Center for a
New American
Security

NOVEMBER 7, 2019

TRANSCRIPT FROM CNAS TECHNOLOGY & NATIONAL SECURITY PROGRAM EVENT

Report Launch Event: “Securing Our 5G Future”

Transcript from Report Launch Event: “Securing Our 5G Future”

I. Opening Remarks

Martijn Rasser: Welcome to the Center for a New American Security. My name is Martijn Rasser, I'm a Senior Fellow here in the Technology and National Security Program. It's my pleasure to host this event, the official launch of the Securing Our 5G Future Report. The report is excellent, it's informative, insightful, offers concrete policy recommendations. I think you'll enjoy reading it and I think you'll end up revisiting it quite often.

Martijn Rasser: It's no exaggeration to say that 5G is poised to bring about tremendous advances across a spectrum of industries. It's more than just improved mobile telephony. 5G is going to enable, greatly improve military communications, situational awareness, autonomous vehicles, virtual reality, telemedicine, and expansive device connectivity for a true Internet of Things. All of this is going to be possible due to the higher speed and capacity and lower latency of 5G networks. There will also almost certainly be innovations that we can't even conceive of today.

Martijn Rasser: 5G promises to be truly transformational and we're reminded of 5G's importance all the time. We see constant headlines about China's rise in 5G, the economic and national security risk 5G poses to the United States and its allies and partners.

Martijn Rasser: Just in the past few days we've seen China announce a 50-city rollout of 5G. The United States and Estonia issued a joint declaration on 5G security. Hungary signaled that it would allow Huawei on its 5G networks. At the same time, in Germany, legislators there have been pushing back on Chancellor Merkel's announcement that Huawei would be allowed in German networks. This report is extremely timely, and this event is very timely. We're very fortunate to have two 5G policy experts here with us to help us make sense of it all.

Martijn Rasser: First, I'd like to introduce Elsa Kania, author of the report. Among the many hats that she wears, she's an adjunct fellow here at the Center for a New American Security. Her accomplishments are extensive. Her writing is prolific. She truly is one of the world's foremost authorities on Chinese military technical innovation and it's great to have you here Elsa.

Martijn Rasser: To her left it Rob Strayer. Rob is the Deputy Assistant Secretary for Cyber and International Communications and Information Policy. In this pivotal role he leads development of international cybersecurity, internet data, and privacy policy with foreign governments. He truly is at the tip of the spear of U.S. foreign policy and 5G, and a leading thinker on global emerging technology issues. Rob, it's a pleasure as always to have you here at CNAS.

Martijn Rasser: I asked Elsa to kick off the discussion with an overview of her findings and her policy recommendations. After that, I'll turn it over to Rob to provide State Department's perspective on 5G security. After that, you, the audience, will have a chance to interact with Elsa and Rob through a moderated Q&A. With that Elsa, I turn it over to you.

II. The Securing Our 5G Future Report

Elsa Kania: Alright, well thank you so much for the very kind introduction and I thank you all for coming out this afternoon for what I hope will be a fairly engaging conversation on a topic that could not be more timely, almost too much so. As someone who was trying to finish a report, I couldn't help but hope things would slow down at least to keep up to speed. But it has been exciting and challenging to be trying to make sense of these policy issues at a time when these developments are taking shape and these issues are evolving so rapidly. I wanted to say as well my thanks to the host, CNAS Tech team, it's been a learning experience, an adventure for all of us diving into the world of 5G.

Elsa Kania: One of my hopes in this report was to think about how to change the conversation and continue to move forward as we think about how the United States can take full advantage of the opportunities and grapple with the unique challenges of 5G. As Martijn mentioned, we've seen China really emerge at the forefront of its deployment with, again, the launch just yesterday of work on 6G, not to mention starting to launch 5G service nationwide as of last week.

Elsa Kania: When we look at this overall landscape of U.S.-China strategic competition today it's become clear that emerging technologies are really at the heart and the center of it. We've seen this in conversations on artificial intelligence and quantum information science, and on biotechnology. And of course, 5G, particularly in the past couple of months has become quite a focus of these debates as well.

Elsa Kania: While it's been encouraging to see the U.S. government across many fronts and many lines of effort start to become more engaged and moving the conversation forward, I think there is still much work to be done in ensuring that the U.S. is fully prepared for a 5G future. For all of the talk in particular of the notion of a race to 5G, I think we're seeing this as going to be more of a marathon playing out in the years to come when it comes to the investments that are required to continue research, to sustain the deployment of 5G, and to look at the multifaceted challenges that will come into play, particularly when we look at a world in which Huawei, with all of the attendant concerns of security that accompany the global diffusion of its technology, is a major player. The U.S. has to continue to work and move forward as to how we ensure we are in a better position competitively, recognizing that there are at the same time so many American companies and other international companies, including among our allies and partners who have their own unique strengths in 5G.

Elsa Kania: As I tried to make sense of these issues and think about what lines of effort could start to come together as more a whole of nation strategy for 5G, I highlighted five particular directions. The first, being simply that we prioritize 5G and invest in it, recognizing that this is truly a critical foundation for American competitiveness. Whether we're talking about realizing the full potential of AI, future smart cities, self-driving vehicles, intelligent manufacturing, 5G is going to be really a foundation for that. Other issues in terms of the digital divide, of how we realize 5G has scaled beyond some of the initial launches we've seen in a small number of American cities.

Elsa Kania: I think that simply we've seen a National Security Commission on AI and AI Caucus, a lot of legislative initiatives starting to emerge in 5G as well. But I think there's much more that can be done to elevate this as a priority and to start to launch policy responses across

multiple fronts among all of the various stakeholders involved in industry and in government.

Elsa Kania: Secondly, I highlighted in the report that I think it's critical to ensure that 5G will be secure by design from the start, rather than racing to deploy it or in some cases, countries that are concerned about being left behind. Therefore, going with what is the cheapest, easiest option to start—which would be Huawei—thinking quite rigorously about the range of security concerns that could come into play, given that 5G really could magnify and intensify a lot of the concerns we've seen with the Internet of Things coming online, possibility of the multiplication of vulnerabilities in ways that have exponential threats, and on the cyber front. I think they're hopefully ways to learn lessons from current and prior challenges, and work to get things right in 5G, and make sure that security is part of the standards and the process, and the screening that should be applied to all vendors and carriers along the way.

Elsa Kania: Thirdly, I wanted to emphasize in the report the importance of contesting leadership and promoting innovation, both within and beyond 5G, recognizing that 5G is still in many respects a work in progress. The technology continues to take shape, including through the standard setting process under 3GPP.

Elsa Kania: A lot of talk these days of 6G, but 5G itself is still emerging in its potential, as well as the application. Even new industries that may build on top of it are still at a nascent stage. There are options for the U.S. to recognize that our current status quo in 5G in which China is certainly quite an essential player may not be optimal. There are options to explore ways to disrupt that and to innovate, including greater network virtualization, potential technical solutions, and of course, a lot of work that has to be done on some very practical measures in terms of spectrum sharing and new techniques to improve the availability of spectrum and ways that facilitate deployment at home. Of course, also under this umbrella, there are major concerns about supply chains in terms of their security and robustness, and how to ensure that we're moving towards more of a vibrant commercial ecosystem within the United States and allied companies worldwide.

Elsa Kania: Fourthly, coordinating and collaborating with allies and partners will be absolutely critical in 5G, and America first approaching this technology would fail to take advantage of the strengths and truly critical importance of working with companies and countries around the world that share our values and share our concerns on security. I think U.S. policies as well have to work to coordinate with allies and partners, both on shared responses to security, improving situational awareness, and providing positive alternatives to what Huawei has been marketing which is cheap and attractive to many countries, understandably, but may not be the best option in terms of security or longevity, and the benefits.

Elsa Kania: Finally, I think fifthly, when it comes to 5G there are both positive and negative externalities for security and from concerns about espionage targeting these technologies to ways in which these technologies can be a vector for such targeting. And of course, the national defense implications of 5G, which are considerable. As the U.S. military explores new directions and innovation, also perhaps exciting opportunities to start to experiment with 5G and how it might incorporate into future vital networks going forward.

Elsa Kania: Hopefully that's a decent overview of the report. It is rather lengthy, but I hope it makes for interesting reading all in all. I will very much look forward to your questions and the

conversation. I will now turn it over to Rob. Thank you all again for being here this afternoon.

Rob Strayer: Great, thanks. I'm going to use the podium if that's all right.

Martijn Rasser: Yeah.

Elsa Kania: Mm-hmm (affirmative).

Rob Strayer: I just sit down too much during the day, so trying to start up here.

III. 5G Security: U.S. Government Perspectives

Rob Strayer: First of all, Martijn, thanks a lot for that kind introduction. I want to thank the Center for a New American Security for sponsoring this event and the other events you've already hosted on 5G. I also wanted to thank Elsa for this excellent report, it's really the reason why we're here today for the thought-provoking points you've made in your presentation just now and the report itself, so I commend everyone to read that report.

Rob Strayer: I thought, Martijn, you hit the nail on the head at the front end by saying that it's not just transformative technology in our lives. It's going to be all the things we can't even imagine today that it will be used for, that tremendous amount of data and the processing of that data through machine learning and then artificial intelligence is going to mean for our lives, which makes this technology itself so critical, and not just with regard to the potential for there to be espionage or protect the confidentiality of that data. But because it's going to underpin so much of our future critical infrastructure, it's going to be the reliability of availability and integrity of that data to ensure that we have these many systems that provide services to the public and to businesses that need to be ensured by having a 5G network and a set of software that underpins that network that's something of the most high level of reliability.

Rob Strayer: In part, that is why we have a global effort to talk to our allies and partners about the importance of having a set of risk-based security standards in place to ensure that as their telecom operators build out the next generation of wireless technology that they are including important reviews in best practices on security. One of those security areas is the supply chain, that is the vendors who are putting in the hardware equipment, as well as the software that runs those systems. That includes not just the operating system software but the firmware that's on all those components in 5G networks.

Rob Strayer: We talk to countries about the importance of developing a set of policies that will ensure that they have trusted vendors providing technology in their networks. We of course recommend that there be a whole range of cybersecurity best practices adopted, including look at the configuration, the authentication, using encryption in appropriate ways. But it's also important that there be a fundamental trust relationship between the country and the operator and the vendor that's supplying this underlying technology.

Rob Strayer: It's a fundamental truth as we move forward with more and more software in all kinds of critical applications in life, including in 5G networks, that among the millions of lines of

code that we cannot detect all the vulnerabilities. In fact, we know of major companies who constantly have to patch their software and they're doing that in good faith. They are not intentionally inserting vulnerabilities. They are correcting vulnerabilities as they come to their attention.

Rob Strayer: We know that with regard to some of this technology in 5G, or at least in the 4G networks of today, that the United Kingdom through their Security Evaluation Center has already found that there are thousands of vulnerabilities in Huawei's equipment that they're deploying. In fact, they've created what is a bug door, so many bugs in the system that one can't tell whether those vulnerabilities are there innocently or there intentionally. In the future, it would be very easy to hide an intentional backdoor among these many bugs and vulnerabilities that exist in the software that a company like Huawei provides today. We need to be vigilant about the vendors that we're working with.

Rob Strayer: We think one of the most fundamental indicators of whether you can trust a company is the legal system that it operates under. Does it operate in the case of a company like Huawei and the Chinese Intelligence Law which requires all entities to cooperate with the security and intelligence services and to do so secretly. In addition, there's no way for a company in China to object to what it's being required to do by the Chinese Communist Party because there's no independent judiciary and there is in that sense no rule of law where American companies can object, and Western companies can object, to requirements that are being placed upon them by going into an independent judiciary that's not available in China. There's a fundamental difference in the construct under which Western companies operate and the contract under which the Chinese companies operate.

Rob Strayer: There's also a big fundamental difference in the transparency about ownership structure. Western companies often are publicly traded, they have to abide by a number of legal norms and legal requirements, everything from all kinds of requirements related to their financial accounting practices, as well as anti-corruption requirements on them.

Rob Strayer: Just recently, you had the most senior official at Huawei claiming that they were negotiating with U.S. companies to license their product to us. Then yesterday they came out and said, "No, no, we've not talked to any U.S. companies yet." I distinctly remember a CEO in Silicon Valley who claimed that he had someone about to buy a bunch of his technology and then was prosecuted by the Securities and Exchange Commission, so there's just a fundamental difference in how companies in China can operate than they can in the Western world.

Rob Strayer: We also think that it's important to look at the ability for a government to assert pressure or coercive pressure on a company. In the case of a company like Huawei there's the ability for the Chinese Communist Party to limit the financing. They have massive amounts of financing that come from the Chinese Export-Import bank and the Chinese Development Bank. In some cases, they're offering 0 percent interest for 20 years to earn contracts in countries around the world. They recently acknowledged that at least 20 percent of their financing just in Europe is coming from Chinese banks, so you can be assured that those are not on commercially reasonable terms that the rest of the companies in the ecosystem of 5G have to abide by. Therefore, it's easy for a government to say we're going to withdraw that financing if you don't cooperate with us on security and intelligence matters. We think it's a fundamental issue to look at the trust and not just best practices for cybersecurity.

Rob Strayer: It is also important to look at the history of what China has done when they have access to data. In the Xinjiang Province where Huawei is cooperating with the security services there, more than a million Uighurs are now in prison. That's in part done through sophisticated use, using facial recognition technology, to surveillance cameras.

Rob Strayer: There's also the use of data in the form of assigning social credit scores to people in China based on their activities and who they associate with. We've seen this facial recognition technology has been perfected by Huawei, and the digital ecosystem in China being exported to dozens of countries around the world. Again, they're doing this in the form of what they call 'safe cities.'

Rob Strayer: But the fundamental difference between what we do in the Western world is we apply a lens of rule of law and legal protections for individuals. That is not something that's on the priority list or anywhere I think in any ethical requirement that's required of Chinese companies.

Rob Strayer: There's also the issue of China's long history of intellectual property theft. There's a history of it with regard to Huawei for sure, but it's also something that's existed within Chinese major agenda—to steal intellectual U.S. property from U.S. companies, particularly to facilitate their 2025 campaign for being leaders in technology in a number of fields. U.S. Trade Representative and others have put out reports that show an alignment between areas of major intellectual property theft and prioritization for areas that China wants to lead in, in the years ahead.

Rob Strayer: Last December, we and 14 other governments attributed probably the largest active industrial espionage in recent history to the Chinese Ministry of State Security. In that case, the Ministry of State Security was working with a private set of companies to gain access to major managed service providers and cloud providers that were warehousing and storing and processing data for major blue-chip companies in at least 12 countries around the world. The Ministry of State Security gained access to this information and then was able to share that sensitive information with their own companies, so they were facilitating this form of economic espionage.

Rob Strayer: What do we do in the United States? On May 15th of this year, President Trump signed an executive order that would protect our domestic communications networks that set off a period for the Commerce Department to design regulations to effectuate this executive order to protect our networks. That process is coming to a conclusion and we should soon have a set of regulations that will be made public to protect our domestic communications networks.

Rob Strayer: In addition, the Federal Communications Commission controls what's called the Universal Service Fund, which is a way to fund our rural and smaller telecommunications carriers. On November 18th, the FCC will vote on a report and order that will declare Huawei and ZTE both to be national security threats and to deny them any future funding under this Universal Service Fund. It also kicked off a process to consider about where there is untrusted vendors in existing 3G and 4G networks in America, how that might be replaced through use of this Universal Service Fund.

Rob Strayer: In addition to that, in May because there had been an indictment against Huawei for its more than decade of activity of bank fraud and wire fraud in order to facilitate the transfer of technology to Iran, we decided to put Huawei under what's called the Restricted Entities List, which restricts the ability of U.S. technology to be sold to a company that's not acting consistent with our national security and foreign policy interests. Huawei has remained on that list and there have been only a temporary general license to allow existing activities, of existing products in the field that existed as of May, so that would be the telephones, the smart phones that were available then, as well as the 4G network infrastructure that was already in place as of that date.

Rob Strayer: As we talk to countries about the importance of improving their communications technology as they move to 5G, there is a couple myths that I hear all the time. One is that it's impossible to move away from existing 3G and 4G Huawei equipment when one wants to move to 5G because they'll either be too much cost or too much delay. Too much delay because the technology is not available.

Rob Strayer: Well, the United States we've already gotten more than three dozen cities that have ruled out with 5G technology using only trusted vendors, which are Ericsson, Nokia, and Samsung. So there's no delay, there's no lack of availability of technology, and the cost is right in line with comparable technology. In fact, the recent assessment by a report from Denmark found that probably replacing all of the recent untrusted vendor deployments in Europe would only cost $3.5 billion, or about seven or eight euro per customer.

Rob Strayer: Another myth that's out there is that we're going to be able to test our way out of this, that there will be enough testing and auditing of untrusted technology vendors that we can have confidence that we are ensuring our security future. As I mentioned before, that's just not the case. You can't test and find all the vulnerabilities in the software.

Rob Strayer: As the UK found and as another company in America called Finite State found, there are hundreds if not thousands of vulnerabilities in Huawei's firmware and operating systems. The UK has an almost 14-year relationship with Huawei and they still in their reports find that there's an inadequate plan to improve their software engineering, and their bottom-line conclusion that there are serious weaknesses in their software engineering and cybersecurity practices. That's not been remedied, so testing it regime alone isn't going to be enough to satisfy security concerns.

Rob Strayer: Lastly, there's a thought that you can just secure the core of the network and not the edge. Well, in a 3G and 4G network, you traditionally had a core where a lot of smart computing occurred, and the edge was just the radio network and really no computing at that layer. Well, the important thing about 5G will be that we will have computing distributed throughout the network and that offers very low latency between communications between devices and the computing. But as you push that computing out and distribute it throughout the network that makes all parts of the network critical, so you can no longer have a core and edge distinction. The entire network needs to be secured. With that I'm happy to sit down and take some questions.

Martijn Rasser: Very informative and helpful overview I think of both the risks and red flags associated with Huawei, the state of the technology and particularly the cybersecurity vulnerabilities, which is still something that I think a lot of people don't appreciate how poorly executed Huawei

software truly is. And of course, the importance of countering some of the myths—this narrative that Huawei has perpetuated—that makes them seem like the only inevitable choice for countries as they roll out their 5G networks.

IV. Audience Q&A Session

Martijn Rasser: Before I open it up to our guests for questions, I'd like to ask each of you a question, if I may. Elsa, there's this Chinese concept of civil-military fusion, which is a very important one, including in the context of 5G. I do feel there's a fair amount of misinformation on this Chinese strategy out there. Could you just explain briefly what civil-military fusion actually is, and perhaps more importantly, what it is not?

Elsa Kania: Sure. Military-civil fusion is a concept that has been elevated as a national strategy under Xi Jinping and seen as particularly impactful and consequential when it comes to emerging technologies where there is that clear dual-use potential. Of course, military-civil fusion, although it aspires to deep fusion of these sectors, in reality, it is still in some respects aspirational.

Elsa Kania: As a strategy, it's a work in progress underway with a number of different local pilots and initiatives, including a new military-civil fusion industry alliance geared towards creating and leveraging some of the synergies for 5G technologies because this is a sector where not only prominent Chinese companies such as ZTE and Huawei, but also stakeholders in the Chinese defense industry such as CETC have different proficiencies.

Elsa Kania: There even is Chinese military research under way on both 5G security and options to exploit 5G networks that sometimes involves deepening collaboration between industry, academia, and the military, so I think military-civil fusion could be an event and a conference unto itself.

Elsa Kania: But I would say as it pertains to 5G in particular, it does imply that the Chinese government is looking for ways to create and leverage these synergies in its development and deployment while also increasingly experimenting with military applications of 5G at the local level, whether for border security near China's border with North Korea or for local military units practicing emergency communications and mobilization, and exploration of how 5G could fit into the future system of systems that the Chinese military would leverage in future conflict. I think this is a rather nascent initiative, but I think it will be something to watch going forward, including as it involves potential collaboration between Chinese companies like Huawei and elements of the Chinese military responsible for cyber warfare, such as the PLA Strategic Support Force.

Martijn Rasser: Excellent. Thank you.

Martijn Rasser: Rob, I touched in my opening remarks on various European countries being on the cusp of making big decisions when it comes to 5G and whether or not to allow Huawei on their networks. I mentioned the Germany example, but the UK is another key ally that's on the cusp of making this decision. What can you tell us about the state of play in Europe as to the debate and the decision-making process?

Rob Strayer: Great question. The European Union kicked off a roughly nine-month process in March to improve 5G security across the member states. On October 9th there was a release of an EU risk assessment for 5G which we thought was very encouraging. It highlighted a number of the concerns that we've been talking about, including the ability for a nation-state to affect the supply chain, to affect the vendors in the supply chain, and that there should be a risk assessment related to vendors that includes looking at whether or not the company is under a legal regime where there's democratic checks and balances on the government's ability to compel it to take certain activities, where there's transparency about its ownership, and whether there's other forms of coercion that could take place. This report also importantly highlighted, which Elsa's report does too, the conflation of the edge and the core distributing smart components throughout the network.

Rob Strayer: Importantly, they particularly cite the ability in the future for there to be compromises of lawful intercept capabilities. Lawful intercept, so the ability to put wire taps that are done by the telecom operators at the behest of law enforcement or a government. Where those take place, data is decrypted, It's not encrypted at that point, it has to be unencrypted. A vendor who's providing that kind of service to a government is fundamentally one that has access to all information that's transiting that point in the network. I think it's a big concern that I think needs to be acknowledged by anybody just thinking about security measures that that edge where that law enforcement intercept capability is being added is using a vendor that's of the utmost trust.

Rob Strayer: We're seeing a number of important acknowledgements in that risk assessment. Now, the EU plans to have by the end of the year a set of security measures deployed a toolbox. We're hopeful that those toolbox security measures match everything in the risk assessment, importantly looking at what they call non-technical measures that look at the ability for a vendor to be influenced or to be compromised in addition to the normal best practices for cybersecurity. I think then many companies will then respond to that tool kit even though it's not binding regulation they will incorporate that into their own domestic regulation. So, as you mentioned, the Germans are still having comment on theirs, but I think a number of countries will incorporate what comes out of the security measure into their own domestic set of security measures they're deploying governing the 5G network.

Rob Strayer: But I agree with what Elsa said at the very beginning, which is this a marathon. This is going to be an iterative process, we're not going to see full deployment of 5G. We don't even know what many of the use cases are now, so it's important along the way to keep increasing the security that's applied to the networks.

Martijn Rasser: Great. We're entering a critical time period, particularly in Europe and Asia right now as these countries decide how to move forward.

Martijn Rasser: With that, I'd love to open it up for the audience for questions. Given that we are recording this for a podcast, if you could please state your name and affiliation before you ask your question, that will help our listeners keep track of the discussion.

Martijn Rasser: You had a question up here? Thank you.

Mariam Baksh: Yeah.

Martijn Rasser: There's a microphone coming to you.

Mariam Baksh: Of course. Thank you. Mariam Baksh from Inside Cybersecurity. Thank you, Deputy Assistant Secretary, for being here and also for the report.

Mariam Baksh: I am especially interested in the second group of recommendations around the need for secure design from the start. I thought it was interesting especially that you mentioned the need to screen carriers in addition to vendors, so I assume you mean U.S. carriers, clarify if you didn't.

Mariam Baksh: Then for Deputy Assistant Secretary, can we expect to see in terms of these more comprehensive security measures, what can we expect to see in terms of screening, establishing a framework for greater visibility in situational awareness, all these details? Not just into equipment providers, but into the carriers as well. I wonder how that might come up in your efforts abroad when other countries like the UK, I think, for example, has requirements on their carriers to implement encryption, for example, which you also mentioned. If you can just speak a little bit to how those discussions might be going.

Elsa Kania: Sure. Thanks for the great question. I suppose I'd say that as Rob mentioned, 5G will be tantamount to critical infrastructure, so we have to treat it with that level of seriousness, especially when we do think about some of the categories of applications, including in healthcare, such as remote surgeries that could be performed via 5G networks.

Elsa Kania: As I argued in the report, I do believe that having all vendors and all carriers subject to screening and evaluation of their security practices, and the security of their products and services, will be critical because although trust is absolutely vital, we also need to recognize that it's not just deliberate vulnerabilities, it could be inadvertent vulnerabilities, including bugs that are all but inevitable when we're talking about such complex networks.

Elsa Kania: I think one example that I found particularly telling was when Huawei was involved in a security evaluation and competition. There was some reporting that Chinese hackers had been targeting its rivals to look for vulnerabilities in their networks. So I'd say that excluding Huawei from U.S. critical infrastructure is only the start of thinking about how we can ensure it will be secure against all potential threat actors who will likely look at the vendors and carriers who we do trust more to try to find vulnerabilities in their network. It's a comprehensive evaluation of security and also looking at new techniques for screening for vulnerabilities, and trying to build in segmentation, and build in better safeguards against potential threats.

Rob Strayer: On the question about the supply chain security, that clearly needs to be improved overall across the board, and not just 5G, but all information communications technology. We should think about that as we're looking at all future emerging technologies as well. The reason I say that is because anywhere there's personal data or important business data we need to think about how that's being secured, and obviously these systems are becoming more and more critical to our daily functioning.

Rob Strayer: The Department of Homeland Security really has the lead on the cybersecurity side of this. As you may know, they have an information and communications technology supply chain working group that's going to develop best practices in this area.

Rob Strayer: We've also got a committee at the Federal Communications Commission called the CSRIC, which is also working in particular on the trusted deployment of 5G and adoption of 5G in two of their committees, I believe. That's all going on.

Rob Strayer: I think that we still talk about internationally with our partners about the importance of the NIST cybersecurity framework. That framework was refreshed in March of 2018 to apply to critical infrastructure in particular and it has a module within that on supply chain. I think that is our model, say a risk-based analysis, why I started my comments that way, is our dialogue to the government has to come from a risk-based framework. There's always going to be vulnerabilities in systems, but we got to think about the best way to address those for our nations.

Jim Hasik: Thanks. Hi, I'm Jim Hasik. I'm from the Atlantic Council. Thank you. Great report. Did read it in advance, really liked it.

Jim Hasik: I'm thinking about a question that generalizes your report maybe a bit, so I'd love to hear from you, Elsa, or maybe from the Secretary too. Part of the argument against Huawei is that Huawei itself, that entity, is not trustworthy because of intellectual property theft or selling stuff to the Iranians, or whatever else it might be.

Jim Hasik: Part of the argument against Huawei I think, as the Secretary was making the case, is that you just can't trust any Chinese company because of the lack of transparency, the lack of a legal regime, the pressure that Chinese government can exert upon. Okay, if I'm buying plastic toys or socks maybe I don't care too much. But I want to know how far logically does this argument extend.

Jim Hasik: That is to say, if I'm interested in how 5G technologies will contribute to autonomous navigation for vehicles, do I want to get Chinese auto parts out of my automotive supply chain in the long run? Does that extend to the electronics or to some things that might have electronic components in them? How far does this go and does it argue for, as I've heard in some quarters within the administration, that there needs to be a selective decoupling of the United States, if that's even possible, of the United States economy from that of China?

Elsa Kania: That is a challenge and I honestly struggle with these questions myself in much of my own research because I do agree that it's not simply about Huawei as a company. It's about the systemic issues that create inherent risk that arises from the nature of how the Chinese Communist Party interacts with companies that are notionally private, but that have Party secretaries, Party committees, in a manner that may influence their decision-making in ways that can be rather opaque at best. Not to mention issues like the National Intelligence Law. I've debated actively with Chinese legal scholars about what exactly that article means and I've heard denials of its relevance and applicability. But I have yet to hear a compelling counterargument as to why we should not think that China's National Intelligence Law says what it says, which is that any company, all companies, shall support national intelligence work, which are terms that can be quite expansively defined. Of course, China's cybersecurity law, which is coming full into effect into 2020, also imposes these restrictions on companies in terms of the level of access and support they should provide to the Chinese government.

Elsa Kania: As you said, this is a tricky argument because it does start to extend to how we look at any company that is subject to the rule by law of China's party-state. I also would agree that I think a selective recalibration in terms of how we think about our level of interdependence and technological entanglement with China is in order. I don't think it should be a complete severing of the economic or technological relationship because there are elements of it that are mutually beneficial and critical to sustain for the competitiveness of American companies and to promote overall innovation in a world of globalized technological development. But I think it does require careful consideration looking at different companies, different sectors, different potential externalities in ways that will really grapple with how do we think about these risks and how do we take appropriate measures to mitigate them.

Elsa Kania: I'd say that I agree that Huawei sometimes commands too much attention in these conversations. For every time we talk about Huawei there are any number of companies that are less prominent, less infamous, but equally problematic, including in terms of their relationship with the Chinese military or security services that are also quite active within the U.S. and internationally. I think we've only just begun to grapple with the full range of issues in play and I think how we recalibrate will be an active debate going forward.

Rob Strayer: I think that's a fantastic question and I agree with most everything you just said.

Rob Strayer: I would say that we're starting from this base of recognizing that 5G and the 5G network itself will be around for probably decades to come. What we build out today in the additional small cell sites or microcell sites will be around for some time. It will be hard to turn away from those. On the trajectory we're on, we may only be one vendor in the future supplying those. I think in this area, we know because of the criticality to our society that we need to have the utmost of security in place. In other areas we can have a case-by-case evaluation of what data is at stake, how could it be misused. I think that's going to be a little more fact dependent along the way.

Aaron Kiesler: Hi, Aaron Kiesler, Lewis-Burke Associates. This question could be for either or both of you. The Defense Innovation Board put out a report earlier that recommended among other things that, in developing 5G, the U.S. needs to prioritize lower spectrum band sub-6 where China's been focusing its efforts rather than millimeter wave higher spectrum bands that might be a little further off in the future. Just curious to see if you all had a reaction to that.

Elsa Kania: I thought the Defense Innovation Board's report raised some really critical points. I would frame it somewhat differently, not that we should prioritize development in one band over the other, but rather the two are complementary. American companies and carriers have great proficiency in millimeter wave or higher band and have started to move forward in deployment and products in those fronts. That is great for small scale more exquisite applications, whereas the mid-band or sub-6 is critical if you're looking to scale up 5G and expand the reach and coverage of it.

Elsa Kania: I guess I would say, I think perhaps diplomatically, that wouldn't say either element is more important than the other, but the two are truly complementary. But I agree with report's recommendations that the availability of mid-band spectrum is a very urgent issue, given that right now it simply isn't accessible to companies that might want to move forward and deploy 5G at scale on that element of the spectrum. I think there's a lot of work to be done

and hopefully, eventually we can reach an equilibrium where there is progress on both fronts or both elements of the spectrum there.

Rob Strayer: I just think it's important to recognize that there's an important role for the low-band, mid-band, and high-band of spectrum. They each have their own characteristics that, as far as propagation and people are most critical about the millimeter wave because it doesn't propagate far enough, but it's important to recognize that's where you're going to have the greatest throughput. In applications like in the uses of automated manufacturing or other places where we're going to have a very tight environment where we really want to see massive amounts of data come through with almost no latency, that's going to be the most important spectrum band for that.

Rob Strayer: We need this full spectrum and mid-band is being built out. I think partially we've had progress because of the likely T-Mobile and Sprint merger will allow more of that mid-band spectrum that's currently in Sprint's hands to be used to help build out a 5G network. I think in three years, roughly three-quarters of the U.S. population will then have the availability under the terms of their merger commitments to have a 5G network in the mid-band spectrum range.

Rob Strayer: The FCC I think is auctioning additional spectrum in next June and they're looking at additional bands in the future, including what's known as the C-band. It's something they're working on. I think the report was a little bit dire in its prognostications on this matter, but I certainly think directionally they highlighted a number of concerns that are completely accurate.

Dakota Cary: Thank you. Dakota Cary, Georgetown University. Mr. Secretary, I was hoping you could expand on whether or not this administration will take actions against traditional—either NATO allies or allies abroad—that do adopt Huawei 5G technology. For Elsa, I was wondering if you could speak to—I know the implications of the Chinese Intelligence Law—how will U.S. companies compete abroad in a post-Snowden revelation world where we don't compel companies, but they are certainly known to have good relationship with the U.S. government.

Elsa Kania: You want to take the first or?

Rob Strayer: Well you want to go first so that I might-

Elsa Kania: All right-

Rob Strayer: ... add onto that-

Elsa Kania: Sure.

Rob Strayer: ... and then I'll ...

Elsa Kania: Great question. I actually was living in China around the time the Snowden incident took place and all of those allegations, so certainly I am aware of the fallout and the fact that

many of the counterarguments when the U.S. government has raised concerns about issues like China's National Intelligence Law has been this sense of equivalency.

Elsa Kania: However, I would argue, and as Secretary mentioned, we do have a rule of law framework, we do have transparency. The fact that these allegations were reported upon and debated resulted in changes to U.S. policy I think does illustrate what the core difference is, that it's about having a rule of law system where companies can say no or protest, or refuse to work with the government even if they may have more cooperative interactions in other cases. I do think that illustrates the complexities of these policy issues, but I think that there are ways in which American companies and other companies operating in democratic systems can speak to the protections that are in place and the procedures and mechanisms that govern these activities. I'm aware that for some countries they may not differentiate between the two but I think there is a real difference, and I think we've seen Chinese companies around the world behaving in ways that are often quite troubling, including with regard to corruption, including aggressive lobbying and compromising of systems as in the African Union Headquarters breach, which has been linked to Huawei.

Elsa Kania: So I think there are plenty of examples that do highlight how some of the issues that come into play for Chinese companies that are supporting the Chinese government, as it is clearly scaling up and expanding global intelligence activities, are uniquely problematic, especially for countries that see China as a challenge or competitor, or even a threat as the Chinese government does take the country in rather troubling directions on many fronts these days, whether that's human rights or military modernization, or otherwise.

Rob Strayer: Right. They're both two great questions so I can just follow onto taking the second one, even though it was Elsa's question. I would just add, we have a rule of law-based system here, as I mentioned, so our companies have to act consistent with that. We have a free press here too that notes things like the Snowden revelations, I'm not commenting specifically on them, so we have a way to cause our companies to act consistent with the rule of law regardless of what the government wants, as everyone's well aware.

Rob Strayer: When Apple was asked to unlock a smartphone following a terrorist attack and they refused to, that went through the court system. It also is like the case that a U.S. company was fined $5 billion for the misuse of data. I'm not familiar with any Chinese company that's been fined any dollars or any yuan for the misuse of data. There is an accountability that occurs in the West that's not going to occur in China because of the lack of an independent judiciary.

Rob Strayer: Your question about what our response will be to partners that use untrusted networks or deploy untrusted networks for 5G. It is an unfortunate reality that availability of metadata in parts of the network, the availability to divine understandings about troop mobilization and other things causes serious concern about our continued cooperation at the same levels with regard to law enforcement, intelligence, and security practices, security cooperation, military security cooperation.

Rob Strayer: Now, we're not saying this is a threat, we're just saying that it requires us to reassess how we're going to do this if the networks aren't secure. The best way to ensure the same tempo and same level of cooperation that we have today is not to jeopardize that with untrusted vendors. Our plea is let's do what we've been doing together without muddying up the ability we have to cooperate by potentially putting this very important information, in some cases,

well many cases, we know people's lives depend on this information remaining secure, not out there in ways that are subjecting it to a potential adversary state to take advantage of.

Rob Strayer: It's really an act that we have to take that reassessment out of sorrow rather than one that we want to throw as an epithet at them to say you need to do this or else. But it's frankly a reality that we want to acknowledge at the front end and not say after all this has happened surprise somebody and say, "Well, we're reassessing this." Say, "Well you should have told us." Well we're telling you at the front end and we're thinking about positive ways we can generate a positive ecosystem of western development and that's where I think it's a much positive direction, but it is an unfortunate reality.

Elsa Kania: As knowledge of that reality, I would just add that I think one critical reassessment will have to be that Huawei is likely to remain a major player in the global ecosystem for 5G. That means there will be some very tricky calculations in terms of how the U.S. military and government operate around the world when Huawei is present to varying degrees in those networks and move towards more of a zero-trust paradigm, and recognize that this will create unique perhaps unprecedented challenges. But we have to recognize that reality and continue to look for positive alternatives. Again, I think part of that includes, as Martijn mentioned, pushing back against this narrative that Huawei is the only option or the inevitable decision, or the best choice for a lot of countries.

Elsa Kania: I think that does, as I discussed in the report, require looking at alternatives in terms of promoting collaboration among allies and partners to invest in digital development around the world and also, again, challenging the narrative that Huawei is number one. They may claim they have the most patents, but if you look at the quality, they drop quite a bit.

Elsa Kania: Similarly, contributions to standards. They've been very vocal in that process but that doesn't mean they're necessarily the leading player for whatever their marketing may claim. I think a lot of work to be done on these fronts and there are some very tricky issues that come into play with recognizing ways in which Huawei is contributing to and shaping this global ecosystem.

Melissa Griffith: Melissa Griffith with the Woodrow Wilson Center. My question is a slight pivot away from some of the conversations we're having today. Even if all of us in this room were to summon all of our magical potential, snap our fingers, get the best world when it comes to cyber hygiene, the best world when it comes to the supply chain and the security of the supply chain, we're still operating in a software-based, much more heavily software-based system around 5G. That brings with it the reality that it's inherently insecure. This is a very complex software system, so it's not just software, it's complex software. This just magnifies the vulnerabilities that we're facing, real limits around how you can test for security, how you can design for security. So this boogeyman in this room is this resiliency question.

Melissa Griffith: Moving away from security, looking at resiliency, what are some of the steps in the United States that you're seeing that we're actually taking, or we could potentially take to think about how to operate securely on inherently insecure systems?

Rob Strayer: Do you want to start?

Elsa Kania: Well great question, I think that is the core challenge here, that we are looking towards moving towards more and more networked societies, but the foundations for that future economy and all of the industries upon it are still insecure, and I don't think there are perfect solutions on these fronts. I think a lot of the work happening, including through the Department of Homeland Security, on thinking about supply chains, on implementing screening and standards are important but there won't be perfect solutions.

Elsa Kania: I hope we can learn lessons from some of the failures of resilience in the cyber domain so far and think about how do we apply those lessons learned to 5G and beyond. Can we think about redesigning this architecture and ensuring that we're not just racing to 5G, but we are thinking about it building a strong and healthy foundation with security designed in, whether that means greater network segmentation, end-to-end encryption as a standard, or simply thinking about what do we not want connected, where do we not want to go yet with 5G given some of those vulnerabilities.

Elsa Kania: I think when we think about healthcare, self-driving vehicles, all of the potential threats and vulnerabilities which we're already seeing to intensify with the Internet of Things, I think there's no shortage of challenges ahead. I certainly have not solved it in this report. But I've tried to remain optimistic that we are not in a world of doom and gloom and that there are ways to, through policy, exercise greater agency and promote greater collaboration between industry and the government in thinking about how do we start to anticipate and respond much more proactively instead of waiting until after a major security incident to start thinking about it. Thanks again for the question and I will look forward to hearing your own answers as well as all these conversations continue.

Rob Strayer: It's a fantastic question. The only thing I would just add to that is, thinking about the appropriate amount of resources that need to be committed to securing the networks and ensuring the right kind of configuration, whether that's for government and for the private sector, ensuring that we're doing enough to make ourselves resilient and we're not cutting corners along the way. Again, applying a risk-based framework, realizing that there's some risk that's going to still remain residual risk but moving ahead with smart decisions about configurations and how we're going to have update cycles on our products.

Rob Strayer: I think also we need to think somewhat about the dynamic threat world we live in. There are so many things that can be done just by good cyber hygiene that we can address. Getting your employees not to click on malicious links, easier said than done. But thinking about that set of best practices, then thinking about cyber criminals in nation-states.

Rob Strayer: There are distinct ways to address each of those. We've been, for more than 15 years, pushing for greater adoption in what's called the Budapest Convention which is a way for nations to set up their own laws to investigate and prosecute cybercrimes, and share that information across borders so there's really no country that serves as a safe harbor for cyber criminals.

Rob Strayer: But then there's the issue of nation-states and that is setting up a set of norms where we've worked on more than a decade to establish norms of how a state should act responsibility in cyber space. The most important one of those is that one nation should not attack another nation's critical infrastructure that's providing services to the public. We've sought to have a greater universal acceptance of that norm and a set of norms.

Rob Strayer: Just recently at the UN on September 23rd on the sidelines of the UN high-level week, we had 20 countries join together in a joint statement about holding malicious states accountable for their activities, including through the deployment of consequences among those like-minded states.

Rob Strayer: I think we also got to think about how we can dial down the threat environment as well as increasing our resilience. It's part of an overall bigger picture. I think there's so many facets to it, but great question.

Martijn Rasser: If I could piggyback on that question real quick. I've been seeing growing interest in an open architecture approach to telecommunications, which I think would address a lot of the security issues that you've raised. What have you been seeing in the ecosystem in terms of awareness of, interest in, moving potentially in that type of direction?

Elsa Kania: I think it's absolutely worth exploring. Again, thinking about if we have an opportunity with 5G and perhaps 6G beyond it to explore different approaches or alternative architectures, could moving towards that more open approach be beneficial. I think it's absolutely an exciting alternative and something I do mention in the report as a potential direction to explore. I don't think it's the only answer, but I think there are certainly ways that it can be part of the overall solution.

Rob Strayer: I think we also need to think about…there's two concepts. One is we've been talking a lot about the…those of us I should say, in this dialogue about how we improve the number of vendors in this space, talking about open architecture. So opening up the interfaces between the radio units and the base band units, basically the tower, the radio access network infrastructure. As we open that up, there can be more players in that space. We also need to make sure that's secured. We talk about this open architecture to ensure more of our, if you will, trusted players would be then able to participate in that environment of building out the next generation and continuing generation of radio access network telecommunications equipment.

Rob Strayer: But part of that discussion too is how much we want to use open source software. Open source software has a benefit of a lot of people seeing it, but it also has the detriment of a lot of people see it. In other words, if there are built-in vulnerabilities those can be exploited when they're just plugged into an overall end-to-end software design.

Rob Strayer: I think we need to be careful about how we use open source software in that environment. But overall, the efforts of, whether that's through the telecom infrastructure project or what they call the O-RAN Alliance of major telecom operators and more than 90 vendors now, to develop an open architecture is a very positive one for the future to allow us to get to a system where we have software-defined networks, and more generic hardware, hardware so that we're not so worried about what's been designed into that hardware from a potential authoritarian state.

Elsa Kania: Just to add, the greater diversity of vendors is going to be critical in terms of resilience because right now if Huawei remains as prominent in the global ecosystem, even if Huawei security were considerably improved relative to where it is now, a single vulnerability could have far reaching consequences. Whereas potentially transitioning towards greater diversity

in vendors and stimulating healthy competition with security as a point of competitive advantage in the process could help to improve the overall ecosystem going forward.

Mariam Baksh: Thanks. I'll note that I checked to see if anyone else was asking first. I have a quick follow-up that riffs on the nature of software being inherently vulnerable. I was wondering, you mentioned the…What's the name of the report…the Free State-

Rob Strayer: Finite State.

Mariam Baksh: Finite State Report and then the Huawei Security Center in the UK, both drawing attention to the host of vulnerabilities in Huawei software. I was just wondering if, as you try to convince other nations to use better quality rather than cheaper goods, or providers, whether there might be a need for a report that does a comparison between Huawei and other vendors. I asked this question to a Nokia executive once and almost got my head bitten off at the suggestion that they were anywhere near comparable. But if the difference is that stark, then why not just get that out there to make the case?

Rob Strayer: Well, my understanding is that the Finite State report they studied…that the report is very much focused on Huawei but they looked at other equivalent equipment of other vendors and they found that the number of vulnerabilities on average to be about 100 in any particular piece of Huawei's firmware. They said relative to others that was much higher, so I don't know other studies like that. I think it's a relevant question, but I just haven't seen it done.

Elsa Kania: Just to add again that I think all vendors whether trusted or not should be subject to intense scrutiny and, going forward, again trust does not mean that their security is perfect. There is no such thing as perfect security; we have to assume vulnerability and respond accordingly.

Chris Boyer: Hi, Chris Boyer from AT&T. I can't resist making a comment and asking a question. When it comes to general 5G security there's been a lot of discussion today about security of the 5G network and the architecture and software, and those types of things. I think it's worth noting that those concerns are not something that the industry is not very well aware of and been working on for a long time, so if you look at the work that's happening at 3GPP SA3 that's an entire group that's focused on security.

Chris Boyer: At the end of the day, I think our view, and I think I can speak somewhat for the industry on the service provider side, that we generally think that 5G we're going to take lessons learned from previous generations of wireless and we'll be able to build in more security with 5G.

Chris Boyer: At the end of the day, there are security enhancements such as the IMSI encryption that's going on. As you push more and more of the compute functionality in 5G closer to the edge, we can start to employ some of the same security mechanisms we use in the core networks like monitoring and looking at different trends and traffic, and doing different things we can push more of that functionality closer to the edge.

Chris Boyer: At the end of the day, I actually would take the position that security, it's not that it's not complex, it requires a lot of due diligence. We have a whole team of people that are working

on this, so it's going to be an ongoing issue for us. But I do think there's some inherent advantages in the long-term for security of the network.

Chris Boyer: The only thing else I would say is that you also need to look beyond just the network. The biggest issue I see in 5G security is that the threat surface gets really big because of all the devices. The issue of not only how do you protect our network that we're building but all those end user devices that are attached to the network becomes a huge issue, and that's where I think we have a bigger challenge to deal with. That's my comment.

Chris Boyer: In terms of questions, I saw in the report that the first recommendation was around prioritizing investing in 5G, and the question I get a lot when we talk about things like O-RAN and different parts of the network is what are the tools that government can use to expedite some of this, like get things deployed more quickly, help with security, help push different types of technologies. Do you have any thoughts on that particular issue? That's a question that comes up a lot.

Elsa Kania: Great comment and question. I agree. I think I'm very heartened and encouraged by all of the efforts and security happening in industry and through 3GPP. I hope that 5G will be more secure in the future, certainly given that the stakes are higher. And as you mentioned, IoT, in particular, is a critical element of that dilemma including because so many IoT devices today are made in China with less than ideal security, so a lot of work to be done in that front.

Elsa Kania: With regard to the role of the government in investment and catalyzing innovation, I think there are a lot of different measures that could be pursued, and I discussed some of those in more detail in my report. But not only investment in basic research to continue moving the frontier forward on these critical and foundational technologies, but also investing in deployment which will require significant capital expenditures and exploring models of partnership to help create 5G as a foundation that new industries and new companies can build upon. Of course, there's also a role for government procurement to stimulate demand and create initial pilots and testbeds going forward.

Elsa Kania: I think one of the core arguments I make in the report is that, while we shouldn't envy or aspire to China's model, which is much more state-planned and state-supported, there are ways that the U.S. government can look back to our own history and our own legacies of supporting basic research, supporting infrastructure and trying to catalyze innovation, and explore alternatives where in some cases the market may be immature or some of the applications are still experimental.

Elsa Kania: I hope that there are ways for government and industry to continue to build upon the great work that's under way and explore ways to partner and collaborate more deeply on thinking about the full range of potential of 5G, which, as you mentioned, for all the talk of security it may not be such a scary future. It may be much more exciting, especially if the security is right and if this is indeed a durable foundation for all of the new applications that can build upon it. But thank you again.

Jared Carlson: Hi, Jared Carlson with Ericsson. Rob, when you were talking about some of the indicators of trustworthiness that you presumably find lacking in China, transparency, is there rule of law, their ability to assert pressure on a company. Do you have either examples or advice to

countries as they look at these things and evaluate them? I think that we can all generally agree on them, but I wonder how countries are evaluating them. We have this recent example from Germany which seems to now be moving in the right direction. But we started off with this idea that you could self-certify and you can just say, "Yes, we're trustworthy." What is your response to that?

Rob Strayer: It's a great question. I think it's actually a concept that we're going to wrestle with for many years to come because of the importance as I mentioned earlier of data and data in emerging technologies. That we're going to want to make sure that the companies that are involved in these ecosystems are ones that we can trust and are not ones that are susceptible to undue pressure or coercion by a government without the rule of law being in place.

Rob Strayer: I can say that I don't know if it's always going to be a bright line. But there's certainly indicia of things going the wrong direction in China recently that even more of a Communist Party influence over the companies. They just announced that they were going to send 100 more minders from the Chinese Communist Party into their major tech companies. I think we got to think about what that means for cloud computing offerings for other types of companies.

Rob Strayer: We recently, in the United States, denied China Mobile the ability to interconnect with our telecommunications network. Part of that was on the national security grounds in addition to some law enforcement concerns we had. But, if fundamentally you can't trust that relationship between a telecom company like that and the government, that's going to be a problem based on their laws, and I think we could see that play out in other technology areas as well.

Martijn Rasser: Well, thank you all very much.

Martijn Rasser: Unfortunately, Rob has to head back to main State for a meeting, so I think we'll end it here today. I want to thank you all very much for your thoughtful questions. It stimulated great discussion. Please join me in thanking Elsa and Rob. Really appreciate it. Thank you.

Rob Strayer: That's fine.

Elsa Kania: Thank you. Thank you all for coming out.