study of the cybersecurity risks and on the supply chain and costs related to 5G. And so the decision to listen to experts was based on listening to both the security experts and the sort of economic and supply chain cost experts. So that's I think, important to note.

And then the issue of the problems found with the sloppy software and other issues, that's sort of changing the goalposts here, because then the argument was, well, maybe they're – we're looking for backdoors here. But now we haven't found any backdoors, which none of the studies have shown. But it's just sloppy coding. So the argument could be made then that all vendors could have similar problems, and none of the other carriers – or, none of the other vendors, as far as I know, have been subjected to the scrutiny that

Huawei has been subjected to, particularly its source code for eight years in the U.K. So I think that the argument there is, again – and in a recent report that came out – are just – there's nothing really new there. All software is subject to vulnerabilities. I think Erin's point, though, is good, that Huawei has a credibility problem here in terms of being able to address the issue and show that it's adopting best practices in terms of software development. So there's general agreement on that point.

I think on the subsidies issue, that's a really tough one, because this really isn't good data out there to assess this. I think that clearly Huawei has benefitted from the large domestic market. But exactly what role the subsidies have played, I haven't seen any very good analysis of this. And so it's really – to differentiate just the sheer scale of the Chinese market, and access to that, and how that allows Huawei to drive prices down, versus the subsidy issue, I think is very – it's difficult to make a definitive case on that because that data just isn't there.

Erin Ennis: Let me add –

Martijn Rasser: Could I respond to that point real quick?

Scott Kennedy: When we get to the question part, sure. They get all the six minutes, so no worries.

Erin Ennis: I feel like I just had a moment from the presidential debate, where I interrupted.
(Laughter.)

Let me summarize very quickly kind of what I think the arguments are that we've heard so far this morning about why the U.S. government actions were justified. I would – first one, Huawei is a Chinese company, and therefore it is tied to the Chinese government. Huawei's products are flawed. China has fraud. China isn't a democracy. China doesn't have rule of law. I would challenge any of you to tell me why that justifies the U.S. government trying to bankrupt an individual company instead of saying: Your products are flawed, so we're going to set high security standards, so you will not be allowed in our products. We have concerns about your ties to the Chinese government, so you must be transparent about your business in this country if you want to do business with our companies.

And when it comes right down to it, if we can't hold ourselves to that standard then we aren't actually addressing what the underlying problem about any of those issues. We are simply moving to a standard that is less based on the rule of law and more based on an approach that China uses.

Dan David: I agree with everything Erin just said, except they'll say no, and have.

Scott Kennedy: OK. So –

Erin Ennis: So allow that process to work, rather than targeting an individual company with policies that are very clearly not laid out in a manner that is consistent with our other –

Dan David: Chairman Ren just said he's not going to allow Huawei to be subject to courts outside of China. He just said that.

Scott Kennedy: OK –

Erin Ennis: OK, so put – (laughter) – this into the context of how the U.S. government action against Huawei addresses that problem.

Scott Kennedy: All right. I love where we're going with this. (Laughter.) We are getting interactive before the interactive element of this. But we now have arrived. And so what I want to do now is let the no team go first. You can ask or repeat a question that you've posed to the other side, to the yes team. And the yes team can respond however they'd like. And I really want to give you all a chance, given that you've put a lot on the table, to be able to ask and respond to some of the questions that are at the very heart of this debate.

So 10 minutes now for the yes team to ask questions and for the no team to respond. I mean, sorry, the no team to ask questions and the yes team to respond, sorry.

Erin Ennis: I'll start. Martin, you, I think, made an excellent point, which is that there actually is not widespread disagreement that there are problems with Huawei. The difference is how other governments are choosing to address those problems. So why is there a difference in how governments are trying to address those problems?

Martijn Rasser: Well, for one, the United States is the only one with the leverage that it has in terms of the ability to deny them certain critical technologies. The other thing is that some countries appear to believe that mitigation is a suitable strategy. I would argue that given the nature of 5G networks, where the core and the edge, that difference is – there really isn't much of a difference. So with all the frequent software updates that you have on networks, the complexity of these networks, a lot of cybersecurity experts are arguing that a mitigation strategy, if it is possible, would be extremely difficult and extremely time consuming, extremely expensive. And frankly, a lot of people are arguing that it's impossible altogether. I think that's the U.S. conclusion. I think a lot of people within Great Britain agree to that, but they were overruled.

Other countries, such as Australia and New Zealand, have reached that conclusion. Other countries, like the Netherlands, Germany, they want to try the mitigation route, by allowing what they call non-core Huawei equipment onto their networks. I think that's the wrong way to go. I think given the vulnerabilities, the risk factors, mitigation is just too risky of an option to pursue.

Paul Triolo: I think that's a – that maybe is a good characterization of the differences. I think the thing to focus on, though, is which government that has a different view of this has the most experience in actually dealing with the issues at hand. And, again, I go back to the U.K. government's long experience in examining this question and working with its carriers – sitting down with its carriers and discussing these issues. So the missing piece here is always the carriers. The carriers have tremendous experience in dealing with these kinds of issues. So in discussions I've had with chief information security officers of leading EU country carriers, they have a very nuanced view of how they deal with network security.

And it gets to that issue I mentioned of multilayer security, where the vendor is an important piece of that but not the most important piece. And they have tremendous visibility on network – the data and flows within the network, and on things like software updates. So that – the carrier's view is very different. When we talk about different governments, it depends on different parts of governments. Obviously, in the intelligence services and other parts of EU governments support the view – the U.S. view that you need to take into account the legal and political structure of the vendor country. And then

economic and other parts of – and trade parts of the EU government have a very different view and tend to take the view of industry and of the carriers.

So I think it's very – it's important to distinguish, when we talk about governments, which parts of the governments are supported, and on what basis they're making their judgements. And, again, I get back to Theresa May saying that she would prefer to listen to experts on the issue. And those experts have focused, as I mentioned, on both security and the economics of the issue.

Erin Ennis: Is there a question there? (Laughs.)

Paul Triolo: Well, may question – (laughs) – yeah. My question is, when you say that Huawei is an extension of the Chinese government, on what basis are you making that judgement?

Scott Kennedy: Who owns Huawei?

Paul Triolo: You tell me.

Martijn Rasser: Well, so – (we'll have to give you ?) the whole – the whole rundown, right, Dan?

Dan David: I'm very interested in hearing the answer to that question. Who owns Huawei?

Paul Triolo: Yeah, I would like to know on what basis you would make a decision or a judgment about who owns Huawei, and what its relationship is with the Chinese government? What's the evidence?

Martijn Rasser: So we know that Huawei is wholly owned by a holding company. Ren owns 1 percent – approximately 1 percent of that holding company. The rest is held by, what is it called, a trade union, I believe?

Dan David: TUC, Trade Union Committee, which is 99 percent owner of the holding company. So the TUC is nominally employee-owned, right? And they would have shares in Huawei. Not regular shares, but virtual shares, right? Not the kind you can hold in your hand, behind a – the kind of that are behind a glass door, where the names are being held. Not the kind that you can transfer to somebody else, but the kind when you leave the company they pay you for them, or whatever. So you don't really know. And if it really is a trade union, by law, in a communist country, don't unions report to a superior union, all the way up to the Communist Party? And the head of the ACFTCU, right, the all Communist Party controlled ACFTCU sits on the Politburo. Unions are controlled. So technically, in their own definition, if it's owned by a trade union, it reports to the party. (Laughter.)

Erin Ennis: You got three minutes to ask more questions. (Laughs.)

Paul Triolo: Well, I don't think there's any evidence that business decisions that the company have made have been directed or influenced by anything other than the company's leadership and its – and the board of directors that controls the – that makes these kinds of business decisions. So I think there's been a lot of speculation about ownership of the country. And it gets back to Erin's issue of transparency and sort of the problems around Huawei's image. And those are – those are certainly there, but I think that we don't really, again, know enough about how that ownership structure works to make a judgement that says the company is somehow an arm of the Chinese government. I think

that's a pretty big leap of faith. And I think that the evidence just isn't there to support that. And so I think – that statement I hear a lot, but I think that it's really not really based on any solid evidentiary base.

Erin Ennis: So maybe kind of a variation on that theme. I am always intrigued in the discussions of these issues about the fact that we have the argument that Huawei's products are of inferior security, and also the argument that Huawei has potentially built back doors. Those two, to me, seems like they would lead to very different policy solutions. If their products are of poor quality, then higher security standards would presumably address those issues. If they are back doors that a foreign government has built into them for a nefarious purpose, then that leads to something that may be more extreme action against the company. So which is it, for Huawei?

Martijn Rasser: It's both. The fact that there hasn't been a public announcement of backdoors being found – you know, there's a great saying that the absence of evidence isn't the evidence of absence. I mean, there's a litany of reporting on the poor state of Huawei's software and their security practices, as called out time and time again. And they fail to address it. So why on Earth would anyone want to install that type of equipment into your networks, when there are alternatives? Now, granted, the price is great. That's why a lot of people choose it. But unless Huawei's willing to address these security issues, unless Huawei is willing to be transparent about their ownership structure, who makes the decisions and really addresses the issue that Paul raised, the murkiness of their relationship with the PLA, can't be trusted.

Paul Triolo: But in terms of the security issues around the quality of software development, shouldn't the market be the determinant of the response to that? Clearly in the marketplace, again, carriers around the world have chosen to use the equipment. And so the question – getting back it's Erin's question – who should – who should decide what the policy response is to that particular problem with the company? And I think, again, the view from industry is that they can – they are using the equipment, and they can handle the security issues around the equipment because, you know, again, it's not just about the particular vendor, but it's the overall security posture that a carrier adopts on the network. And so that's clearly been the case so far.

So the issue of drawing attention to Huawei's software development practices does seem like it's moving the goalposts here, because in the absence of a smoking gun that's what people are pointing to. But I still think that it's – this is an issue that has really become – come up recently. And now – you know, if there were really – if there was a smoking gun, do you think we would know it by now? Since this issue – since Huawei has been of concern for, you know, more than a decade?

Scott Kennedy: OK. Thank you both. Excellent questions. Thoughtful answers. Interesting framing. We're now going to turn over to the yes team and let you all ask questions of the no team.

Dan David: I'll just ask a question for either of you. As it stands right now, in current situation, with our cooperation on legal issues, legal matters, do you think that Huawei would pose a national security threat to our 5G network?

Paul Triolo: We don't have any Huawei equipment in our 5G network.

Dan David: I said, do you think they would pose a national security threat in our 5G network?

Paul Triolo: It would depend on – it would depend on all these other issues that we've discussed about how the – what the approach would be. Whether the European approach was taken. Whether things were wide open, what type of restrictions were place on the company in terms of where its equipment could be. So there are so many factors there that – and, again, I think – again, I would leave it up to the carriers to make that determination. It's not something that you could make without understanding how that equipment was deployed, where it was deployed, and, you know, what the circumstances were around that. So I think it's kind of a – it's an interesting hypothetical, but I think the details there would really matter – as they do in Europe too.

Martijn Rasser: So you would leave it up to private industry to make decisions with extreme national security consequences? Don't you see the state as having a role to play?

Paul Triolo: Well, as is the case in Europe, the European governments are heavily involved in determining standards for things 5G supply chains and in determining how equipment is used in their networks. So I would – I would argue that the European approach that combines public and private discussions around the issue is the approach that seems to be the most balanced in terms of taking into account both national security and realities of supply chain costs, for example. So in Europe, it's very much a government and private sector enterprise. As I mentioned, the U.K. government discusses these issues with the carriers. This is happening in Germany and other countries in Europe, in France and in the Netherlands, for example. So, yeah, the government has a key role to play, but the government is trying to balance industry concerns and global supply chain realities. And that, I think, is the most productive approach.

Dan David: So within the 5G network, as it stands now, trying to – I'm not – (laughs) – it turns out, I couldn't become a national security expert in the last two weeks. It just didn't work out for me. Or an expert on Huawei, even though the news flow in Huawei was incredible over the last two weeks. It was a full-time job. It's been – it's been ridiculous, actually. I think part of inundating us has been ridiculous with this news. But with the 5G new ecosystem, it's a gamechanger, right? It's not just from 3G to 4G. 4G to 5G's a gamechanger, correct? So now anything entering that ecosystem really changes the game as far as finding where the errors could be, or where the malware could be, or how hard security could be and detection could be, is what I'm hearing from our national security apparatus. Is that true?

Paul Triolo: Well, I think – first of all, I think it's important to note that, you know, in addition to the news in the last couple weeks about Huawei, we've had a – we've had news about major cyber campaigns conducted against U.S. companies and European companies around the world by advanced threat – advanced persistent threat actors. And those have all occurred way above the level of, for example, the vendor. So those have all occurred in the cloud. This is where typically most of the vulnerability and the intrusions and cybersecurity issues are found. They're found well above the network level of particular equipment. In some cases, it doesn't really matter what the equipment is. The intrusions are all happening at a very high level in the network, and in this case particularly among mobile providers and in the cloud. And so that's sort of, I think, the perspective that's important to note.

5G is a gamechanger, yeah, because there's – there are many more devices that will be connected. There's a lot of machine-to-machine communication, there'll be more critical infrastructure data flying around in 5G. And so that requires a really hard look at supply chains, but, more importantly, about the sort of – again, the overall security posture of the

network. And 5G standards, for example, build in already of course – build in a lot of security. And then really – but the real burden for security around network and end-to-end falls, again, on the carriers and on the customers, and the individual needs of the individual customers that are – that are using those networks. So, again, the vendor part of it is important, but it's only a small part of this much broader security posture that will have to be adopted, and will be adopted, around 5G applications and networks.

Martijn Rasser: Erin, one of the main counterpoints that Huawei, Ren in particular, has made as far as addressing security concerns is that he would never allow Huawei to do anything contrary to their customers' interests. Do you believe that Huawei would be able to defy Beijing's orders if the intelligence or military agencies would tell him to do certain things?

Erin Ennis: I guess I would challenge any company that is operating anywhere in the world to violate the law or a request of the government in the market in which they are operating.

Martijn Rasser: Unless companies have legal recourse.

Erin Ennis: I think that argument is a ridiculous argument when it comes right down to it.

Martijn Rasser: Come on. U.S. companies have a legal recourse. They do not have to do what the FBI tells them to with their products. They're not forced to install backdoors. A U.S. intelligence agency cannot order people to do that. It's different in China.

Erin Ennis: So I guess what I'm asking you is, do you think that that is unique to Huawei?

Martijn Rasser: Well, Ren says so.

Erin Ennis: Do you think that there is any company operating in China's system or in Russia or in any other place where if the government says that they need to comply with a government order, that they have the ability to do that?

Martijn Rasser: I'm just telling you what the CEO of the company said.

Erin Ennis: I'm just putting this back to you. I'm saying this is not unique to Huawei. This is a condition of doing business overseas.

Martijn Rasser: But the CEO of the company is saying nothing to see here, I won't do it. Do you believe that? Do you believe him when he says that?

Erin Ennis: As I said, I don't think that that is a legitimate argument because, be it Huawei or any –

Martijn Rasser: I'm not the one making the argument. The CEO of Huawei says –

Erin Ennis: I am giving you my response, and I am saying that I do not agree with that statement that Mr. Ren has made.

Martijn Rasser: OK, I see. OK.

Erin Ennis: I believe that Huawei and any other company operating that market would have to comply with that kind of a request. That does not make it unique to Huawei. And as a consequence, the point that I have been trying to make here is that this is why the

solutions that we need to be having should not be to try to target an individual company. It needs to go after the quality of the products that Huawei is putting out. If it does not meet our standards, then we need to have the high standards that we put into it. But having the U.S. government intervene in a way that targets an individual company because it might have to comply with a request from the Chinese government means that we are targeting one company rather than addressing the broader issues of the rule of law or the security of the products.

Martijn Rasser: Well, the reason I believe Huawei is being singled out is because they are the national champion. There's really no alternative.

Erin Ennis: Well, there's lots of national champions, though.

Martijn Rasser: Not in telecommunications.

Erin Ennis: You don't think that ZTE was considered to be a national champion?

Martijn Rasser: Much smaller player than Huawei.

Erin Ennis: But nevertheless, a national champion. I mean, how you get defined as a national champion in China is that you become a strong large company. It's not actually a designation that you get as you are coming up. It is that you have risen through the ranks to be a large and market-dominating company. So, again, that standard, in itself, is what I'm saying should not be the criteria. There's plenty of national champions in China. But again, this is an issue from a business standpoint of what is the appropriate way to address security concerns about this individual company versus what the risk is to the United States. And my argument is that we are best in dealing with this by holding ourselves to the highest standards not only on security but on our own rule of law.

Dan David: Would you agree we don't have that standard today?

Erin Ennis: I'm not a tech expert, so I'll leave that one to Paul. (Laughs.)

Paul Triolo: Yeah, I mean, I think that when it comes to 5G supply chain security, there's been a tremendous amount of work done on that. And again, similarly in Europe, the Commission came out in March with guidelines for supply chain security that raised the bar. And this issue has become very salient in the last six months, and so I think the U.S. is tackling the issue, somewhat belatedly, of trying to determine how far back for example in supply chains one goes with concerns over the vendor and country of origin. So I think, yes, U.S. is moving towards setting a very high standard around supply chains. And I agree with Erin that that is the way to go, rather than, again, singling out a particular company. The standard should be applied to everybody. We've been telling China this for years, that the country of origin doesn't matter. And now we're singling out not just Huawei but other Chinese companies on the basis of what the Chinese view as very politically motivated criteria and not based on standards.

Dan David: I agree, too. We're moving toward it, but we're not there. And our national security agrees.

Scott Kennedy: Terrific. That was an excellent discussion. I really appreciate both teams asking and answering the questions as best they could.

We're now at closing statements. The yes team gets to decide whether you want to go first with your closing statement or whether you'd have the no team go first.

OK, so we'll have the no team go first. Five minutes, and floor is yours.

Erin Ennis: So I'm sure it's going to surprise all of you that when I was in high school I was on my debate team. One of the things that I think my remnants of those years is that you always came down to which arguments were asked and answered, so were they rebutted or not. In this discussion, the question that has not been answered is why the United States government should be targeting an individual company, and what the consequences are of that.

I think the answer to that is clear. We need to set high standards, we need to hold ourselves to the highest quality of security standards for those things, but also the highest standard of what the rule of law is in this. That is not only because that's who we are as a country and that's how our economy and our system has worked well, but it's also because that means that we are holding other governments to the exact same standard. We should not want to target an individual company here, lest one of the other American companies that is in technology or any other area around the world will be the next target in China or any other market around the world. That is a cost that will be serious for us. And I think that it will actually undermine our innovation leadership in the world. We cannot cut ourselves off from these issues, but we can push everyone to a higher standard. And that's where we should be going.

Paul Triolo: I would just add I think that the focus should be on the consequences, the unintended consequences. So I think that the costs, unintended or intended, of a decision to target an individual company will be felt globally. They'll be felt in Europe. They'll be felt in – we haven't even talked about the developing world, where I think the only country in Africa that doesn't have Huawei equipment is Rwanda. So I think the sort of cascading costs of a decision like this, we really don't really know fully what they are, but they're substantial both as I mentioned for the sort of global infrastructure that is depending right now on infrastructure equipment from Huawei, and then, again, on the supplier side.

I think the consequences of this kind of a decision have to really be looked at the second- and third- and fourth-order effects, and particularly the impact on U.S. industry and its ability to innovate, which also has national security issues around it. So the issue I think is really important to get at all aspects of this complicated problem. But I think there hasn't been enough attention on the consequences. And part of that is because some of them are unknown, because, again, a year ago nobody was thinking about this issue. The 5G industry was moving forward with the plans to deploy 5G and standards were being set, and now all of that has been called in to question because of this U.S. government action. And I think part of the challenge is, as I mentioned earlier, finding that middle ground that balances the national security concerns with the sort of global realities of this issue.

I think, interestingly, when I was in Europe a couple months ago and talking with some foreign ministry officials from various European countries, they said, gee, it would have been nice to have this discussion three years ago. Now the U.S. is coming out with concerns about Huawei at a point where 50 to 70 percent of European infrastructure is built on that company's equipment. And so this makes the issue much more complicated.

It's easy for the U.S. to be pushing this issue without an installed base in the U.S. of any consequence of Chinese equipment. But for Europeans and for virtually every other region – Latin America, Africa, Middle East – this issue is very salient and has – and the costs and consequences of the decision around Huawei and the entity list have huge ramifications. So I think that's where we're coming from.

I haven't really heard a good argument about – I've heard something like, well, U.S. companies will have to pay the costs. But who's going to pay for all these other countries to have to tear out equipment and replace it and lose any chance, for example, to deploy 5G in a more timely fashion? And even before this, the costs of rolling out 5G were going to be substantial and they were going to be difficult decisions, but now this has added a whole 'nother layer to that.

Scott Kennedy: All right. Thank you. I'll turn to the yes team for your concluding remarks.

Martijn Rasser: All right. Thank you.

Again, the relationship of Huawei with the Chinese state and the quality and security of its equipment fully justify the actions the U.S. government has taken. Given the foundational role 5G technologies will play in our economy and the impact it has on our national security, there simply is no other viable option at this time.

That said, the situation we face today should also be a call to action, right? U.S. policymakers and business leaders have the opportunity to build a foundation for American preeminence in the technologies that come after 5G. So we must be able to provide secure and cost-effective alternatives to the global market – the innovation that you spoke about. Many of the challenges with 5G the United States is dealing with today were avoidable with more prudent planning a decade ago. With decisive action now the U.S. can ensure its status as an undisputed leader in wireless technology over the next decade. Policymakers and business leaders should make it a goal to ensure that the U.S. produces the most capable, reliable and secure full tech stack communications solutions by the end of the next decade.

So this means devoting resources to research and development of next-generation technologies and exploring strategies such as network virtualization. In doing so, the U.S. will lock in the ability to build secure critical infrastructure for ourselves, allies, partners around the world, with all the economic and national security benefits that go with it. And with that, I turn to Dan for the final word.

Dan David: Thank you. I was not on the debate team on high school, but I would say that we all seem to agree that the answer is yes; that until changes have been made, legal structures have been made, agreements have been made, Huawei should be restricted. If those agreements have been made, then maybe we're on that side. Erin has made some very good points where that's concerned; that there is a pathway. We're just not there. And they've agreed with us many, many times in this debate.

In the media, however, somehow the issue of Huawei and China, for that matter, has been framed in a way that makes us seem to have to make the choice on whether Huawei and its people are good or bad, or whether China and its people are good or bad. And I take great exception with this. We're not saying Huawei is a good or a bad company, and its people are good or bad. I take great exception to the thinking that we're saying that Huawei's employees are dishonest or somehow the people of China are bad. I don't

believe that at all. I want nothing but peace and prosperity for the people of China, and I truly believe that. And I truly believe that that's what they want for our people, as well. That's not why we're here today.

No, our problem is not with Huawei's employees. Our problem – and the reason we're here – is our governments are completely incompatible on a national security level, and Huawei can be coopted by the PRC government at any time. We all agree on that. They can be coopted by the PRC government at any time. And any person in China, even running a company like Huawei, who values their freedom and their life, will do whatever the government tells them to do. It's just that simple.

On an emotional level, I would love to live in a world where we can reasonable have no doubts about Huawei or China spying and hacking on us, but that's not the world we live in; that's the world we wished we lived in. And the matters of national security – we have to set aside emotions and get to the facts. The fact is China has engaged in state-sponsored IP and innovation theft and continues to do so. China forces technology transfers through acquisitions and continues to do so. China has committed massive amounts of fraud on our financial markets and continues to do so. China spies on the United States, its people, and its corporations, and continues to do so. And you know what? The United States does the same thing in many cases. That's right. There are no good guys in this movie.

So I would point out one difference; that our spy agencies are accountable to a democratically elected government and could not coopt a public or private company to work for the CIA, but let's call it like it is. This is our relationship. We spy on each other. We don't have a good relationship. And I don't care. The best piece of wonderful chocolate cake at Mar-a-Lago is not going to change that. (Laughter.)

So rather than taking a national security position on this is what our relationship should be, this is how the world should work, we must be in the here and now, and make national security decisions in the here and now, not just in the hopes of a better future, but in the reality of today. In the reality of today, today China and the United States are further from national security cooperation than we were 15 years ago when we had so much hope for a democratic – a more democratic China. Today, China is more committed to communism with Chinese characteristics than ever. Today, China is committed to military parity with the United States. Today, China is committed to mass surveillance, social scoring, no freedoms of press – especially ones critical of the government or President Xi. They are fine with criticizing us and our press – Huawei taking a full-page ad in The New York Times criticizing us. You can do that here; we can't do that there.

Today, China is the lifeblood of North Korea and flouts sanctions to Iran. Today, the courts in China are still controlled by the government, civilly and criminally. Today, China's President Xi has done away with term limits. These are growing, fundamental differences between our countries.

In the United States, presidents will come and go. There will be no doing away with term limits – I don't care who says what. Presidents will come and go. Members and Congress will come, they will stay far too long, but they will go. (Laughter.) What is consistent, however, is our national security – the FBI, the CIA, the NSA – and our military who all agree that Huawei should not at this point play a critical role in our infrastructure or our energy grid, for that matter.

Our politicians must listen to our national security advisors and, once and for all, we must stop trying to make China more like America by giving them America. Globalism at any cost is to know the price of everything today and the value of nothing in the future. China is willing to pay any price today for their future values. When will our future values be worth paying for again?

Scott Kennedy: OK.

Dan David: Every day brings a new chance to get it right; that's what I love about the United States. Tomorrow is another day. Let's get it right.

Scott Kennedy: Super.

Dan David: Thank you.

Scott Kennedy: Thank you. Both teams have done a tremendous job. (Applause.) First of all, let's give both teams a round of applause. (Applause.)

We still have several minutes left. The next thing that we're going to do is we're going to – you both did great, but we want to see how the audience was moved, in one direction or another, so we've got the voting up again. And please choose which side you agree with. We'll give you a few more seconds to make a choice.

(Pause.)

So then we can take that one, and we can put up the slide from before, and we can show where the results were originally.

(Pause.)

OK, so here we are. So the yes team increased their support by 4 percent, so congratulations in persuading a few members of the jury – (laughter) – out here. But I think what – although not a whole lot of opinion – minds were changed, I think what we did do is put a whole lot of evidence on the table on both sides of this issue.

We have time for a few questions, and so if you've – we'll let the audience now ask questions. If you would identify yourself and keep your question to a question, that would be terrific.

We're going to come right over here. This gentleman –

Q: Thanks, David Lynch with The Washington Post.

President Trump has suggested he is ready to bargain over Huawei in order to get a trade deal. Would a viable compromise or the sort of middle ground that Paul mentioned potentially be keeping Huawei out of the U.S. network and presumably out of allied networks, but allowing U.S. companies to continue supplying Huawei? So, in other words, preserve the executive order that the president issued, but do away with the entity list designation.

Martijn Rasser: I think that would be mistake. I think both should be kept. This is not a bargaining chip in the trade dispute that we have in China; it's a national security concern and, you know,

unfortunately the administration's messaging on the issue has been a little muddled, conflating the national security and the economic aspects, but they should be kept separate. This Huawei issue should not be a negotiating tactic.

Scott Kennedy: Do you want to chime in?

Paul Triolo: Yeah, I think – (laughs) – a good question. I think there's a potential off-ramp here that could allow this – the Huawei to be removed from any list because that's what the Chinese have intimated will be required to get a trade deal. So fortunately or unfortunately, the Huawei issue now is deeply intertwined with the trade issue because both sides now are talking in those terms. So I think that makes the search for some sort of middle ground here, for some sort of a viable off-ramp necessary.

Now it's very complicated because Huawei would have to come and agree to some sort of admission of guilt over the legal charges that led to the entity listing, agree to pay some sort of fine, and then agree to some sort of other conditions around some of the issues we have discussed today – around subsidies and around, you know, market access, and other issues.

So I think that the problem is it's – these issues are sort of outside of the trade realm, and so the – in terms of the discussions, but they are intimately linked now. So I think that's going to be the challenge coming out of the G20 – is figuring out is there room for trying to find a creative solution to this that meets all of these conditions and doesn't lead to – you know, to both the trade talks and the Huawei case being – you know, going forward as is because I think right now we're on a path to further decoupling, and to further impact on U.S. industry, and sort of a downward spiral in the relationship without resolving the Huawei issue.

Scott Kennedy: OK. We have time for one more question. We're going to come right here to this woman in the middle.

Q: (Off mic.)

Scott Kennedy: If you would just wait for the microphone and then identify yourself and your organization.

Q: Sure. Thank you. My name is Ling Shingu (ph), graduate student from Johns Hopkins University.

I have a quick question for you, too, because based on – although you hold very different attitudes towards yes or no towards Huawei, but from your debate it's obvious that you also agree upon some common ground, and I wonder, you know, based on that, when it comes to the real actions and, you know, specific measurements, we – you know, what things and which measurements would you agree upon, you know, to take from U.S. towards Huawei?

Thank you.

Scott Kennedy: Maybe Erin, do you want to identify what you thought the sources of common ground?

Erin Ennis: Yeah, I mean, I think we are all in agreement that Huawei's products have security flaws, and really, the only question is what the best way is to address that. You know, again,

from the business community's point of view, it needs to be a consistent standard, you know, it needs to not be company or country specific because when you go down that path of targeting individual companies, you are opening up American companies to having similar standards held against them in foreign markets.

I will leave the gentlemen to talk about what the security standards might be that would need to be set for that, but that is – the bottom line is it has got to be not country or company specific. (Audio break.)

Scott Kennedy: OK. This has been a fantastic discussion, and I think a lot of the disagreement comes down to whether you want to emphasize the question restrict – the word restrict or do you want to emphasize the word severely. You know, precisely where to you draw the line, and how do you – can you mitigate the risk by allowing Huawei into the system to some extent, or is that mitigation – really, is that not anywhere close enough. And I think we at least now understand precisely sort of what are the lines of that and what questions we would need to pursue to come to that understanding.

I think we also have discussed what the potential costs are of either option, both in terms of national security and commercially. It's not just one is a national security argument and another is a commercial argument. There's on both sides which makes this difficult.

And I think from our perspective it is – you know, if the president were to ask, what should I do, that we would be able to present a nuanced explanation of these risks of either action and then propose the best course of action.

I think we have identified what we need to do in terms of coming to a place where we'll be able to make those kind of recommendations. Obviously, this is a moving target going very quickly. Who knows what is going to happen in the next few hours in Osaka on the other side of the world. That could affect this.

MR.: I'll be up late tonight.

Scott Kennedy: Yeah. Yes, you will. And I would just second exactly what Dan said. We are all very, very busy following all of this, but we appreciate that this needs to be a public policy conversation, and we're going to continue to work on that.

I want to thank the audience, our CSIS staff – particularly in the Freeman Chair – who helped out today. And I want to thank the debaters, who did a fantastic job.

So if everyone could please join me in thanking our guests. (Applause.)

(END)