THE BROOKINGS INSTITUTION

WEBINAR

EXAMINING CHINA'S TELECOMMUNICATIONS AMBITIONS

Washington, D.C.

Wednesday, April 28, 2021

PARTICIPANTS:

Moderator:

MICHAEL E. O'HANLON
Senior Fellow and Co-Director, Center for
Security, Strategy, and Technology
The Brookings Institution

Panelists:

EMILY de LA BRUYERE
Horizon Advisory
Senior Fellow, Foundation for Defense of
Democracies

KEVIN MCGUINESS
Former DoD SkillBridge Extern
Center for East Asia Policy Studies
The Brookings Institution

NATHAN PICARSIC
Co-Founder, Horizon Advisory
Senior Fellow, Foundation for Defense of Democracies

* * * * *

P R O C E E D I N G S

MR. O'HANLON: Good morning everyone, and welcome to Brookings. I'm Mike O'Hanlon with the Foreign Policy Program and I have a real privilege today, essentially pinch hitting for a colleague who's got into the administration, Rush Doshi, and who is the co-author of two outstanding papers with the great panel we have this morning as the other co-authors. It's a remarkable set of people who have remarkable talents, tend to have excellent Chinese language skills, excellent research and technical skills really do put their nose to the grindstone of understanding China's role in global telecommunications, the stakes, the history of how we should think about the importance of sort of the high frontier of new technology and global communications even going back to the 19th century and what that may tell us today.

But also the kinds of strategies China is using today and the way in which its own domestic discourse within its country. Chinese speaking to Chinese reveal a lot more perhaps about the real intentions or their awareness of the nationalistic stakes that we may hear from more international and English-language kind of discourse that reaches us.

So that's the broad set of issues and things we're going to hear about today. Again, Rush Doshi who is now at the National Security Council was important co-author of both these papers while he was at Brookings as a postdoc. And we are very grateful for his work. But I also would like briefly to introduce the other writers and speakers today who again, are all remarkable, young scholars.

And one of them I've had the privilege of knowing for about a decade, Emily de la Bruyere. She helped create Horizon Advisory, which is an organization that she and another panelist, Nate Picarsic have built up really to do cutting-edge research on Chinese language documents that reveal and help us understand more about China's ambitions as a global power. And the ability to go straight to the source and straight to the actual documents as they've been written often by the Chinese for other Chinese or sort of before they've been filtered or translated or otherwise adjusted in English is I think one of the most fruitful ways to really get at the nature of the competition we are now in with China.

By the way, I say this not as an uber China hawk, and as someone who personally has been a little concerned that we may overdo it in our national haste to view China as the next adversary. But I'm not concerned that anything about today's panels or panelists or papers is pushing us in that direction. What it's doing is providing information and hard-edged technical analysis of what's going on.

So with another scholar, John Ferguson, actually a young, even younger undergrad at Harvard, they wrote a paper, Emily, and Nate, and John, and Rush, on how to compare and understand China's internal communications versus its external communications and if you will, public relations in terms of what importance China ascribes to the high-technology competition, the 5G competition the Huawei issue, and so forth.

But before they speak, Kevin McGuiness, who was the other co-author of the other paper with Rush, is going to put things in historical perspective. And I also really like this paper. I recommend them both. They are both on the Brookings website. And this paper traces back to the 19th century when the telegraph and undersea cables were first making their entrée and they were making their arrival as an important means of national power. And one thing Kevin will do is help us understand for example how Britain's dominance of those technologies actually affected the course and outcomes of both world wars. And so these are not small issues that we are discussing today, the high frontier of telecommunications.

So thank you for indulging me that brief introduction. And without further ado, I will now turn to Kevin to speak first about his paper on history. And then we will hear from Emily and Nate thinking and talking about more recent Chinese strategies on telecommunications.

We'll look for thereafter to some discussion between the panelists and your questions, which you can still send in even at this point, to events@brookings.edu. And they will be fed to me so I can then pose them to the panelists. Without further ado, thank you everyone for joining us. Thank you especially to Nate, Kevin, and Emily. And Kevin, over to you.

MR. MCGUINESS: Thank you very much, Mike. Also wanted to thank everybody here at Brookings for kind of helping put on this this webinar. So really appreciate all the folks behind the things with the technical issues, kind of troubleshooting, helping us out. So thank you, guys.

So I'll kind of go over a little bit of perspective on the report, kind of what led us to that and cover some of the key findings or lessons from a historical perspective that we kind of relate to the modern discussion on Huawei. So I think when we started this project there was a tendency to kind of bifurcate telecom industry and technologies and national security into different conceptual buckets, especially as we consider options of 5G development and the evolution of next gen infrastructure. It's sometimes easy to look at this just from the angle of tech innovation.

Now, when I'm just kind of downloading soccer matches or streaming music or reading articles, not necessarily thinking about the mechanisms of national security or state competition. I'm big about cost of services, capabilities of tech, things like download speeds, network services. But kind of as a holistic view, that's kind of shortsighted. And to truly framed the issue surrounding Huawei on really CCP governance or behavior by extension, we wanted to build off the history of telecom. So the intent behind our research and report was really to contextualize the current dialogue and discourse here on Huawei and telecommunications competition.

Reflected in these case studies in historical analogs are really that national security components and the link to telecommunications competition is not new. There is an inextricable linkage between power, state power, and telecommunications advantages. And that is definitely not new.

So our historical case studies, I always kind of like to lead with a little bit of disclaimer. These are not prescriptive, but they do offer invaluable lessons that help provide context to the contemporary debate. Furthermore, the lessons that I will talk about from history segue a bit into the research findings that my colleagues will present here in a few minutes. So readers and audiences are really able to follow what we would expect from a historical residence and what behaviors are also expected, what internal CCP communications reveal and kind of what picture they paint.

So we followed the evolution of telecom technologies and their integration into great power competition specifically with parallel integration into warfare. Warfare is kind of the inevitable reality beyond periods of peacetime the kind of illustrate the complexities here with telecom competition. So communications have long been foundational to wartime strategies, but as telecommunications technologies were invented, as they evolved, they became integral to, inseparable from military strategy and national security.

Just something that I would also like to say for additional context to keep in the back of your mind, is that modern military strategy, doctoring capabilities are all built upon ICT advantages. Information and communications technology is the foundation of modern warfare. And while not completely within the scope of this current conversation, it is a domain of warfare and that's what's in the PLA doctrine too.

So our report focused in on a few different case studies across history that illustrated a few key themes that was saw echoed repeatedly across the evolution of telecommunication. So we started out looking at case studies during the Spanish-American War which kind of revealed that this concept of neutrality is more of a dream. It's not really holding up in reality. So we talk about neutrality of telecommunications, it doesn't really hold up. So in the Spanish-American War specifically, undersea telecommunications cables were cut when the United States and Spain entered into a great power conflict often to the detriment -- the United States cut cables in the battle of the Philippines that also would've impacted their own abilities to communicate. But it was perceived to be more of a disadvantage for the Spanish. So the United States pursued that strategy anyway.

So the next kind of historical period that we look at in the report is the Anglo-German rivalry leading up to World War I. In this kind of illustrates the power of standard-setting. So during this period of time the British were able to essentially monopolize different telecommunications technologies infrastructure and translate that into wartime advantages as the -- kind of the globe walked into World War I. So Britain, in World War I also illustrated this pursuit of information advantages, having a

monopoly on those technologies and powers. And that really enabled their successes in World War I and led us do the period post-World War I as well.

We also focused a bit on German victories at the Battle of Tannenberg and World War I against the Russians, which illustrates the dangers of interception, lax standards, and really user error when it comes to emergent technologies, encryptions, or just protecting your own networks. Following that we looked at World War II, kind of the activities related to the Enigma and the Lorenz ciphers, how user error, complacency for example on the side of the Germans led to the British being able to break their ciphers and really exploit that to their advantage. Also kind of U.S. abilities to the same to the Japanese purple cipher in the Pacific region.

The final kind of case study we often talked about in depth in the report is actually kind of focusing on the Cold War being a U.S. operation called Ivy Bells where the United States were able to infiltrate Soviet controlled territories and waters and actually develop technologies, equipment, and capabilities that were able to provide or place a tap essentially on Soviet communications that were left unencrypted. And the advantages of that -- a lot of that is still classified, kind of what we are talking about today. But the stuff that is open source revealed it yielded significant espionage related advantages for U.S. and its allies in the Cold War.

So we focus on this case studies. We got a little bit into contemporary discussion over Russian activities in Georgia and the Ukraine, Chinese activities, things that are kind of all out there in the public domain right now of telecommunications evolution and how this has been integrated into political power, into state power, cross it every fundamental developmental period of telecommunications.

And we came up with a few key findings. I will kind of just talk about them real briefly right now. We can go further into Q&A if individuals read the report and have further questions. But the main kind of key findings that we're talking about is things like control over global telecommunications networks. It is political power. British dominance in undersea cables, land-based network infrastructure, they were all able to leverage stuff for economic primacy and military advantage. And that's leading through World War I.

Telecommunications networks have never been politically neutral. From their conception, even the most idealistic promises of states, to include the United States, that they would leave this out of great power competition or conflict, that didn't hold up as soon as these countries started coming to blows or actually got into conflicts. The United States cut cables in the Spanish-American war after kind of pledging net neutrality, or their version of net neutrality or telecommunications neutrality previous to that.

Another kind of key finding that is important for today's discussion is long periods of peace generally lead to complacency. And this complacency leads to telecommunications risks. And this is kind of echoed in the historical period leading up to World War I, the dawn of telecommunications. Great Britain benefited from complacency of others, exploited their nodal positions, forced the German traffic onto British networks in World War I, and it really translated into their strategic advantages in wartime periods and postwar time periods as well. And states that are complacent about that telecommunication security like the Germans were in this Anglo-German rivalry, the results can be disastrous and reshape world politics. So in addition to Germany complacency and reliance on British networks, Russian indiscipline in radio telegraphy during -- or wireless telegraphy in their battles also spelled disaster for their strategic ends.

Another kind of component for folks to kind of consider in this – kind of the same color here, states seek their own telecommunications champion when they realize they are at a disadvantage. Kind of like the CCP, the PRC, and Huawei today, when they are at a disadvantage states will use all instruments at their disposal to create this telecommunications champion and not rely on vulnerabilities of competitors. It introduces vulnerabilities into your own system, and it is a core component of national security strategy.

So the -- another way that manifests itself as actually a struggle for telecommunications standards. For example, in the Anglo-German rivalry, the British had a monopoly on the infrastructure of wireless telegraphy, the technologies, the Marconi systems, which essentially wouldn't communicate with other systems. So when Germany tried to create its own alternative to the British systems, they actually

weren't able to because radio nodes essentially would only communicate with its own standardized partner systems essentially. So other countries tried to get together and kind of set the standards to break that British monopoly. At the end of the day, the British had first mover kind of advantage. So they were able to kind of turn that into military advantage in World War I.

Another kind of echoed sentiment in this discussion on Huawei and evolution of telecommunications technology is that there are often advances in security or encryptions and things like that. The historical precedents really demonstrates that even though new technologies lead to advanced systems of encryption or increase the barrier to entry for adversaries to access the information or gain their own advantages, at each stage of evolution adversaries have always also evolutionized their way to intercept and exploit those technological advantages.

States turn to encryptions as interception becomes inevitable, but determination and user error have shown really time and time again that blind trust is misguided. Many states also discount the degree to which an adversary will go to compromise their networks. The United States went into Soviet territory and were able to tap undersea communications lines from the Russians. This was something they had to sneak past the enemy defenses to kind of go in and be able to enable, but they were committed to this process. The value was pretty great.

So discounting the links your adversary will go to, to explore your networks is only done at your own risk. Network security is not only about interception, it's about preventing the exploitation or denial of those services as well. So not only did the United States infiltrate Soviet territories to be able to exploit those technologies, but also, we have to consider the final lesson that we are talking about from these key historical findings is that the adversary's ability to leverage infrastructure and denial is also extremely important.

States use telecom as leveraged when they possess the capacity even if the actions pose harm to themselves. We see examples of this that countries will pursue whatever means are necessary to harm their adversary in the telecommunications sphere even if it might pose an issue to themselves. The ability to impact harm or affect harm on adversaries is much more desirable. So that's

something that we always have to consider when we are talking about lessons in telecommunications as well.

And I know we are going to get a little bit more into the discussion here when we do Q&A. So I would like to use this kind of quick summary to kind of turn it over to my colleagues here. But keeping all of this in the back of your mind paints a picture of expected behavior. So when you combine that with the internal communications of CCP, of the PRC in the telecommunications sphere, it kind of helps you to see a fuller and understand a better conceptual framework for looking at this issue with Huawei. So without further ado, I will turn it over to Emily and Nate. Thank you, guys, so much.

MR. O'HANLON: Thank you, Kevin. Let me just say a brief additional word by way of transition, which is I should have mentioned that Kevin is an Air Force veteran and a former professor at the Air Force Academy as well as his affiliation with Brookings.

And also, I really want to just summarize one quick take away I get from your paper, which is you don't necessarily need to attribute fundamental malevolence to China in order to expect them as a matter of great power behavior to try to exploit any advantages they have in telecommunication's. And maybe we will hear more from others about just how malevolent we should view China. But you don't have to necessarily view them as fundamentally evil.

A lot of the examples, Kevin, that you invoke are the good guys doing this. Or what we like to think of as the good guys, the United States, Britain, etc. So I thank you for the excellent paper and presentation.

And now indeed, Emily over to you. I should have said before that in addition to your affiliation and actually creation of Horizon, you and Nate are both at the Foundation for Defense of Democracies too. Thanks very much for joining us today, and over to you, my friend.

MS. DE LA BRUYERE: Thank you for the introduction. Also from the onset, I want to thank both Brookings for putting this together and also of course our co-authors, Rush Doshi and John Ferguson, who are not here today.

I think that teeing up of this as ICT as a domain of great power competition, there could not be a better place to start here. In the effort better to understand the stakes and nature and dynamics of today's ICT competition, we focus on China's lens, on the value that Beijing assigns to ICT in competition and how China goes about pursuing that value. What we find, perhaps unsurprisingly, is a competitive strategy, not the win-win discourse that's propagated internationally, but rather a competitor approach that treats emerging ICT systems as tools for power projection.

Broadly speaking, China's telecommunications and ICT ambitions exist as part of the larger cyber or network great power strategy. The strategy was first publicly raised by Xi Jinping in 2016. It is a global project and a competitive one. Effectively the cyber great power strategy is the blueprint according to which China seeks to shape the network standards and platforms of the Fourth Industrial Revolution.

Beijing pursues its ambition by deploying dedicated industrial policy. And industrial policy is a deliberate framing here. It's not scientific or technological policy per se because this approach looks really throughout the ICT industry chain. It doesn't focus primarily or only on -- or even most significantly on advanced technologies and their applications, but rather on the basic industrial and technological inputs into them.

So for example, industrial materials like rare earths, but also basic technologies like sensors and chips. These basic inputs are called core technologies within the Chinese discourse. And core technology is actually one of the fundamental pillars of the cyber great power strategy. A 2016 quote from Xi puts this framing neatly, “The control of core technologies by others is our biggest hidden danger. No matter how large an Internet company is, no matter how high its market value is, if it is heavily dependent on foreign countries for its core components and if the major artery of the supply chain is in the hands of others, it is like building a house on someone else's foundation.”

As this quote suggests, Beijing invests in these core inputs in order to foster asymmetric independence, in order to ensure autonomy within domestic supply and domestic industry chains while at the same time building positions of leverage within international ones, encouraging for example, Chinese

companies like Huawei to go out and to penetrate global market so that the international system becomes dependent even as China remains as relative independence.

In parallel with this industrial policy, Beijing also seeks to proliferate its ICT systems and standards and influence globally. It seeks to set the global rules or standards for ICT and the networks. This – I'm going to turn again to a quote from Xi Jinping in 2016, “We must accelerate the promotion of China's rulemaking power in cyberspace.” Chinese strategic discourse paints standards as a “commanding heights,” tools of which to lock in power. As Beijing sees it, the U.S. and Europe were able to set the standards in the last Industrial Revolution and that allowed them to submit architectural influence necessary to lead the global order. Now with the new industrial revolution taking shape, China has a chance to break that control, to compete to set the global systems. A new generation of rules is taking shape and Beijing wants to set them.

Should China's ICT project succeed, China would therefore, A, have asymmetric leverage over global ICT systems. Beijing would be able, for example, say to hold semiconductor supply at risk globally without facing reciprocal threats or breach other countries' networks without allowing its own to be similarly affected. More strategically, China would also be able to govern the emerging international ICT architecture, therefore granting its own commercial champions advantages, shaping how and where and what systems develop, and as a result, claiming both superior access to information and the ability to shape that information as well is the networks over which it transits.

So many of the concerns over Huawei and China's 5G ambitions in the past have really oriented around this question of spying and the risk of Chinese espionage. But the strategy here is bigger than spying. It's really about information enabled global control.

Finally, I also want to stress that Chinese strategic discourse suggest that such power, such control would be used and could be used for coercive ends across military and civilian domains with military and civilian tools. For example, domestic Chinese discourse treats commercial information networks like 5G as core elements of military civil fusion. This discourse suggests that those networks

could be used both to support kinetic operations and in order -- less kinetically or less traditionally, to disseminate propaganda and otherwise compete within the global order.

And on that note, I will hand it over to Nate.

MR. O'HANLON: Thanks Emily. And Nate, straight over to you.

MR. PICARSIC: Thank you, Mike. This range of insights from contemporary Chinese discourse that Emily has framed raises several policy relevant questions that we hope to report, and continued analysis can contribute to. China's approach to deriving strategic value from its commercial state champions is different from the approach pursued by other actors across the ICT landscape. And the nuance of that difference demands new thinking from U.S., allied, and private sector actors that need to grapple with China in technology competition.

Treating the domestic market as distinct from the foreign is not a novel framing for Chinese strategist. The fundamental economic development concept of two markets, two resources is premised on just that, realizing that the foreign marketplace is an opportunity to be seized while the domestic is an endowment to be protected. This asymmetric orientation toward the domestic and the foreign has shaped Chinese economic and technology strategy since the early 1980s, and it comes through clearing the messages that Beijing conveys about its ICT ambitions.

Take for example, industrial policy as Emily offered. At home, industrial policy is encouraged as the solution to the core technology vulnerabilities, while abroad Chinese firms are portrayed as normal, private sector profit seekers and not the beneficiary of the CCP's largess. They are meant to be treated like any other free-market participant despite the nonmarket support they enjoy in domestic discourse.

And it is clear that military and civilian networks are be understood as one in Chinese domestic discourse. But foreign messaging downplays any security risk that that reality may trigger in favor of emphasizing benefits to be delivered by the virtue of technology advance or low cost that Chinese vendors can offer.

And finally discourse on technical standards comes through clearly in Chinese discourse as an orienting objective across domains while China's overseas messaging for Huawei and others aims to strike chords of cooperation, collaboration, and win-win mutual benefit. This distinct set of voices and the asymmetric means that support them globally underscore the need for a competitive response from the United States. Lines of effort shouldn't actually start with competing in terms of narrative where reports like those that we are briefing today may provide a contribution as well as multilateral coordination of defensive and offensive mechanisms to compete with Chinese actors who have ties to the Chinese military, the Chinese surveillance state, and human rights abuses perpetrated in China and abroad while also shaping and amplifying investments as we look to build back better with allies, partners in the private sector.

And with that, we would like to thank our co-authors again, and Brookings for this opportunity to contribute to this timely and important dialogue.

MR. O'HANLON: Nate, thank you. And a question for you and for Emily and then you may just want to interact a little bit here before going to the audience questions of which there are quite a few. But I was just going to give you and Emily a chance after your excellent presentations to really drive it home and reiterate your top recommendation for American policymakers.

So beyond being aware of these trends and disparity between how China talks about and views this issue and essential strategy and is domestic discourse versus is the international public relations, was the most important thing we can do to be more resilient against this, to conquer this, to compete with this? And again, you've touched on these questions already, but I want to give you a chance to really underline them before we move on. We will be starting with you Nate, if we could. Or either way.

MS. DE LA BRUYERE: I might start if that's allowed.

MR. O'HANLON: Actually that's great. It's absolutely allowed.

MS. DE LA BRUYERE: Thank you for teeing this up. Two things I will focus on. First is industrial policy and industrial policy in an adversarial informed way across the industry chain. We know

that we have really critical dependencies when it comes to industrial and technological inputs. And we know that Beijing is ready to exploit those dependencies in order to accomplish its goals. And to that end, I think it's absolutely necessary that we, when we look at investing in ICT, invest at the basic input level as well as the flashy, shiny, high-end, high-value add level. That's going to require working with allies and partners, which is a theme undergirding all of this, because there -- we need allies and partners in order to find sources of the necessary inputs.

This leads to a next recommendation which is actually competing over ICT standards. For long time these have been framed as primarily a collaborative domain, but China does compete for standards. And China sees that as really integral to shaping the emerging architecture. So that means that we too have to treat this as a competition. And again, we too are going to have to do so in a multilateral fashion but because that's aligned with U.S. ideological approaches and because that's the only way we have the scale necessary to rival China's approach.

And in addition to competing with -- or to cooperating with allies and partners on this, is also going to require public-private partnership because we no longer exist in a world where countries are the dominant players in shaping standards or networks. Companies do that. And if we're going to have influence over these, and also to actually be able to scale their applications, that's going to require a new era of collaboration between the government and the private sector.

Those are my two cents.

MR. O'HANLON: Thank you. And Nate, would you like to add to Emily's excellent points?

MR. PICARSIC: Yeah, that was a fantastic answer. I think the only thing I would add is that we may want to pick about framing this competition less as a traditional innovation race where a fundamental breakthrough is our goal because the spoils in the broad ICT industrial change may go to those who can deploy and apply technology quickest and at scale.

So that means in the 5G case we looked at things like base stations and experimental deployment sites and nationwide networks as opposed to emphasizing, prioritizing funding, funding at a

more basic fundamental level of algorithmic and advanced and – grabbing patents. So I think there's a balance to be struck between realizing the role of technical standards and then also understanding the application race that we may be facing.

MR. O'HANLON: And presumably it's a race that may last the rest of our careers and the rest of your careers as young people. I don't sense that you're anticipating there's a certain finite time duration during which this happens. We may be at a crucial moment now but there could be many such future crucial moments too; is that correct, or do you really see the early to mid-2020s as maybe the key moments in the entire trajectory of the next few decades? To either one of you.

MS. De La BRUYERE: I'm going to answer with both of those things. I think we are at a pretty critical inflection point right now, and one that was probably accelerated by this past year of global health disaster because that's really seen a new recognition of the new systems taking form, and also an acceleration of their emergence.

And there are certain key foundational type standards in networks that maybe are going to be determined now whereas those built on top of them are going to be part of the next decades worth of process. That said, I absolutely agree that it's not like there's one quick, one year, window and then everything is decided. So this is an inflection point, it's really critical that we compete now but it's going to remain, yes, a race for the rest of our lives, careers, times.

MR. O'HANLON: Thank you. Nate?

MR. PICARSIC: I have nothing to add.

MR. O'HANLON: Well, let me go (inaudible) one more time and then what I'd like to do is just invite anybody else or all three of you who have a comment on each other's papers to do so and then we'll go to audience questions.

But specifically, Kevin, now to tie back to your paper. One of the things that you warned with Rush in your Huawei meets history examination of this whole domain of telecommunications from 1840 until 2021, great sweep and scope. You emphasize that it's especially dangerous when we're in sort of a period of complacency because we've had a long period of peace.

Are you at least partly reassured that as in the last five to seven to 10 years in the United States we've increasingly viewed the rise of China as a potential threat across many domains including technology that at least we're starting to, perhaps, mitigate that normal vulnerability and we're no longer in the sort of lackadaisical complacency that typifies long periods of great power and peace? Or do you still see us as just barely waking up with a very long race to go if we're going to avoid creating vulnerabilities?

MR. MCGUINESS: Thanks, that's a great question. I would agree. So, I would say the national security community and the consensus, as well as the intelligence community consensus is that this has been a significant concern for quite some time. I've been -- I started learning Chinese way back in undergrad, many, many years ago so my attention was always focused on China from a maybe different perspective.

But as I went through my career in the military you start seeing these changes and these emphasis items focused on China and that's, I think alleviates some of the concerns but kind of back to Emily and Nate's points is that 5G telecommunications infrastructure competition.

It's not just about the United States and what we can do. We're pretty resolved in our position on Huawei. The bans for Huawei in our telecommunications technologies, the NDA, the National Defense Authorization Act, from FY '19 to FY '20, it lays it out clearly our position.

The allies that we share interest with, some of them have adopted the same mentality as us and the same responses. The security concerns of Huawei isn't so much a discussion, I feel anymore, or at least in this core group of United States and some of our security partners, but it is the question for the broader global community not all governments are in the same position to be able to mitigate security concerns by banning Huawei or LTE technologies into their -- edge or their core infrastructure of their 5G technologies and systems.

So it is a less of a concern for one, I guess, now. But also more of a concern because of the global interconnectivity of all these systems that countries and other actors also need to consider the vulnerabilities introduced by incorporating these technologies. And again, they may not all be in a position to be able to outright ban so how do you now, amongst our allies and other partners that cannot

outright ban, how do you mitigate the risks? Because the global community, at least on telecommunications is connected.

So it's tough to kind of separate some of those things. It's not essentially a clear-cut barriers that oceans presented back in the day. It's everything is linked. And that's part of the concern of where we go from here when we do this evolution to 5G infrastructure and 5G technologies.

MR. O'HANLON: Excellent. Does anybody want to add anything at this juncture in the conversation before I go to audience questions?

Okay. If not, what I'm going to try to do is to group the question. And that way, rather than have each of the three of you respond to each question, if you have a notepad there, you can maybe each choose one or two.

Because one set of questions neatly organizes itself sort of naturally into a geographic kind of frame. There is a question about what is your set of findings and concerns mean for Pacific Command or Indo-Pacific Command in our operations fairly close to China. There is another question about how China is working in Africa and establishing various kinds of presence and infrastructure capability there. And how much that should concern us. There's a third question about the Middle East, which is essentially the same question, but for a different theatre.

There is a fourth about the Belt and Road Initiative which of course, can in theory, cover Africa and the Middle East but is more commonly and immediately associates, at least in my mind, with Southeast and South Asia and maybe Eastern Europe. And so any comments you would have on how we should think about Belt and Road.

And then, finally, space and satellites. To what extent do the concerns -- I mean, in one sense it's probably impossible to separate out the satellite dimension and you've all essentially been speaking to it already. But to the extent that we've been thinking a little more so far, about fiberoptic cable and some undersea communications to what extent should we think about satellites and space communications as a special arena of concern?

So that's a lot, but at least there's a geographic theme to the set of questions and maybe

ladies first. If you don't mind, I'll go first to Emily and then we'll just work back to Nate and Kevin. Over to you, my friend.

MS. DE LA BRUYERE: These -- they're broad. They prompt for me a couple of things. Starting with China -- a combination of One Belt, One Road, the Middle East, and Africa. You know, three particular points that I would raise in response to that. First, going back to your question about U.S. policy response. I'd like to think this is implicit in our responsive framing but part of the U.S. and its allies competing with China in ICT is having alternatives to Chinese systems. And right now, that's just not the case.

And Beijing is able to export its ICT companies and networks internationally with very little resistance, no matter the security concerns that exist, simply because there's no alternative for an African government that's looking for a low-cost 5G system or the necessary infrastructure inputs. And so this goes back to the idea of public/private partnership and industrial policy.

But it's really, really critical that we not just block Huawei in the U.S. and not just take defensive actions, but also be proactive about investing in global alternatives and scaling them. So that's like the scale context that exists.

There's also -- because I'm maintaining all my existing frameworks, the question of industrial inputs and how Beijing is able to leverage its international presence in Africa, in the Middle East in order to acquire those. And when you look at Chinese investments in Africa so many of them orient around capturing the critical mineral resources that are necessary for emerging industries, including ICT industries and on which the world depends. And China invests in these not only to meet its own needs but rather so that it can control the global market. And so when we look at China's industrial policy it's really critical that we factor in the investments that are made internationally.

And the final point I want to raise in response to these is on the space front. This is perhaps one of the strongest examples or most pointed examples of how China fuses military and civilian information infrastructures. And their uses and their development. BeiDou, China's base satellite system is treated in Chinese discourse as the paragon of military civil fusion. And it's largely organized and run

by military entities but then supported by civilian ones and it serves both military and commercial purposes and increasingly global applications are being built on top of it, both in China and elsewhere.

So if we want just sort of a really concrete example of what China's military civil fusion approach means in the ICT domain space might actually be the strongest and, perhaps, most unsettling of them. That's my disjointed answer.

MR. O'HANLON: Excellent. Excellent answer. Thank you. Nathan.

MR. PICARSIC: I may just pick up on this final point from Emily and look to point out that BeiDou and the space component here as a paragon of military civil fusion means that while this competition may largely play out as a long-term peace time competition, with economic warfare and commercial interaction at the fore, embedded in the way that China is going about their global expansion project whether it be BRI or in proliferating BeiDou and networks connecting to it, embedded in there is the risk that there are operational and kinetic risks for escalation embedded, and seemingly as China's discourse will tell us in their outward facing messaging, commercial and market-based actions.

Embedded in there are these risks for escalation and operational kinetic risks and that points out, I think, a key aspect of any narrative response that the U.S. government and allied and partner states may want to pursue is educating the private sector on those risks. So if you're incorporating BeiDou or if you're signing up to BRI information sharing agreements and cross-boarded data transfer flow agreements with the Chinese state or with Chinese military civil fusion actors, you may be incurring a latent cost, or a latent risk that, I think Chinese discourse would try to lead international players to ignore or not believe is there.

So I think this military civil fusion component, when we get to space, but I think it is also just as prevalent in the way the BRI infrastructure approach plays out more broadly. I think that's the one thing I can add.

MR. O'HANLON: Thank you very much. And Kevin, over to you.

MR. MCGUINESS: I guess that just leaves the Indo-Pac Con question for me. So I think, first of all, I mean, there's a lot of these things that are all integrated together; the concerns of civ-

mil fusion, the concerns of civilian industry and telecommunications exploitation advantage, all this kind of stuff even from a military perspective or from maybe a security perspective in the Indo-Pac Con region, the whole point of an historical lookback in the analogs is that this stuff is inextricably linked.

So if you're kind of an Indo-Pa Com geographic regions of authority or geographic regions of concern, particular challenges in that theater from a military perspective definitely relate to things like communications. I mentioned briefly at the beginning of my presentation that ICT is the foundation of modern warfare.

Cybertechnology, cyber is a domain of warfare, and that's not just from the United States perspective. If you take a look at China in the region and cyber being a domain with PLA warfare as well. And that's an evolution that's occurred across time, but something that I believe is firmly rooted in their doctrine nowadays, and how they look at the problem set of warfare.

So in the Indo-Pac Com region you're talking about a massive geographic area, right. The largest combatant command geography that kind of exists in the globe. So it's a lot of area to cover. And some of the predominant concerns you'd have to ask yourself if you're operating in that region with China or with whatever your interests are in that region or what are your vulnerabilities?

One of the ones we commonly think about, you know, in analogs back to historical precedents underground, or underwater, undersea maritime fiber optic cables, right? You have to take a look at what vulnerabilities exist that you have built your offensive capabilities or your power protection capabilities on. What communications infrastructures do you require to effectively operate across the region?

It's a massive geography and speed of communication is an extremely important consideration. When you're talking about generic scenarios across Indo-Pac Com one of the common refrains you see in modern discourse or current discourse is actually, you know, the PRCs intention across the Taiwan Strait. Reaction and ability to respond in real time are one of the significant variables in the calculus of PRC policy makers. And U.S. policy makers as well. So I would not expect anything in telecom to be off limits in any sort of situation. And that's what the historical precedence has

demonstrated, that if entities possess advantages or capabilities that give them an opportunity to apply leverage, you've seen that leverage applied time and time again regardless of their either nefarious or altruistic intent, when they need to, they apply that leverage.

So if you're susceptible or vulnerable to that leverage you're going to be in a position to have to work through that. So that's probably the main point I'd bring up when we're talking about maybe some of this stuff's applicability to Indo-Pac Com or the Pacific region in general.

MR. O'HANLON: Thank you. Thank you all.

And so now I'd like to go to a second round of questions which I think I'll keep a little bit shorter, so we have time for a third round and conclusion after that.

So one question comes from Michael Nelson at Carnegie Endowment and he asks what's a better metaphor for U.S. China tech tension, rather than saying tech Cold War, or digital decoupling? Do you have a framing that you would use? And of course, you've all already been speaking to this. But his specific question what's a better metaphor for tech tensions rather than tech cold war or digital decoupling?

And then, there is also a question about whether we should try to create or apply an international commission to control ICT standards and establish ICT standards, rather than sort of let the first mover or the predominant early mover essentially establish those de facto. Or is that illusory, or you know, idealistic and utopianistic to think that that's possible?

And then finally, there's a set of questions about -- well, I'll say there's some stuff on AI and revolutionary military affairs, but I'll save that for the final round. So why don't we leave those two questions on the table for now and maybe go in reverse order starting with Kevin?

MR. MCGUINESS: Yeah, absolutely. So the first one's a good question. In terms of the current situation I personally don't like to use the analogies that we're talking about different a rehash of the cold war. I think the variables there are way too different, and it kind of oversimplifies the comparison between what is going on between the United States and China.

The historical look in our report, the precedents -- I don't even know if it really needs any

more of an explicit label versus this is kind of the nature of the reality of telecommunications and its evolution. It's an area of competition, it's a domain of warfare. It is the stuff of kind of great power competition and what you would expect.

So that's the framework I look at it, and I think for me, and my perspective is more, of course, this is what's going to be occurring in this domain, in this realm. These are the behaviors that I would expect to see because these are the behaviors that I have seen in the past. And these are the behaviors that I have seen previously. So a lot of people sometimes try to draw parallels to the Anglo-German rivalry and that's a lot more, I think, applicable then perhaps a cold war 2.0 or some other issues that we've seen thrown out there.

So that's personally the way that I framed this reference. It's not always directly adversarial in nature, nor does it have to be, in my opinion directly adversarial in nature. But these are the areas at which we are concerned about, and we look to mitigate vulnerabilities and we look to, you know, develop our own advantages.

MR. O'HANLON: Great. Nate.

MR. PICARSIC: I may jump on the technical standards question, if I could, and avoid, or shirk the metaphor one. So I think in technical standards we do – there exists a range of international technical standard setting bodies. They function at one level with companies participating, and then also sort of having company to company negotiations and interoperability decision-making processes that help to flesh out those technical standards.

So I don't know that there is need for an overarching system to be more redundant than what exists now. I think there is a need for applying a security mindset and a strategic mindset to national and private sector approaches to those technical standard setting bodies that do exist. China clearly has its own playbook and national strategy for this. And I think that's something that can be developed both domestically in the United States and then alongside allies and partners. And I would look to entities like NATO as a vehicle that may have a role to play and latent capacity to contribute to the technical standard setting approach.

And while I agree with Kevin's reaction on the Cold War framing and don't want to endorse that, I would look to the Cold War analogy for multilateral modes of competitive cooperation like the COCOM, coordinating committee for multilateral export control where there may be a need for reinvigorated and updated models like COCOM to address not just export controls of technology but also the role that capital plays today in access to technology and influence in these critical product chains that we are thinking about.

And again, that's another area where there are some institutions that exist in what may lack is a coherent national strategy and one that can be pursued in a multilateral fashion.

MR. O'HANLON: Super. Thank you. Emily, anything to add?

MS. DE LA BRUYERE: I'd like to go quickly back to this metaphor thing. I agreed entirely with Kevin re Cold War framing, and this is not flashy, it definitely needs some work shopping. Something along the lines of a competition over integration is how I would see this which I think captures the idea that the competition in the Cold War largely took place in relatively isolated spheres. Whereas, in the current environment no matter how much we may want to talk about decoupling, we live in a world of exchange and the competition is very much one for the upper hand in that exchange.

And I think the idea of competing over integration captures within it both the question of asymmetric independence or dependence and the ability used not to weapon eyes that very integration if you have asymmetric upper hand, and the idea that were competing to shape a global architecture, which is fundamentally an architecture of integration and of exchange.

MR. O'HANLON: Excellent. So final round of questions, and please weave in any concluding remarks you might have as well in your answers to whichever of these you would each like to address. There are a couple of more from the audience and I'm going to add one more of my own.

The one from me is about domestic infrastructure because I think that while you've all touched on civil military fusion and the whole enchilada of our military and economic interests, we've tended to prioritize a little bit the military specific side of communications in the history of that. And what I'm wondering is in this cyber and digital age to what extent does 5G potentially allow China into the kinds

of railroads, and electricity grids, and air traffic control networks, and telecommunications systems up on which not only national economies, but military forces deploying abroad need to move on trains and planes in order to get where they're going. And so there is a big vulnerability here.

I just wanted to ask if you wanted to speak to that particular dimension of the question a little bit more emphatically or with a little bit more detail than you have so far.

And then, in terms of other questions from the crowd, there was a question about AI, and whether 5G is a key element herein. said the question specifically is does 5G technology assist in the early adoption of artificial intelligence in military affairs. So it's a big question but to what extent do you want to speak to that?

And then finally, what are your thoughts on the future of the so-called splinternet? And maybe, you know, in other words imagining, I suppose multiple internets and whether we're headed for that, should be headed for that as a way to ensure resilience. Maybe that links back to my question about domestic infrastructure and its digital dependability and resilience.

So I think that's the sum total of -- well, there's one last question about the Trump legacy and whether you see any particular consequences of four years of putting America first, or if that's now sort of receding, at least in this domain, too, you know, broader structural and technological trends and realities that really aren't so much a dominated by the particular style of our previous president?

Okay. So that's a lot. Please be selective, don't feel obliged to answer everything. But why don't we again start with Emily add then just go to Nate and Kevin as you wrap up.

MS. DE LA BRUYERE: Thank you. I'm going to focus on your question and will try to keep myself short on this one. But I just want to start off with a quote I think we have in our paper which I find very valuable for the overall framing. Which is from a Chinese state council researcher who says that, "A new generation of information technology revolution has made national security issues no longer limited to traditional military an economic security."

Now, and I'm going to paraphrase, the entire system is dependent on the Internet and that means that suddenly financial, commercial, transportation, communication, education, and health

care systems are all core parts of this security system depended on the Internet that can be at risk, or benefit from the overall competition. All of which is to say yes, absolutely, you know we've been talking about the military domain, but the point is that the commercial as well becomes a critical competitive and security element.

And I think this is where there's actually remarkable potential for U.S. policy. You know, with the new emphasis on build back better, and construction of domestic infrastructure there's actually a really remarkable confluence between those goals and also what we need to do to compete over emerging international architectures.

And then, within that overall framing there's also room to focus on this new emerging domain of kind of foundational information infrastructures that are, in turn, going to govern the physical world. 5G might be an example. There's another that we talk about a lot which is this Chinese IT logistics network that's designed as a hub to aggregate information on global logistic movement of goods. And that's something that's fundamentally commercial but that promises information advantages and control across all domains, With remarkable implications for national power.

And now, I have not been as concise as I would have liked to be. Over.

MR. O'HANLON: You were just fine. Thank you. Excellent answer. And Nathan, over to you.

MR. PICARSIC: Yeah. I think I would just echo those things and add that we see from the Chinese an emphasis on vertical integration in selective supply chains whether that's ICT for railroad. So if we think about the role of domestic infrastructure contributing to our logistical capacity either economically or in security terms it's necessary to look at not just the new and the emerging, whether that's industrial control systems or electronic braking systems for railroads, but it's also a look at the rolling stock, and do we have the capacity to generate the fundamental inputs that are needed to move things around. And the stark reality is that China's approach to vertical integration even in that, you know, relatively boring and less sexy field has really worked and they are the dominant player. Several of their state champions are the dominant player, just as we fear that this playbook may be applied in ICT, it's

already been applied across all these other realms where the Chinese approach to vertical integration has pushed our economic system to seek the highest value add, roll and run after the innovative advance that might break through the next thing, but we are left with building on a foundation that is largely controlled and influenced by Chinese industrial policy. And that exists in rare earths, that exists in the Poly Silicon that's needed for solar panels and for semiconductors. And it exists in ICT application technology like what we are discussing today.

MR. O'HANLON: Excellent. Thank you very much. And Kevin, for the last word of the day?

MR. MCGUINESS: I think all -- both of those responses kind of reiterate how blended everything is and how this concept of decoupling might not be physically or entirely possible. When we consider the evolution of 5G technology and the technologies more importantly that are enabled by this next foundational leap in capabilities in infrastructure it may not be possible to mitigate all the vulnerabilities that exist in the system. And it may not be possible to really insulate yourself and just kind of be worried about your own borders. This isn't as simple as a back in the day of telegraph lines that only sent messages across and were only used for communications. This is the foundation for everything that we have in our economy, in our society, it is extremely important. So to kind of touch again on a little bit different point that we talked about previously, and to maybe kind of answer the last question you had on the previous administration or different priorities, it has been acknowledged that there are security implications here, that there are economic considerations here, and the path forward, in my opinion, is like minded groups of allies, friends, partner nations, countries, governments, etc. that need or want to establish different ecosystems, or an ecosystem conducive to their interests and their values. What the ecosystem of Huawei existing within the CCP or the PRC may not be congruent with that. But to be able to have a different alternative would require consensus and cooperation, and a lot of concerted effort to be able to join your allies and kind of create partners in that endeavor.

MR. O'HANLON: Well, Emily, Nathan, and Kevin, thank you very much for an excellent discussion today; for your outstanding papers which again, can be found on the brookings.edu website,

and I recommend them strongly. They are also highly readable and have very nice executive summaries if you want to work your way in gradually, a couple of pages that really highlight the key findings, but they are well worth reading in their entirety.

I thank again our former colleague, Rush Doshi doing good things over at the NSC in this space. And I wish you all very much the best. And thanks to the audience for joining us as well as your excellent questions.

So signing off from Brookings, and best wishes for the rest of the day and the week.

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Carleton J. Anderson, III

(Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2024