Center for a
New American
Security

JANUARY 14, 2021

TRANSCRIPT FROM CNAS TECHNOLOGY & NATIONAL SECURITY PROGRAM EVENT

CNAS Event Transcript: Building a Trusted ICT Supply Chain

CNAS Event Transcript:
Building a Trusted ICT Supply Chain

I. Opening Remarks

Martijn Rasser: Good afternoon, everyone. It's a distinct pleasure to welcome you to this event, hosted by the Center for a New American Security and the Cyberspace Solarium Commission. I'm Martijn Rasser, Senior Fellow here in the Technology and National Security Program at CNAS. Now, the topic at hand is what steps the U.S. government can take to reduce critical dependencies on untrusted information and communications technologies, or ICT, for short. We're reminded of these dependencies and the risks they pose all the time, whether it's the SolarWinds attack, semiconductor shortages in the auto industry, or China threatening to cut off critical raw materials, such as rare earths.

Martijn Rasser: The Cyberspace Solarium Commission's white paper on building secure ICT supply chains couldn't be more timely and important. I'm delighted to have this great panel here to talk about these issues. I'll start off with some questions of my own, but I really encourage you in the audience to participate. You can tweet your questions with the #CNAS2021 hashtag or you can send an email to my colleague, JJ, at jjzeng@cnas.org. With that, let me introduce our panel. We're here with Congressman Mike Gallagher, Representative of Wisconsin's eighth district and Co-Chairman of the Cyberspace Solarium Commission.

Martijn Rasser: The Congressman serves on the House Armed Services and the Transportation and Infrastructure Committees. He's a former United States Marine Corps officer and a former intelligence officer. Welcome back to CNAS, Congressman.

Mike Gallagher: Good to be back. Thank you.

Martijn Rasser: Great. Next, we have Dr. Sarah Sewall. Sarah is the Executive Vice President for Policy at In-Q-Tel. Previously, she served as Undersecretary of State for Civilian Security, Democracy and Human Rights. She also served as the inaugural Deputy Secretary of Defense for Peacekeeping. She is the former Director of the Carr Center for Human Rights Policy at Harvard University. Great to have you with us, Sarah.

Martijn Rasser: Up next, Dr. Sheena Chestnut Greitens. She is an associate professor at the LBJ school, faculty fellow with the Clements Center for National Security, and a distinguished scholar with the Strauss Center for International Security and Law. She's the award-winning author of "Dictators and Their Secret Policy: Coercive Institutions and State Violence." Welcome, Sheena. I'm so happy you're able to join us.

Sheena Chestnut Greitens: Glad to be here. Thank you.

Martijn Rasser: And finally, Mark Montgomery. Mark serves as the Executive Director of the Cyberspace Solarium Commission. Previously, he was Policy Director for the Senate Armed Services Committee. Mark served for 32 years in the U.S. Navy, retiring as a rear admiral in 2017. Welcome, Mark. Great to have you here.

Mark Montgomery: Thanks, Martijn.

II. Building a Trusted ICT Supply Chain Discussion

Martijn Rasser: Okay. We're here today to talk about the findings and recommendations in the Solarium Commission white paper, "Building a Trusted ICT Supply Chain." Let me begin by commending Rob Morgus, the lead author of the paper, for this impressive piece of work. It's comprehensive and makes important policy recommendations. There's a lot to unpack. The report covers technology alliances, manufacturing capacity, supply chain restructuring, global competitiveness—all very important aspects of the broader geostrategic competition with China. Congressman, before we dive into the white paper itself, could we start with you giving an update on the status of the Cyberspace Solarium Commission?

Mike Gallagher: Yeah. Well, thank you for hosting this. I'll confess, my mind has not been on cyber issues or national security issues over the last two weeks, so it's good to be back and engaged in this—if for no other reason, it gives me a sense of normalcy. Thank you so much for hosting this. We had a very positive conclusion to our legislative process in the context of the National Defense Authorization Act. As you know, we released our final report in March 2020, the week before Congress shut down for coronavirus. That was inauspicious timing. Thanks to Mark's leadership, and Jim Langevin's energy, and Angus King's general likability and the goodwill he generates, we were able to get—Mark, correct me if I'm wrong—I think 26 of our 50 legislative recommendations effectuated into law, most of which were in the National Defense Authorization Act, and that was a great batting average for us.

Mike Gallagher: We—actually, lest anyone be confused, because Angus and I tend to come off as nice people—we are very competitive, and we actually took a look at the historical batting average for commissions and wanted to make sure that we beat that. We have so far. That being said, there's a lot of work yet to be done. We are still constituted as a commission. Albeit in somewhat scaled-down form, but we will be continuing our work into the new Congress and I'm very excited.

Mike Gallagher: I have engaged with the incoming Biden national security team. I am, let's say, cautiously optimistic about some of the personalities they might be considering for key cyber-related positions. I told them that—not that I'm exceptionally influential or that high-ranking—but I will look forward to working with them in the same way that I worked with the previous administration on areas of mutual interests that were good for the country. All of that, I think, puts us in a good position to build off our initial report, build off the supply chain white paper, and have some real legislative successes going in to the 117th Congress.

Mike Gallagher: The final thing I'd say is obviously the SolarWinds hack, I think, underscores how important this issue is. And I think that while we're still sorting through all the implications, it directly implicates not only the white paper, but some of the recommendations that we had in the original paper that were subsequently put into law, most notably giving CISA the ability—the authority—to do threat hunting on .gov networks, as well as the creation of a National Cyber Director. With that, I'll stop talking and I really look forward to this discussion and I thank you for it.

Martijn Rasser: Well, great. Thank you so much. It's a real pleasure to have you back and congratulations for the tremendous impact that the commission has had so far. And it sounds like the future holds a lot of very good opportunities for the commission. Let me turn to the supply chain issue, Congressman, with just a top-level question for you. How do you define the issue from the Hill's perspective?

Mike Gallagher: Well, I think, if you look at our original report, we called on the government to take steps to reduce critical dependencies on untrusted information and communications technology. In addition to recommendations to improve intel and information sharing around supply chain risks, core to our recommended approach was the creation of an ICT industrial-based strategy to ensure we had more trusted supply chains and availability of ICT technologies. The white paper we produced is our effort to further this recommendation and lay out a strategy and some recommendations for implementation. And put bluntly, I would say in the context of supply chains for ICT, we have a China problem.

Mike Gallagher: Over the past two decades, China has mobilized state-owned and state-influenced companies to grab a dominant position in markets for several emerging technologies, especially the market for telecoms equipment. That's not an accident, but rather the result of a concerted strategic effort by the CCP to capture these markets through a mix of government-led industrial policy, unfair deceptive trade practices, and IP theft. As a result, we believe the critical strategic competition between the U.S. and China—and our friends and partners—is taking place in an international system of commerce that, due to Chinese intervention, is neither free nor fair.

Mike Gallagher: Our strategy is an effort to get in that game because, in short, I think in our eagerness to do something about a very real challenge, the United States has leapt without a plan of action. And we've had some positive developments—we have congressional proposals like the American Foundries Act, the CHIPS Act, the Telecoms Act, but we need a broader strategic effort to shore up our ICT supply chains.

Martijn Rasser: Yeah. No, I couldn't agree more on that point. The need for a broader strategic vision on these critical technology policy matters is key if we're going to be successful in this geostrategic competition. Sarah, let me turn to you real quick. You've written about the need for the U.S. government to focus on disruptive innovation, including in microelectronics and 5G. Can you help us explore the difference between onshoring or re-shoring the supply chain versus innovating solutions to the supply chain challenge?

Sarah Sewall: Sure. Thanks for the question and thanks for the opportunity to be here, Martijn. Thanks to CNAS and thanks to the Solarium Commission for doing an enormous service to the country by giving us the comprehensive way to think about many dimensions of the problem. In terms of your specific question about on-shoring, re-shoring versus innovation—I think there was a bit of a bias in the national security framing of the problem, to want to own and to protect, physically, the supply chain. That's really important. And the ICT white paper has some great recommendations on having to do that and there's a lot of momentum now in Congress for how to do that.

Sarah Sewall: But at the same time, one of the things that we know from the history of American innovation is that—well, we know two things—one, as the commission points out, you can't onshore everything. We live in a globalized world; we have a globalized supply chain. You have to figure out what's the minimum required amount that you need to be able to produce at home and have reliably available to you. And you also have to accept the fact that you're going to still rely on external components in some cases. But as we think about what it means to secure a supply chain, we also have to recognize that what's allowed us to be leaders in these technologies overall has not been the reliability of our supplies or the ability to make them on American territory. It's been our ability to innovate. And there, I think, we have a different set of national challenges that's harder for us to think about because we've had a particular model for thinking about innovation since the early Cold War. That model has been the U.S. funds research and development, predominantly in the context of weapons systems and defense applications, and the private sector commercializes the rest.

Sarah Sewall: As the report helps make clear—as it struggles with "What's the national security technology" and "What's a civilian technology"—is that many of the technologies today that are privately purchased, that are commercially sold, and sometimes that create greater national security vulnerabilities by their existence overseas and even in the domestic market, are not issues that the U.S. has traditionally thought about as being national security concerns. If the market isn't seeing them as a place where it can get a good return on investment, we've got gaps, and the government has typically not wanted to have anything to do with that.

Sarah Sewall: The plea from the commission to think afresh about definitions of national security, what constitutes as security vulnerabilities, and the role of government in trying to address them, I think is super important. But innovation is not our go-to. We tend to go to the protected, created ourselves, the know-that-we-have-it, and I think we can perhaps come back to this, but that the innovation piece is something we absolutely can't lose sight of.

Martijn Rasser: Thank you very much for that, Sarah. That's a very important point. Mark, let me turn to you real quick. I mentioned at the outset there's this issue of rare earths, and I think the report does a really good job talking about the importance of raw materials. I see that ICT supply chains contain numerous vulnerabilities when it comes to raw materials. Can you walk us through what the current situation is, some of the challenges the United States faces, and where does the commission see opportunities to address these problems?

Mark Montgomery: Thanks, Martijn, and Sarah was exactly right when she talked about that we almost immediately turn every issue to a national security issue and quickly look for a U.S.-based solution. And we at the commission tried hard not to do that because rare earth elements... And we looked at materials in three ways. Silicon and germanium, which are not rare elements and aren't rare, but where we do have some challenges. But then rare earth elements where—these are the raw materials used in the production of a lot of high-tech products—and while we do mine and extract them, we don't refine near enough for ourselves.

Mark Montgomery: What's happened over time—we used to be a leading extraction, mining, and refining country, but it is a very messy process. And years ago, it was an extremely, very messy process, and it really ran into our own cost of labor issue and environmental protection issues. So, even as the United States, sometimes you'll see an effort by a company that will go mine this, but the reality is what we mine right now are to get sent back to China. I guess one of those areas: we have to broaden our vision, open up our spectrum a little bit, and look for other solutions than just mining and refining in the United States. From my perspective, China has too much of an advantage in that for us to compete.

Mark Montgomery: It would just be putting a lot of money down a hole to do that. Instead, we should rely on allies and partners. There are allies and partners that can do this refining where their costs of labor are less for technical skills, and that's where our cost of labor really drive up high or are at the high end of technical manufacturing, and I think there's a way to do this overseas. And frankly, where even when you meet an environmental protection safeguard in the United States, say for the construction of nuclear power plants, there's still a "not in my backyard" mentality that takes over and prevents you from doing something that you could do in an environmentally safe manner.

Mark Montgomery: And I don't just say that as a naval nuclear engineer, but I guess, generally understand that we can do these things safely, but sometimes NIMBY takes over. I think rare earth elements is where there's great opportunities to identify allies and partners that we can rely on to either...to mine if they have the mining, or do the refining using our minerals or another ally and partners' minerals to build up a supply chain that isn't completely reliant on China. That's going to be important because the rare earth elements are critical parts of technology hardware production and that kind of dependency is probably not wise, national security-wise, but forcing it into a U.S.-only solution would be equally unwise.

Mark Montgomery: One other thing that I would mention here is that is that the United States already has brought Taiwan manufacturing into our country and done those kinds of investments. I think it's appropriate to take it back the other way to some of our allies or partners. I'm excited about the opportunities we have in rare earth elements, but I fear trying to either legislate, or through the executive branch, direct a U.S.-only solution.

Martijn Rasser: Yeah. No, that's exactly right, Mark. I'm encouraged by the fact that we're already engaging very well with Australia, for example, in the rare earths issue, but Japan as well. And one thing that the Japanese have a lot of expertise in as well is the recycling of rare earth elements. They had their supply cut off in 2010 and they invested quite a bit of energy into researching novel ways to reuse these materials. And that, I think, is another thing that the U.S. government should think about investing more in, and in particular because that type of basic research tends to have a lot of follow-on effects that are beneficial for the economy as a whole. So, something to discuss further, I think, within the Congress and within the administration.

Martijn Rasser: Sheena, I wanted to ask you, the report devotes quite a bit of attention to standard setting. Can you walk us through why standard setting is so important and tell us a little bit about how you see the United States approaching standard setting and how that compares and contrasts with the Chinese approach?

Sheena Chestnut Greitens: Yeah. Thank you. First of all, let me say that this report, I just want to commend the author for a really, really thorough look—and comprehensive look—at this issue and appreciate this discussion. I was particularly heartened to see the emphasis on standard setting, because I think it is such an important tool that the United States could be using to shape the ecosystem in which we think about ICT supply chains. But the reality is that this is an area where I think China has been much more strategic and proactive to date than the United States has and, as the report highlights, that needs to change.

Sheena Chestnut Greitens: The way that China has organized domestically to come up with and decide, "What are the set of standards that are in PRC interest and in the interest of Chinese companies?" So, China has been domestically quite strategic in developing and formulating a coherent set of Chinese standards. Then it's been equally strategic in going out and using various international fora to get those standards adopted, and to be a leader in the standard setting process. And the report does a great job of pointing out that this has knock-on effects on patents, on cost competitiveness, on interoperability, on any country that then wants to upgrade or expand what it currently has.

Sheena Chestnut Greitens: These are all things that the United States should care about. I guess the one thing I also wanted to highlight about the importance of standard setting is what's at stake in terms of global freedom and democracy. One of the areas I work particularly on is tracking the export and use abroad, or globally, of Chinese surveillance technology. Again, this is an area where China has been incredibly strategic and proactive in terms of its leadership role in the ITU, in terms of the number of submissions it's made about, for example, facial recognition technologies to the ITU. It sounds like it has a batting average at the ITU that is competitive with this commission's track record in Congress.

Sheena Chestnut Greitens: In that case, I don't think the batting average is necessarily a good thing, but about half of the standards that Chinese companies have proposed on facial recognition have been adopted by the ITU to date. That's an issue, because it's in the United States' interest—again, as other parts of the report highlight—that we have both technical standards and regulatory frameworks around the use of this technology that make it compatible with liberal democracy.

Sheena Chestnut Greitens: Part of the stakes of the standard setting process, I would say, are not just about U.S. national security in terms of the narrow issue of the supply chains, which isn't all that narrow, but I think it's important to place that in the context of the impact that a lot of these technologies are having on freedom and democracy worldwide. The recommendation to work with like-minded allies and partners is really important, and standard setting is one of the best tools the U.S. could be using in terms of pushing and working multilaterally to get some of these standards adopted.

Sheena Chestnut Greitens: But I think that's going to take the United States adopting a much more strategic approach itself. In some of the work I've done in surveillance technology, my recommendations have been that the United States really come up with a comprehensive plan looking at which fora should set the rules and standards for which technologies. Who and how is the United States going to push and advocate for those standards? And what is the role of partnerships and alliances in those fora? What is our specific plan for engaging in these different standard setting bodies in order to try to advance United States and democratic interests?

Sheena Chestnut Greitens: But the reality is that at this point we are playing catch up, so I was just really glad to see that the report highlighted the urgency of that task, and I very much hope it's something the administration picks up. I also very much hope it's something that Congress will hold the administration accountable for and do its own part in pushing that process forward.

Martijn Rasser: Great. Thank you so much, Sheena. Congressman, let me pivot back to you. I think one striking aspect of the white paper is you're advocating for a kind of industrial policy that the United States hasn't done in decades. You know, really making the argument that market forces alone can't address these problems successfully. In the executive summary, you and Senator King write that the framework laid out in the white paper could inform similar strategies for other key technology areas and critical items. Do you envision the commission's work serving as a springboard for formulating proactive strategies in other areas, and ultimately, do you see your work essentially making the case for a true national strategy for technology?

Mike Gallagher: Well, anytime someone says the "I" word, a little conservative devil on my shoulder looks me in the face. But yes, that's what we envision. I'd like to make a quick point though, on rare earths if I can, just because I think it's important. I went with the Chairman of the Seapower Subcommittee of the House, Joe Courtney, and the Chairman of the Friends of Australia Caucus, to Australia last year or two years ago, and that was our biggest takeaway. We went to Western Australia, and our big takeaway was the need to do exactly what Mark and Sheena are talking about, and really enhance our partnership—in particular with our Five Eyes allies—and there seems to be an obvious one when it comes to Australia and Japan, as was mentioned before.

Mike Gallagher: We had a small victory in the National Defense Authorization Act. It was an amendment that Courtney and I authored that would require the SecDef to prioritize the acquisition of strategic and critical minerals from U.S. and allied sources, ensuring their continued protection of our supply chain. I just wanted to bring that up as a shameless plug for something productive that Joe Courtney did. But yes, I think if you look at the original report, our original Solarium report, what you'll see is a very concerted effort to get this balance right, between recognizing that the private sector is the main effort and at the leading edge when it comes to cybersecurity.

Mike Gallagher: [Inaudible] owns 80 percent of the critical infrastructure. Therefore, it would be counterproductive for the federal government to come in with a one-size-fits-all, a very onerous regulatory policy, that tells the private sector what to do. We tried to adopt a more incentive-based approach, but I think when it comes to industrial policy, or as we talk about an ICT industrial-based strategy in the original report, we do believe that that's an area where the federal government needs to be more proactive, a little bit more prescriptive, and where we as a commission can provide a little bit of the thought leadership and some potential models that we can build off going forward.

Mike Gallagher: I guess it's up to you guys to determine whether or not we struck the right balance, but certainly that's what we were going for and it was amazing to me how many of the Republican commissioners, both legislators and outside experts, were willing to utter the dirty "I" word from the start of our discussions.

Martijn Rasser: It's really remarkable to see how the conversation about industrial policy has shifted just in the past few years. I think ultimately, it comes down to everyone recognizes we're in this very serious competition with China, with a mercantilist approach, and the status quo just won't get us to where we need to be. And frankly, and the report points this out as well—one of the appendices—is the United States has a very rich history of technology strategies that it applied, if you look at World War II and during the Cold War. We can very much do this type of policy and still have it be in the spirit of the broader free market. I think there's definitely a lot of opportunity there.

Mike Gallagher: Can I maybe add one thing there—I'm sorry.

Martijn Rasser: Yeah. Of course.

Mike Gallagher: I don't know who said it earlier, but just talking about how the old model of the federal government making massive investments in research and development, I will say one of the more remarkable things I've encountered in my four years in Congress is that I currently have a bill with a very progressive colleague of mine, Ro Khanna, who represents Silicon Valley, and the Senate co-sponsors are Chuck Schumer and Todd Young, that would amount to a massive investment in research and development from the federal level while also trying to modernize the process through which federal R&D dollars are allocated, and spreading that out across the United States and not having it concentrated on the coast.

Mike Gallagher: And I think anytime you have something where a conservative House member like me and Chuck Schumer are in near alignment, maybe that's a suggestion that we're onto something, and that there's a lot of bipartisan support around these ideas. I'm really optimistic about that in the new Congress, for whatever that's worth.

Mark Montgomery: Hey Martijn, can I jump on one thing? It's interesting, you said over the last few years we've gotten better—I would say it's over the last nine months—on industrial policy. In January, Representative Gallagher and I were going to staff and member meetings, trying to get minor changes to the Defense Production Act. We just acknowledged cybersecurity as a national security thing where, during a crisis, we could bring in Title 10 forces, military forces, to help FEMA or CISA. And we were getting pushed back. Two months later, we're doing DPA for cotton swabs. The Defense Production Act and how we see industrial policies changed much over the last 10 months.

Mark Montgomery: Operation Warp Speed is industrial policy on the level of the Tennessee Valley Authority, on the level of the World War II reprogramming of our plane and automotive factories to produce—how we won World War II. And certainly much, much bigger than SEMATECH, which is the example we tend to use of industrial policy in the modern age where the United States—I want to say propped up, but—heavily supported its microchip industry in a challenge from Japan. I think there has been this dramatic change over the last 9 or 10 months and I think a very, very small silver lining to COVID has been this recognition that sometimes the government is the best person to really tackle a hard challenge.

Martijn Rasser: Yeah. I think the widespread brittleness of our supply chains...that realization was a real eye-opener for a lot of people, what we experienced in March and April in particular. Yeah, to your point, there'll be some very interesting changes up ahead.

III. Audience Q&A

Martijn Rasser: We're starting to get some questions from our audience, and there's one that I'd like to just throw out to the group here. It pertains to one of the key themes in the paper, the importance of partnerships with like-minded countries. The question here is, "What is the best grouping for the United States to develop a secure supply chain?" Is it the D-10, the Democracy 10, this grouping that the Brits proposed? The Quad? Five Eyes? Or if all are useful, how do we manage different levels of sensitivity? How do we manage different technology areas? Just to open that up to all of you, whoever wants to take a whack at it.

Mike Gallagher: Well, I'll just quickly say—and then I'll defer to Sheena—I always view things through the lens of Five Eyes first, just because we have so much history there, and there's been so much legislative work that's gone unnoticed around incorporating Australia into our national technological industrial base. And it just provides a very easy framework to build off of, although I really do like the D-10 concept. I just think there's some really low-hanging fruit with our Five Eyes allies.

Mike Gallagher: I advised the Trump administration and I advise the Biden administration to really put a gold standard free-trade agreement with the UK, now that they've navigated their exit from the European Union at the top of their agenda. And that, of course, would have huge implications for ICT and for all other manners of technology. I just throw that out there.

Sheena Chestnut Greitens: Yeah. First, to second the Congressman's recommendation there, I think that makes a lot of sense. I guess the other point that I would make is that we're talking about a pretty large range of technologies when you use the term ICTs, right? Reading the report, for me, really brought home just how broad the scope of the challenge is. I think we're going to need a layered strategy. It's going to take somebody a lot of time to get into the weeds and figure out which of these groupings should tackle which pieces of this problem.

Sheena Chestnut Greitens: But I guess I would start with the assumption, if we're talking about crafting this strategic, coordinated strategy, that all of these groupings are going to be useful at some level and in some way, but we're going to have to figure out how to layer, in sequence, the pieces. That's why being able to have the kind of organization and strategic approach that the report highlights is so important, because figuring out exactly how to match the pieces, layer them, and then sequence the steps is going to be in an immense challenge. It requires a lot of legwork and a real knowledge of both the diplomatic and geopolitical fora we're talking about, and of the specific issues related to the range of technologies that are covered in the report.

Martijn Rasser: Great. Thank you, Sheena. Mark, I think you have a follow-up point you want to make.

Mark Montgomery: One quick point. I agree completely with Representative Gallagher, and especially Sheena's point, that this is a very large bag. One country that has to be in it that wouldn't naturally make the list of the Five Eye or Quad or D-10 is Taiwan. We are not going to get ourselves into a safe, secure, trustworthy, IT hardware and software supply chain without Taiwan, and I think this is a great opportunity. We are Taiwan's security partner of choice, really because there are no other choices, but we are their security partner of choice and I think they understand that.

Mark Montgomery: They do tend though, to flip quite a bit, and their trade's about double with China than it is with us, and I'm okay with that trade as long as it's sneakers and clothing and things like that. The degree to which it becomes some of the high-tech, Rosetta Stone tools, is where then we ought to have a problem. I think there's an opportunity here. You've seen a change in our Taiwan security posture over the last year. I think we'll continue to some degree in the next administration, and we should integrate that and have an economic partnership lead the security partnership. This is a democracy—over the last 40 years have gotten to a full-blown democracy—with fights between legislators on the floor and growing their economy twentyfold in 40 years. This is the absolute right partner for us, but they'll have to make a choice about becoming a trustworthy and secure partner with the United States and protecting what they divulge and/or provide to China.

Martijn Rasser: Yeah, that's an excellent point, Mark. I think the question of Taiwan and the broader U.S. Indo-Pacific strategy is a super interesting one, and I think something over the course of the next four years, it would be very interesting to see how that relationship develops. India as well, I think. There's a lot of opportunity to engage much more strongly with India, particularly on these high-tech matters. They've got a lot of expertise, a good foundation that we can build off of with them in order to better integrate in these types of supply chain matters.

Martijn Rasser: Sarah, let me turn back to you real quick. Let's talk a little bit more about R&D versus investment and commercialization. I'd love to get some more of your thoughts on that particular point.

Sarah Sewall: Thanks, Martijn. I think Congressman Gallagher makes a really important point about the extent to which we have to reckon with a very different form of a geopolitical competitor in China. Russia wasn't doing what China does, which is essentially growing our industries at home, protecting them, and then subsidizing them massively on the international front. The United States is never going to be able to compete with that because we're not going to want to play that infinite subsidization game. Innovation—coming back to innovation as being really the key.

Sarah Sewall: And one of the things I was really pleased to see in the paper is the thoughtful recommendation that the government needs to do more to think about the gaps in private sector investment. Not to displace private capital, but instead to fill gaps where, for whatever reasons—and it could be the huge amount of capital investment that's required upfront, it could be that the returns are going to be a much slower coming in then your typical venture fund can wait, it could be because the profits simply aren't there right now because the market's not there right now—but there are critical opportunities for the government to say, for example, we want to open the RAN. We're going to try to fuel that by making key investments.

Sarah Sewall: There are some areas of microelectronics that we absolutely cannot afford to lose, but we need to find capital to fill some of the gaps that the private sector is not filling. Whether it's in things like tooling, or whether it's in things like advanced packaging, there are some really important opportunities for the government to think about equity investing as a tool in its toolkit. That's very different from an industrial policy like China's that essentially will subsidize till the cows come home. Then the other point I wanted to make just very briefly—and I think it's something that Congress as a whole needs to spend more time thinking about—but there's a lot of energy. As Representative Gallagher said, there's a lot of energy in terms of more R&D, and I think there's a lot of bipartisan support, but the reality has been historically, that's all the government's funded, and a lot of that R&D stays locked in the labs. It doesn't make it through that chasm into commercialization.

Sarah Sewall: Typically, the U.S. view has been, "That's not what we do as a government, we let the private sector do that." What we're seeing now is that the national security implications of so much of the commercial technology and things that are dual-use or even primarily civilian in use...but when used by the German citizens or by others overseas, can create vulnerabilities for us.

Sarah Sewall: We need to have a different attitude, and we need to really focus on commercialization of the great R&D work that we've already done. I think there's a maturation process in terms of, there's a gap between we just do R&D and we do industrial policy, and it has to do with these key two pieces, investment and commercialization, where I think there's a lot of scope for us to grow as a country.

Martijn Rasser: Sarah, are there any specific capital market incentives that you have in mind to help bridge that gap?

Sarah Sewall: Well, there are a host of different mechanisms that we can use. At In-Q-Tel, where I am, we're fundamentally interested in finding places where the strategic investor who's concerned less about profit and more about mission can make a difference. For example, with microelectronics, if we can start to develop some of the new tooling that we can then prototype, and see how it plays in, you're going to begin to build an interest among the design firms for using the new tooling, and it's going to become basically a self-sustaining process that the government would then be able to back out of and let the private sector take over.

Sarah Sewall: That's the catalytic role that we'd really like to see, I think, the government play, when we think about overseas and the scale of what does it mean to begin to try to give people choices that are different from Huawei when they're thinking about their 5G infrastructure. That's on an entirely different level. And there you do want to do, I think, as the paper quite rightly points out, you want to think about some of your international investment tools, you want to think about loan guarantees, you want to think about re-insurance. You want to think about other tools that can create options for governments to not feel trapped, that they have to buy Chinese technology that could make them vulnerable, and that will build in vulnerabilities for decades to come.

Martijn Rasser: Great. Thank you, Sarah. Sheena, I wanted to go back to you real quick. There was a little bit of talk just now about R&D spending and some other human capital components. What are your thoughts on that aspect of this issue and how does the human capital component fit into the broader ecosystem?

Sheena Chestnut Greitens: Yeah, that's a great question. First, let me just amplify one thing that Sarah said that was really important, which is about the United States having the energy and having worked with its partners to create alternatives. In many of the cases that I look at with Chinese surveillance technology, it is the easiest off-the-shelf, cost-effective step that a mayor or a provincial governor in a country somewhere can take to solve what they view as their most pressing electoral challenges, which are things like crime, attracting investment, boosting job growth, all on a specific electoral timetable.

Sheena Chestnut Greitens: China has provided certain ICT solutions that make it very, very easy and appealing for it to be a partner of choice, and I think it's really important that the United States think in this global context about how to create that alternative. Just wanted to highlight that piece of what Sarah was saying. I guess the other point here goes in a little bit different direction, but I really think that it's important when we think about the issue of R&D funding, STEM education, etcetera, that we think through what the human capital dimensions of this challenge are. Again, this is an area where I see China as having been really pretty highly strategic.

Sheena Chestnut Greitens: We've all read at this point about any number of cases, about China's Thousand Talents program. I just saw that a scientist at MIT was arrested last night or this morning for failure to disclose grant funding to the Department of Energy. We've all read about Thousand Talents and the multiple talent recruitment programs that China has. When I read through statements and documents from Xi Jinping, all the way down through the Chinese Party-state, there's a real emphasis on the development of AI in tech talent as an incredibly important priority for the Chinese, not just for Chinese education or for the technology sector or for innovation, but as a national imperative.

Sheena Chestnut Greitens: I guess the one thing that I think would be helpful to think through and talk about is what kinds of policies are necessary in terms of human capital, education, and R&D to compliment some of the other steps that we've seen outlined and proposed in the report. Again, I think it's important for Congress and I'm glad to hear that there's bipartisan support for putting funding toward some of that R&D. I think that would be a great and really important step. The only thing I guess I'd add to that is that in the work that I do, it's really important to understand how different countries use that technology and how ICT—the tech pieces themselves—interact with the political and regulatory frameworks in some of these countries. I would say particularly China, but maybe some of the other countries that Commerce has emphasized—like in the rules that it put out this morning, I think it named six.

Sheena Chestnut Greitens: I think we need to have funding specifically for R&D for these technologies. The one thing I would say is we also need to pay attention to the politics of how they're used and employed because that, again, is what's going to shape the impact that they have on national security, as well as on global democracy and U.S. Interests in different countries—from partner/ally countries, all the way throughout the world.

Martijn Rasser: Great. Thank you so much, Sheena. Congressman, Mark, there's an audience question that I'd like to pose to you. The question is, "Given China's history of intellectual property theft, how can the United States balance collaboration and information sharing with our allies while also protecting our innovation base?" Do you want to go first, Congressman? Mark?

Mark Montgomery: [Crosstalk] …teed up perfectly for the Congressman. On this first one, what I'd say is, far be it from the United States to criticize other countries' security about information, when you look at the WikiLeaks scandal in our country and Snowden. We got to be very careful when we say, "You guys need to do more or less on this." I think that we should work with our allies and partners to share best practices on cybersecurity. I think we try to do that. I think we need to do a better job.

Mark Montgomery: I do think that we still need to work with allies and partners on getting the agreements on what's appropriate behavior in cyberspace settled, and how you rapidly attribute an adversary action so that we can take a response action to it. I think we need to work through those things, but I think our allies—when you start with the Five Eyes and then work your way out—we can work together as a team on this for intellectual property theft and for protecting our industries and protecting our .gov, but we're certainly in no position as say, "Do as I do." Probably we are in a position to say, "Do as I say."

Mark Montgomery: And I think we just need to work more closely with those allies or partners—and ourselves—to do a better job, but our defense innovation base needs to be international. It will be a failure if we relied only on American companies and only on American engineers, because we have benefited through these rich relationships with the Five Eyes, and with NATO partners, and with Japan and South Korea over the last three decades. I'm hoping we'll continue to push that out, but certainly, there are some that argue for a much more insular approach to this—and I hope that doesn't prevail.

Martijn Rasser: Great. Thank you, Mark. Congressman Gallagher, here's a question specifically for you. You mentioned that we have a China problem and the audience member would like to know, "Does this mean we have a CCP problem, or a strategic problem, or both?"

Mike Gallagher: Well, my view is that we have a CCP problem, not a China problem, and we need to be very clear in our public messaging and in our diplomatic outreach that that is an important distinction as well as seize on opportunities to highlight the way in which the CCP is the enemy of its own citizens. I'm not sure we have effectively done that in recent years. To the extent we have a strategic problem, I would say we have a geopolitical problem, which is to say, the Trump administration's national security strategy and national defense strategy are advocating for a very radical shift in U.S. foreign policy, one that prioritizes the Indo-Pacific over CENTCOM, and it's not even close.

Mike Gallagher: Similarly, to the late-stage Obama administration's failed pivot to the Pacific—as yet, this is primarily a rhetorical commitment and not one that has manifested itself in terms of military hardware and diplomatic focus, notwithstanding some incredible and heroic work that certain Trump administration officials, particularly Matt Pottinger, have done. I think we still find ourselves having to balance the exigencies...

Mike Gallagher: So, that's the geopolitical problem I think we have right now, and I think the Biden administration will confront that problem. There's a risk if we don't get a few things right that we could find ourselves sucked back into CENTCOM as we're struggling to prioritize allies and partners in INDOPACOM—if that makes any sense, if I understood the question correctly.

Martijn Rasser: Yeah, absolutely. I think that answers it very well. Does anyone else want to weigh in on this particular point, because this is a pretty fundamental issue that we'll be grappling with over the coming decades. All right. Well, let me pivot to Mark real quick. The commission has a lot of ideas for public-private partnerships, and one that I've found particularly interesting is creating a National Security Investment Corporation. What would the mission of this entity be and how does the commission envision this corporation working?

Mark Montgomery: We can't rely totally on the existing USAID, USIDFC programs that are running right now. Our theory was that we needed to backstop U.S. investment in getting proper funding in particularly the IT hardware industry. I was going to jump in when Sarah was talking—she made a great point about when you're asking about investment out in Silicon Valley—as I recall now, somewhere between 95 and 97 percent of the startup money is going towards software versus hardware enterprises.

Mark Montgomery: And I think it has to do with what she also—I think she mentioned having strategic patience—and getting investors that have strategic patience to deal with a hardware startup. I just think it takes a lot longer from initial investment to the realization of a decision that you're going to succeed or fail—not profit, just the recognition that you're going to succeed or fail—and that there's not enough patience in the investors to do IT hardware. And so something we dominated in—if you go back to 1998 and Lucent Technologies—the IT hardware industry equipment areas that we dominated in, or at least had a plurality stake in, we're down to one, two, three percent.

Mark Montgomery: The only exception I can think of to that is the microchip assembly tools, where we still compete with the Dutch and the Japanese, the three countries, in making the really high-end ones that go into the U.S. and Taiwanese and Japanese microchip foundries. But the truth of the matter is, we don't have the strategic patience to do IT hardware investment. Part of the vision was that we would create a backstop funding to support the time consideration that went into that and try to get more private sector investment into the IT hardware industry.

Martijn Rasser: No, thank you for that, Mark. I really think that's a very interesting recommendation and something I hope that the incoming administration and Congress looks at very closely. I want to turn to another audience question now. Of course, the SolarWinds hack is still very much in people's minds. How can the recommendations of the report—the main report by the commission—how can they apply to helping to prevent or responding to the hack?

Mike Gallagher: Well, I'm happy to jump in unless someone else... As I view it, and obviously there's a tendency to think, "Well, if only they had listened to us, this would have been prevented." And who knows? That's a counterfactual that's impossible to play out. As I mentioned before, we do think, and Mark can jump in if he thinks I'm wrong, that even allowing CISA the ability to do threat hunting on .gov networks—because you have to start from the assumption that your networks are compromised—would have at least allowed us to detect this quicker. And I think it's notable that it was FireEye, not the federal government, who sounded the alarm originally.

Mike Gallagher: I think also funding of the hunt and incident response teams at CISA is absolutely critical to preventing or mitigating an attack like this. And there are several provisions in the NDAA that were aimed at strengthening CISA's capacity to carry out its mission. If you read just the executive summary of the Chairman's letter that Senator King and I put out, we explicitly say, we believe the right approach is to elevate and empower CISA to do its mission. And while neither CISA or the NSA will ever be able to compete with the private sector on salary, they can compete on mission. The NSA and CYBERCOM compete quite well on mission right now.

Mike Gallagher: And we think eventually, CISA can compete on mission if we give it the tools it needs to actually accomplish its mission. The other things I just would highlight is we had NDAA provisions ensuring resiliency of the nuclear command and control systems from a cyber perspective. Then finally, we believe that a National Cyber Director that is well-resourced and has the ear of the President would be in a great position to be a point of coordination and leadership within the federal government, and then do outreach to the private sector, which we think would be critical in a SolarWinds-type scenario. I'd ask Mark to chime in with anything I missed.

Mark Montgomery: No, I think it's spot on. It would be wrong for us to say, "If all 82 of our recommendations had been taken up in November, this wouldn't happen." This clearly was already happening. I would say, if you went back 10 years and did the institutional changes that we recommend across technology, people, and processes—and Congressman Gallagher mentioned all three in his discussion there—and you are consistently funding those properly across the .gov and allowing the .gov to build the relationships with the private sector it needs to have, maybe something like this would have been harder to achieve, certainly at this scale. But you can't rewind the clock 10 years.

Mark Montgomery: We have these 82 recommendations—30 to 40 have been taken up between law and executive branch actions—and if we continue to do them, we'll be in a safe condition. But I do think anomalous activity detection and threat hunting, red teaming, are key to operating in a zero-trust environment where you can never be sure that the software and hardware you have running on your frontiers is keeping out the adversary. By doing the anomalous activity detection, doing the threat hunting, you put yourself in a better position. Congressman Gallagher mentioned the three or four different places where we have pushed that, and which were agreed to in the current authorizations or appropriations.

Sarah Sewall: If I could just chime in here. I think one of the interesting challenges that we've consistently had is whether or not the paradigm that we've been using for cybersecurity—and whether the kinds of incremental innovations the industry has been offering—are really meeting the bill for what Mark just rightly referred to as the need to move to a zero-trust environment. Do we have the kinds of AI applications that we need to be able to have the ability to monitor in real time? Are we thinking in the right way about the tools that we're going to need to verify hardware, regardless of its provenance—where it comes from? Because we're going to continue to live in a globalized environment and we're going to need to be able to look at hardware components when they come in.

Sarah Sewall: Those are some of the innovation angles that I think will remain critical because we are, I think, at a point where we really need to not do more of the same in the way that we've been proceeding, but with this larger paradigm shift that—I think the Solarium Commission is really an important lever to begin to move us—we've got to think about the problem in a different way. We've got to recognize that we're going to be managing risk, we're not going to be eliminating risk.

Sarah Sewall: We're not going to be moving from perimeter security to identity-based security, and we're going to be having to recognize that we're in an environment where we never really have full trust, and we're going to have to learn to manage that. And it's a really different paradigm for the country and for industry. The key is, how do we get government to incentivize private sector to not just make more profit off of a model that's not really working for us as a nation, and instead shift into a different way of problem solving to move in the direction that the commission is recommending?

Martijn Rasser: Great. Thank you, Sarah. We have another audience question and I'd love to get everyone’s thoughts on this. The question is, there was an interesting point raised that our innovation base needs to be global and it's not just American talent we should be relying on. What should the Biden administration do on this front? I'll open that up to anyone, so whoever wants to jump in first, go right ahead.

Sarah Sewall: Well, I'll jump in. We need to welcome talent. This is a theme that a lot of the different entities that have looked at innovation have been harping on—and it's immigration writ large, it's visas writ narrow, it's even, and one of the interesting things is, we were talking earlier about Australia—the Australians have extraordinary quantum talent, and there's really limited quantum talent globally, and the U.S. and Australian firms like to share talent. Some of our export regs even seem to implicate the movement of persons, and their ability to come to an American firm and work for an American firm can trigger all kinds of legal ramifications. We have to look at all of that miasma that gets in the way of what I think Mark and the Congressman were talking about, the need to really build a democratic coalition of trusted partners to tackle the most important questions.

Sarah Sewall: We're going to have to divide and conquer on particular problems, and we're going to have to really pool our intellectual learning together. There's a host of stuff that I think is quite congruent with President-elect Biden's mentality about what it means to open America to a global world. I expect to see progress on that front.

Sheena Chestnut Greitens: Yeah. If I could jump in on that as well. I think that the United States should be thinking about itself as engaged in a competition for global talent, and thinking about how we attract the best, most innovative people to come and work in the United States. And I think—unfortunately, to a certain extent right now—we've started to frame the problem as innovation or security, because of some of these really pressing issues that we've had with the use of, and misuse of, researchers in the Thousand Talents or other talent recruitment programs in China in particular.

Sheena Chestnut Greitens: I think it's a mistake then to see it as, "Well, we can enforce these reporting requirements and we can do the appropriate counterespionage or counterintelligence work on university campuses or in our laboratories," as it relates to these technologies, and that is somehow incompatible with also competing for and recruiting the best global talent for our own innovation base. However exactly we debate and talk about these issues in the future, I think it would be a mistake to frame that question as an either-or—it has to be both-and. We have to pursue effective security and innovation at the same time until we need immigration visa and education policies in particular that approach it as a both-and not an either-or.

Martijn Rasser: Great, thank you, Sheena. Mark, Congressman, any thoughts on this particular question?

Mark Montgomery: Yeah. I would mention one thing—and first, I talk domestically, there's something we can do. We have a program called Scholarship for Service, pays the ROTC bill for about 380 kids a year right now. About a thousand are in it right now. It's for two to three years, and they then go work for the federal government. They get their clearances while they're in the program, they do internships at federal agencies. They then go work for the federal agencies, pay it back. Similar to ROTC, the program I did to get my commission in the Navy.

Mark Montgomery: I think it's a very effective program, and it's one that, when we dreamed it up 23 years ago, it was supposed to be 2,000 a year, which is how many federal cyber security workforce had to join the workforce that year. It's now up to 4,000 a year, need to join, and we're still stuck at 350 graduates. If you put money in, the program grows. And here's the beauty, it grows the computer science department, the STEM departments and the computer security departments at all the universities, colleges, and community colleges that you invest this in.

Mark Montgomery: And it has in fact, if you study the 75 or 80 schools it's at, it has improved all those schools well beyond the 10 to 12 scholarship students they have in place, but it's paid for professors, paid for more labs. It is a fantastic enabler, and that's where the government's best. And I suspect that there's a foreign student aspect to this in the sense that if we can grow these departments better and better, we allow these students to come in, we allow them to stay and work, we're going to benefit long term from this, for the building of this STEM education infrastructure. It's still one of our great advantages.

Mark Montgomery: There's a reason the Thousand Talents come to the United States to mess around with our professors—because we have the good professors, because we have the good labs, because we have good students coming from around the world. And we need to reverse any effort to stop that, and enable it, and particularly enable it for people who could eventually become federal workers.

Martijn Rasser: Yeah, that's an excellent point. Thank you, Mark.

Mike Gallagher: I had one—

Martijn Rasser: Yes, Congressman. Go ahead.

Mike Gallagher: I'm sorry if Mark covered this and I'd zoned out, but Mark and I've just had a lot of each other the last two years. Just as a military veteran, my own experience, and this might just be a Marine Corps thing, but the TAPS process is terrible—the transition assistance—and there's a lot of talent coming right out of the military that could be seamlessly integrated into a government civilian job, but we can't even convince the military to allow people to put their email address on a DD-214, let alone identify proactive talent. That's a low hanging fruit that I think we're not grabbing for what that's worth.

IV. Closing Remarks

Martijn Rasser: Well we're coming up on time here. Congressman, I want to give you the opportunity to have the last word, share some closing thoughts, and then we'll wrap.

Mike Gallagher: Well, first of all, I'm the only non-expert on the panel. You want me to have the last word, but I'll do my best. Thank you to Sarah, thank you to Sheena, and thank you to Mark for letting me be part of this discussion. I just think it's absolutely critical. And not to get sappy, but at a time when I think we're obviously seeing divisions in political tribalism front and center and manifested in some very dark and ugly ways, I just want to assure you that as a member of Congress, work like this is exceptionally bi-partisan and there's just a huge opportunity to build upon it. It's so critically important.

Mike Gallagher: Then the final thing I'd say is, so much of what I do is just leveraging the expertise in places like CNAS and from Mark—that exists in the think-tank and the private sector—and just stealing good ideas where we see them and putting that into legislative language, that discussions like this are incredibly helpful for the legislative process. I salute you for convening it and thank you to all the panelists for your intellect and your thought leadership on this issue, and I really look forward to working with you over the next two years.

Martijn Rasser: Well, thank you so much. That's a great note to end on. I want to thank our speakers, Congressman Mike Gallagher, Sarah Sewall, Sheena Chestnut Greitens, and Mark Montgomery. Thank you to our audience for tuning in. Thank you for your excellent questions. This was a really great discussion. I'm sorry we weren't unable to get to them all, but we'll be doing more events like this in the very near future. Finally, I want to say thank you to my colleagues behind the scenes who made this event possible: Jasmine Butler, Shai Korman, Chris Estep, JJ Zeng, and Ainikki Riikonen. Have a great afternoon, everyone, and see you next time. Thank you so much.