Center for a
New American
Security

MARCH 26, 2020

TRANSCRIPT FROM CNAS TECHNOLOGY & NATIONAL SECURITY PROGRAM EVENT

Engagement and Competition: China, Technology, and Global Supply Chains with the Cyberspace Solarium Commission

Transcript from Engagement and Competition: China, Technology, and Global Supply Chains with the Cyberspace Solarium Commission

I. Opening Remarks

Martijn Rasser: Good morning everyone. Welcome to this virtual panel discussion hosted by the Center for a New American Security in conjunction with the Cyberspace Solarium Commission. I'm Martijn Rasser, Senior Fellow in the Technology and National Security Program at CNAS. Our topic today is a critical one, engagement and competition, China, technology and global supply chains. How the United States navigates these issues will have considerable impacts on the course of the 21st century.

Martijn Rasser: The Cyberspace Solarium Commission made a key contribution to shaping how we address this challenge by crafting a cyber strategy underpinned by dozens of specific recommendations for action. The strategy and findings are laid out in the Commission's Report that was released earlier this month. I encourage you to check it out. The report is thoughtful, compelling, and well-written. It's available on the Commission's website, solarium.gov. We'll dive into the broad themes and several of the specific recommendations made.

Martijn Rasser: A few housekeeping items. We'll kick off the discussion with several questions and then invite our attendees to join the conversation with open Q&A. As a reminder, this event is on the record and being recorded and when we come to the audience Q&A portion, I ask that you identify yourself by name and affiliation. Before we begin, I'd like to introduce my colleague, Megan Lamberth. Megan will manage the interactive portion of this webinar and she'll explain to you how you can engage with us, whether you're on your computer or on the phone. Go ahead Megan.

Megan Lamberth: Thank you, Martijn. And many thanks to all of you for joining our webinar this morning. There are a couple of different ways that you can participate and ask a question in today's session. If you are joining via video conference, you can submit questions in the Q&A box in the toolbar at the bottom of your screen and if you're joining by phone, you can press *9 to raise your hand. Martijn will call out the last four digits of your phone number and we will unmute you at that time. We ask that you please introduce yourself then. Finally, if you're experiencing any technical problems, please feel free to email Ainikki Riikonen at ariikonen@cnas.org. Back to you Martijn.

Martijn Rasser: Great. Thank you, Megan. Allright, let's get right to it and introduce our panel. We're here today with Congressman Mike Gallagher, Representative of Wisconsin's Eighth District and Co-Chairman of the Cyberspace Solarium Commission. Representative Gallagher is a former Marine, a combat veteran, and a former intelligence officer. We have two Cyberspace Solarium Commissioners joining us today, Dr. Samantha Ravich and Chris Inglis.

Martijn Rasser: Among the many hats she wears, Dr. Ravich is the chair of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies and its transformative cyber innovation lab. She's the vice chair of the President's Intelligence Advisory Board. Chris Inglis is a former deputy director of the National Security Agency, currently serving as the Looker Distinguished Visiting Professor of Cyber Studies at the United States Naval Academy.

Martijn Rasser: Rounding out the panel is my colleague, Carrie Cordero, the Robert M. Gates Senior Fellow and general counsel at the Center for a New American Security, adjunct professor at Georgetown Law and a CNN legal and national security analyst. Representative Gallagher, let me begin with you, as co-chair of the Commission, set the scene on the Commission, its mandates and the core message of the Commission's report.

II. Panel Discussion

Rep. Mike Gallagher: Well, thank you for doing this. I'm glad we were able to adjust given the unique needs of the coronavirus crisis and I hope everyone watching is staying safe and staying healthy as we try and get good through these very difficult times.

Rep. Mike Gallagher: Though it was framed a bit differently in the legislation that gave life to the committee, one thing my co-chair, Senator Angus King, and I have kind of become fond of saying as a way to describe what we were after with the Commission was, and we want to be the 9/11 Commission without the 9/11. In other words, what are the changes we need to make now in terms of government structure, authorities and resources in order to restore some semblance of deterrence in cyberspace and prevent a massive cyberattack in particular? What is the mix of cost in position, denial of benefits and norms that we need in order to keep the country safe in cyber?

Rep. Mike Gallagher And though the Commission draws its inspiration from the early part of the Cold War, and what we wrestled with in terms of concepts in the early nuclear age, I do think there is sort of a fundamental difference in terms of how we're thinking about deterrence and so much of the report focuses on deterrence itself.

Rep. Mike Gallagher In other words, if the fundamental dilemma of the nuclear age was insuring deterrence could not fail and that the military must be in the business of waging peace, there was very little room for error and you can sort of read the works of Bernard Brodie and how that influenced Eisenhower and Eisenhower's Solarium sort of went through this issue. I think the fundamental dilemma of our cyber age is that right now it seems that deterrence is almost constantly failing below the use of force threshold in particular and that non-military instruments, particularly private sector actors, must step up and develop sufficient resilience to withstand cyberattacks and strike back with speed and agility.

Rep. Mike Gallagher And I think if there is an overarching sub-theme besides this question of whether the deterrence is possible in cyberspace, to which we answer yes, I do think it's this concept of resilience. How can we incentivize more resilience in the private sector? How can we develop more resilience in the federal government? And over time, through that mix of denying benefits, of punishing bad actors, how can we establish norms or rules of the road in cyberspace, which are not something that are going to be created in a laboratory or even necessarily in a room full of diplomats at the outset?

Rep. Mike Gallagher And so I just would finally say, this experience has been really a unique one and my most rewarding one in my time in Congress. And I think that's entirely a function of the quality of the commissioners that we have. I mentioned my co-chair, Angus King, who was fantastic to work with. Other legislators on the Commission, including Senator Ben Sasse and Congressman Jim Langevin. And then obviously we have two incredibly brilliant

commissioners with us today, Samantha Ravich and Chris Inglis. And there are many times when Angus would lean over to me while we were watching these debates among some of the most brilliant minds of our day in cyberspace and say, "This is how Congress should work every day and doesn't."

Rep. Mike Gallagher And so it was really an honor to be part of this and I want to thank my fellow commissioners for their sincere effort. There were a lot of vicious disagreements, but everyone approached us with a spirit of not necessarily bipartisanship but just trying to figure out what works and what doesn't in cyber, trying to steal the best ideas, fix deficiencies in the federal government, and there really was just a unique mix of people in this effort. And so I really hope everyone will read the report.

Rep. Mike Gallagher Just to end where I began with this idea of avoiding a cyber 9/11, it's why we did some unique things like begin with a narrative written by the authors of Ghost Fleet about what the future might look like if we don't make change right now. We're trying to get your attention. We're trying to engage everybody. That's why we wrote an unclassified report. And so thank you for allowing us to talk about it today.

Martijn Rasser: Absolutely, absolutely. I wanted to just ask you a question. So one challenge I see when formulating recommendations for cyber issues is the rapid pace of change. So how did the Commission address this in this work? Take cloud computing for example, the report emphasizes the benefits of cloud-based services and make several related recommendations. How did the Commission anticipate its recommendations to keep pace with the private sector, such as with changing architecture of cloud services and the varying security capabilities of cloud providers?

Rep. Mike Gallagher Well, first I would say implicit, if not explicit in the report, or at least the chairman's letter in the beginning, is that a recognition of the federal government, to a greater extent sometimes than those of us who are embedded within it tend to appreciate is often not structured to act with the requisite speed and agility necessary to keep up with what's happening in the private sector, and therefore defend our interests in cyberspace. It's not to say we can't, it's just that we need to get comfortable with the idea that since so much of our critical infrastructure is owned by the private sector, there are times when the federal government needs to be a supporting effort and provide supporting fires as opposed to being the main effort. This is why so many of our recommendations are intended to, not with a heavy hand, but you know with the right incentive structure, incentivize the private sector to step up, strengthen their security posture, improve willing to partner with the federal government so as to avoid a breakout on their network.

Rep. Mike Gallagher In fact, whenever we recommend a private sector regulation, our goal or our intent was really just to give the C-Suite a financial incentive to prioritize and improve their cyber posture rather than saying, "You must do it this way and that is the inflexible position of the federal government." It's also why we took a look internally at ourselves and did things like recommend the creation of a House Permanent Select and Senate Select Committee on Cybersecurity, not only to consolidate authority, but hopefully they get a repository of expertise on cyber within the legislative branch that can then do more effective oversight of the executive branch and ensure that it's keeping up.

Rep. Mike Gallagher: Finally, I'd say, as it pertains to cloud computing in particular, we are recommending certain things, like recognizing the security disparity among cloud providers, so we recommend the creation of a cloud security certification that providers can voluntarily attest to. But we also recognize that this could drive up the costs of cloud computing services even if only marginally and driving up costs could serve to either slow or decrease adoption, which would defeat the point entirely, and I think that's part of your question. We therefore call on Congress to direct the Department of Commerce, Small Business Administration, and DHS to conduct a study to figure out how best to incentivize the uptake of cloud services for state and local governments and small and medium-sized businesses, whether through small grants, tax incentives or other means. So, with that, I'll stop because we have much smarter commissioners here that can talk about this stuff.

Martijn Rasser: Thank you, Congressman. So, this report comes out of a very consequential time in our nation's history. We're at the cusp of what many believe will be a fourth industrial revolution fueled by technologies, such as artificial intelligence and 5G, fifth-generation wireless telecommunications. Cybersecurity is more important than ever. The current pandemic crisis further underscores the need for secure, robust and resilient cyber infrastructure. So before we discuss further details of the Commission's report, I want to take a step back and place it in a broader context. Carrie Cordero, what lessons should we draw from the Commission's report at this difficult time and what are relevant lessons from past systemic shocks the United States has faced?

Carrie Cordero: Thanks, Martijn. So first, I think I want to step back and just talk about the report a little bit in the context of what we're all currently going through with respect to us all being working remotely, and some of us working from home, and having to adjust all of our personal and professional lives and the disruption to the economy because I think there is a very common thread that we can draw from the current environment to the warnings that are provided in the Commission's report.

Carrie Cordero: And so the Commission has really done an incredible job of laying out the entire breadth of issues and really serving it up on a platter for action to be taken both by the executive and the legislative branch. I think the tension that some of us in the national security community are feeling, this week and last week, and I expect in the coming days and weeks and months, is that on one hand we have this current crisis with the coronavirus and on the other hand we want to make sure that other national security issues, other issues relevant to defense and foreign policy aren't ignored and don't get shoved to the side.

Carrie Cordero: In this particular circumstance, when we're talking about strategic issues related to cybersecurity, they actually are really interrelated and so I want to first underscore Congressman Gallagher's comments that what we don't want to do is wait for that so-called cyber 9/11, that the Commission is a call to warning to provide impetus for action and what we don't want to happen, what I would hate to see happen is these 75 plus recommendations be put on a shelf only to be taken off the shelf when something dramatic happens.

Carrie Cordero: Now, second, why I think that is particularly relevant, and actually more urgent given our current situation, is that one of the aspects of the report, one of the recommendations of the report, calls for a plan for continuity of economy. Well, what the report was talking about, and what the Commission was addressing, was continuity of economy in the context of a

major cyberattack. What we're seeing in the coronavirus environment is that our government did not have in place a continuity of economy plan in place for a pandemic incident, and so now the Senate has taken action. But we certainly are in a position of where there is dramatic effects on the economy and we're playing catch up by trying to develop a quick plan on the fly.

Carrie Cordero: What the Solarium Commission recommended, and which is really I think urgent given the current circumstance, is that we need those types of plans and those strategies and those playbooks to be ready to go when the incident happens. And then the last thing I'll just add to that in terms of the connections between our current environment and the Solarium Commission report, is that there is not a day that I have logged on in the last two weeks that I don't fear what a maligned actor could do to our operations and to our economy now that so many more of us are conducting our business online. So I feel not that the Solarium Commission's Report is something for another day in the current environment with the coronavirus, but my perspective is that its recommendations and action on them are more urgent in the current environment.

Martijn Rasser: Thank you Carrie. Thank you. Chris Inglis, let me post this question to you first and then we'll explore this topic from several angles. What are the challenges that China poses in cyber? And as a corollary, I also want to ask you since we already, through our chat screen, have a question from Se-yong Kim from Voice of America, North Korea being the hot potato in the realm of cyberspace. If you're ready to address that point as well, please do so. But go ahead please, Chris.

Chris Inglis: So thanks for the question. If I can just first add a point to Carrie's points. The Commission, when you look, has quite a lot of detail, over 80 recommendations, but you'll note that we avoided the technical details of specifying, either in technology or in implementation, particular responses that would be relevant to the current circumstance, or perhaps technology specific. And what we really tried to do was to look at roles and responsibilities, such that we could harness all of the talent, all of the perspectives in our larger society. And because at this very moment we're finding that we have a massive reframing of how we deal with the infrastructure that we know as cyberspace, agility is probably the number one feature of what we need going forward.

Chris Inglis: Most of us today are dealing with this particular teleconference from places that we would never have imagined a week or two ago would be our primary workplaces. That last tactical mile may or may not be as well defended as we would hope. If we have agility in terms of reframing the architecture on the fly, if we've got built in the necessary resilience and robustness anywhere in our society, we can in fact stride for stride, stay a pace of current changes that are taking place in the current situation.

Chris Inglis: You asked specifically about China, and perhaps by extension North Korea, which might be another player in the room. I would say that what we see in the form of China is an attempt using economic methods, using perhaps engagement of global standards bodies and a rapid push of technology, which perhaps leaves security behind. A great challenge to us, us being the United States and like-minded nations, in terms of having the sort of technology, the resilience and robustness and that technology and the competence that the legal regimes that go hand in glove with that technology to serve our purposes.

Chris Inglis: 5G as a case in point, that very dense, somewhat autonomous brand or bent bag of technologies, which is now being introduced to the world is going to fundamentally change our opportunities to have some degree of autonomy, whether that's in self driving cars or devices that constitute an ability to manage our critical systems. But if that's not done in a way where we have confidence in the inherent security, resilience and robustness, if that's not done under our legal regime where we have confidence that we'll defend the privacy interest of those persons whose data is inside of that, we will wind up ruing the day that we gave that away to a player that doesn't have the same values, standards and approach that we do.

Chris Inglis: In all of those areas, we believe that China is not essentially approaching this in a way that is suitable or consistent with our interest. They massively invest in companies like Huawei to perhaps tilt the economics in favor of national industries. You can buy 5G gear from Huawei at probably 40% below a what would be a fair market price. They've taken over the standard's bodies largely through sins of omission on the part of the United States and others in ways that they've locked out American or like-minded nations have ability to play fairly and freely on that market foundation. And the security, while we've looked for smoking doors and not necessarily found them in gear like Huawei, the security is sufficiently bad that there are a number of front doors. The stuff is just not built very well. Even if it was built very well, the legal regime that China could bring to bear in terms of accessing the content of the information that's coursing through those systems, should concern in any privacy advocate within the United States.

Chris Inglis: All of that says that China is a real and material competitor. They're essentially trying to compete on a playing field that they've established according to their own interest and we need to challenge that. We need to do that using our own values. The report talks about what that approach might be. I'll leave it to a further discussion about some of the specific recommendations we've made. But it is a real and material challenge to us. It comes in the form of not simply China but Russia and North Korea, others taking unfair advantage with no consequences for their bad behavior in this space.

Martijn Rasser: Great points. Thank you. Samantha Ravich, how do you assess the China threat and what should the United States do in response?

Samantha Ravich: Well, thank you. Let me also kind of key off of some of the other comments first that that were made even back to the cloud computing that Representative Gallagher had talked about and some of the recommendations from the Commission. I think over the next hour, we're going to be drawing a lot of lessons about, we're currently in a live fire exercise, right? About what we have talked about, what we said might be coming in the cyber realm. We're seeing it now obviously play out on the coronavirus level on our economy and even when we talked about the cloud computing, the smaller cloud computing companies right now could be facing extremis, right?

Samantha Ravich: If they have one or two people in, in their organization that come down with a virus, will they be able to staff correctly? Will they be able to take care of the cybersecurity measures that they have to? The big ones, yes. The small ones, maybe not. Like other companies, they're kind of potentially moving resources away from cybersecurity just to stay alive in this very, very challenging environment. So, when we put recommendations out on a cloud security certification, that there are standards that that need to be met, if we had those in

place at this time, I think we would be stronger for it, even in that particular instance on cloud computing. But we'll be able to draw that out as we continue this conversation.

Samantha Ravich: In terms of China and the threat from China, no surprise to anybody in this audience that China is using lots of different tools and methods to really fuel its economic rise to undermine our strategic capabilities. We came into this Commission thinking about the notions of cyber-enabled economic warfare where an adversary, such as China, uses cyber means to undermine key components of our economy in order to weaken us militarily and strategically as both Chris and Representative Gallagher have said. Up to this point, we really haven't been positioned well to defend against it, to understand how this is rippling across our economy, even prior obviously to coronavirus. And I want to get back to this moment in time and how it connects to all of this and what to do about it.

Samantha Ravich: [Inaudible] we see following now that certain parts of defense, industrial base, certain parts of the innovation base particularly so that China can grow stronger and we weaker because of it. I'm very concerned that again at this moment where our economy is being set back by coronavirus and the ripple effects that China will once again press its advantage. I mean there's going to be companies inside, very important strategic companies, small ones, medium size ones, probably not the largest ones, although I don't know about that, within our DIB that will be looking for lifelines, right? Whether it's bags of cash, whether it's bridge loans, whether it's just buying devalued stock.

Samantha Ravich: We could wake up from this nightmare of the virus and find that a number of our key economic assets are now in the hands of a competitor/adversary. So, on the bringing it back to the cyber side of this, this is we really did look at in the Commission through the lens of we are the number one military in the world because we are the number one economy in the world. We cannot separate these aspects protecting the strategic strength of our country on cyber without understanding the absolute critical, vital role of our economy and our economic actors in this. China understood this well before we did, and so the lens and the focus of the commission is to kind of reorient and realign that balance.

Martijn Rasser: No, great. Thank you. Representative Gallagher, Carrie Cordero, anything you'd like to add to these points?

Rep. Mike Gallagher No, I just would say, I mean, there are so many things to unpack when it comes to the challenge posed by China and cyber. I just would say beyond the technical challenges, the sort of challenge or concern associated with a country that doesn't share our values dominating the future of 5G internet. I do believe there are more insidious ways in which China is openly and legally exploiting certain aspects of D.C. to wage information warfare and political warfare.

Rep. Mike Gallagher Right now, obviously we've all seen in the context of coronavirus certain rhetoric coming from the Chinese Communist Party threatening to block exports and therefore plunge us into a sea of coronavirus to steal their phrase. But for a long time, they've been exploiting loopholes in FARA and LDA disclosure requirements to hire a lot of very senior former legislators and cyber aficionados and that can inject an enormous amount of influence and disinformation into our political bloodstream. And so not trying to, I'm very conscious of the fact that my district produced Joe McCarthy and I'm the second Marine intelligence officer ever elected to Congress from Wisconsin. But I just do think there's a whole, an

under-explored issue of CCP influence domestically in the United States that makes these technical issues very challenging to unpack.

Carrie Cordero: I would just add also Martijn, that I think one of the challenges that has taken place, and I think the Solarium report moves us and advances us in this respect, is that so much of the malign cyber activity by foreign nations, particularly China, have been so behind the scenes that it's not a malign foreign activity that has been apparent to those sort of outside either the economic community that has been impacted by it or outside the defense community that has been victimized by it, if we want to talk about the theft of IP for example, or beyond the cyber policy community, absent some immediate news articles that focus on a particular attack or particular activity, all of the malign cyber activity that is going on, on a daily basis, it's not apparent. We don't see it in the physical world.

Carrie Cordero: And I think that that, it sounds obvious, but that challenge I think has then made it difficult from a public perspective and also from a legislative perspective to gain traction on these issues. I think one of the most valuable contributions that the Solarium Commission report makes at a high level beyond the end of all of the many valuable individual recommendations, but at the bigger picture level, the contribution that it makes is it coalesces in one place, in one unclassified report, all of these events that have taken place and that have taken place over a period of the last 10 to 15 years. Whereas normally the public is used to digesting them as, well there was this particular incident or that particular incident. So I think the fact that the report identifies all those and identifies them in an unclassified way, in a very digestible way, is an important contribution. And I hope that the transparency about the activities that are going on is something that we can do more on in the future.

Martijn Rasser: Yeah, that's very true Carrie. I mean, it's a very compelling report for exactly the reasons that you identify. I think this is probably a good time to perhaps dig into the tenants of layered deterrence, which this report lays out. Chris Inglis, would you like to tell us about what exactly that means and what it entails?

Chris Inglis: Yep. Thanks. I'm mastering a technology that I've only first used in the last two weeks, so thanks for your patience. Yeah, thanks for the question. So, as Congressman Gallagher indicated early on, while we believe that deterrence has not been working, and certainly classic deterrence has practiced in the nuclear age has not been working, we believe it can. And we recommend kind of from the top down a three-part strategy. We call it layered deterrence in the report, which essentially has three broad lines of effort.

Chris Inglis: The first would be to shape the environment, to essentially set expectations about what rational behavior is, to essentially establish roles, responsibilities such that folks, individuals, nations who engage in activities in that space have an understanding about what the U.S. and like-minded nations expectations and aspirations are in that space.

Chris Inglis: Second, broadly to practice what we used to call them in the traditional deterrence age deny benefits, to build in sufficient resilience, robustness, an ability to discern how the environments are actually being used and to counter either malicious activity and malign activities in a way that it's harder for an adversary to essentially have their way with us.

Chris Inglis: And then finally, for those adversaries that still come at you, whether they're criminals or nation states and everything in between who violate, intentionally violate those normative behaviors, to impose consequences on them, to impose costs. And in that regard as Congressman Gallagher indicated, while we have affirmed the use of military power, Cyber Command particularly, what we really did was to describe an environment where we have to use all instruments of power, some of which actually are already owned by the private sector in terms of what they can do using the various perspectives, authorities, capabilities. We don't go so far as to put the private sector in an inherently governmental role but the private sector and the governments, plural, working side by side can in fact impose consequences in a collaborative manner on adversaries in the space that make it such that if you're an adversary coming at one of us, you've got to beat all of us.

Chris Inglis: Across to all of that, we tried very hard to use market forces, regulation where necessary, but use market forces to effect defense in a collaborative integrated manner, as opposed to a division of effort where everyone defends their own patch and we can be essentially picked apart one by one, and imposing consequences to do that in the largest possible context, and international context is the one that is most strongly preferred. And so there's a very high premium given to working with international partners to ensure that when and whenever we can, we essentially approach this with the common values underpinning those alliances and use the mechanisms that broadly are available across many governments.

Martijn Rasser: Yeah. Multilateral approach will be critical to executing this well, including I think for the supply chain vulnerability issues that we're facing now. It was something I'd like to dig into some more right now. Dr. Ravich, why are our supply chains so vulnerable? How did we get here and, more importantly, what can we do about it in response? I'd love to get your thoughts on that.

Samantha Ravich: Well, we got here because the world is an interconnected place and market forces were looking for the most efficient, most cost-effective way to build their supply chains, and not a lot was thought about resiliency for this in a national security context. So over the last decade, decade and a half, we've seen these supply chains grow out for the major companies, especially the major companies in the defense industrial base, to thousands if not tens of thousands of contractors, subcontractors, and so on and so forth down the line. So much so that the Department of Defense really doesn't have any idea who is in the supply chains of the most critical parts of the defense industrial base. And when we kind of all open our eyes to the fact that all you need is a weak link to get into a supply chain, whether it is counterfeit items, which we have seen counterfeit items go into numerous, numerous quantities go into our defense industrial base, defense supply chain, or malicious code, we realize that we have a serious problem.

Samantha Ravich: So as we thought about, okay, what steps can the Cyber Solarium Commission make and recommend to kind of harden that supply chain? First of all, you need to understand it better. So we have recommendations in there on how the government needs to collect the data to better understand who is in the supply chains or in the defense industrial base, and the broader parts of, let's call it the national security industrial base, because first you have to know what's out there to be able to know what to protect. Then be able to prioritize those critical pieces that have to either be brought back onshore or for a like-minded, friendly country so that we are not put at risk from having those parts of the supply chain ended during crisis or extremis, manipulated counterfeit items put into it.

Samantha Ravich: We had talked about, again, live-fire exercise, what we're going through right now. Where are the N95 masks? Where are the respirators being made? Where are the pieces that are so important to our current medical supply chain, our pharmaceutical industry? We can talk a lot about that. Obviously important for our citizenry as well as our military capabilities that we have the ability to produce onshore or in friendly nations what we need. But again, it goes to a fundamental piece of the Solarium Commission, which is this if we want to have deterrence and, as Chris had said, resilience is a major part of deterrence, right? So that the adversary knows that if they attack us, we will be able to stand strong. We will be able to reconstitute what we need and what we must to be able to impose costs back upon the adversary.

Samantha Ravich: Hardening our supply chain is a key component of continuity of the economy so that the next day after a cyber day after we have those components ready to go. If I may, let me just talk for one second about this continuity of the economy, which Carrie had mentioned at first. It's a key component, key recommendation of the commission. We can talk about how it would actually be put into place with the planning cells. But it again fosters deterrence, it's not just what the government can do for the country. Deterrence also in resilience has to be what our economy can do, what it must do, as well as the citizenry itself. So things such as in continuity of the economy, understanding what are the key critical nodes that all else depends on in the economy so that they can be protected.

Samantha Ravich: We're seeing again in the coronavirus live-fire places like Walmart, places that know how to do distribution on a large scale. Who would have thought that they're a critical or essential infrastructure, right? I mean, all of the technology that we're doing to be able to communicate, to be able to share information, not just our electric grid, which of course is key and vital. Let me do a very clear shout out to Tom Fanning who was a commissioner on the Cyber Solarium Commission, CEO of Southern Company. They're a major grid utility operator [Inaudible] they serve. Tom Fanning was absolutely fantastic as a commissioner. He kind of brought to the Commission the understanding that in the grid and other places part of resilience might mean going back to analog, having the ability to actually pull a lever that will shut off a system if need be.

Samantha Ravich: We need to be thinking, and we are in the commission, what we've put forward as a pathway for continuity, the economy, things such as, as I said, critical nodes, going analog. How do we protect and restore C-data for key parts of the economy to be held here or potentially to be held in overseas friendly nations and the resilience of the American people themselves? In the cyber context, throughout the report, we have key recommendations that give the American people the ability to understand what is maybe more safe and less safe in terms of the technology that they are buying, that they are using. Right now, who knows as an American citizen, if you buy one device versus another, what's more secure. Pushing it down to even the citizenry level because we are all in this together and we cannot have resilience if we don't have the economy and the citizenry as key parts of it.

Martijn Rasser: Thank you for that. Carrie Cordero, as a lawyer and legal scholar, what's your perspective on how to restore credibility to supply chains?

Carrie Cordero: Well, a lot of it are some of the things that Dr. Ravich and Chris Inglis just described, which has to do with international, making choices about what we are going to bring back onshore. But then also I want to underscore something that I think they both mentioned, which is the

importance of international partnerships. We have friends in the world, and we need to, as the Commission report encourages us as to do, develop those partnerships and work with those that are allied countries to counterbalance the malign influence and counterbalance the bad actors.

Carrie Cordero: Those partnerships, in this area, in the supply chain area are at the intersection of national security issues and the economic issues. So the countries that we should be looking at and the partners that we should be exploring how to do this with are those who are aligned with us both on the economic aspects and who we think that we can produce productive partnerships with and on common national security interests. The other piece that I'll mention, which hasn't been mentioned yet, but is also relevant to our current national conversation, and so I think it's worth flagging that it also was in the Commission report, is the role of the Defense Production Act. So many of us have learned more about the Defense Production Act just this week as it has been invoked in the coronavirus response as to whether or not it should be used and how it should be used to mandate industrial production of certain devices and equipment that will help first responders and help the medical community.

Carrie Cordero: The Commission report has some specific recommendations about the role of the Defense Production Act, where it can be used, and how it can be used, and proposes amendments to it in ways that can potentially help with this supply chain issue. And so I thought that that was something that hasn't really been explored before and that the Commission provides them new recommendations in that area. The other area that the Commission spends time making recommendations on to help improve the supply chain is the investment in research and development. And I think also because the Commission draws its mandate from a historical perspective of the critical role that U.S. federal government has played in funding at the nascent research and development level important and really globally changing technologies that have affected the world. On the R&D side, the Commission report recommends that more investment be placed on the research and development side to help drive the investment and the increased development and innovative thinking on the U.S. end that can help get us way out ahead on the supply chain issues.

Martijn Rasser: Congressman, I'd love to get your thoughts on this issue as well. And also, do you see any historical precedents that are applicable in this scenario?

Rep. Mike Gallagher Well, first let me add a point to what Ms. Cordero said about the importance of allies. There was a Chinese academic, I forget who it was, who wrote an op ed, I believe in the New York times, in 2015 talking about U.S.-China competition before great power competition was the dominant phrase in our lexicon. And he ended with something that has sort of haunted me ever since, that I think is true. And he said the core of competition will come down to who has better friends. I do think while if you were to sequence the various layers of our strategy, I mean it'd be very difficult to do, we kind of place a premium on deterrence by denial while recommending more speedy deterrence by punishment and recognizing that over time it's going to be difficult but not impossible to entangle our friends and adversaries in a web of norms.

Rep. Mike Gallagher At the end of the day, I just would like to underscore the importance of allies in this space, particularly at a time when we see the CCP trying to actively exploit this pandemic in order to expand their influence around the world. And so, I really think that the question of what

does responsible decoupling from China look like? Not total decoupling. In other words, I suspect we'll always want Wisconsin farmers to sell soybeans to China, we'll always be willing to buy cheap t-shirts from China.

Rep. Mike Gallagher Here in the United States, I do think over the next decade, almost regardless of who the president of United States is, because I think this is the new consensus position in U.S. foreign policy, we're going to have to go through this very difficult process of identifying what supply chains we are willing to pay to shore up, make more resilient, and bring certain manufacturing involved in those supply chains back to the United States. The obvious topic right now is our pharmaceutical supply chain, our medical supply chain, but the same could be said about a ton of aspects of defense industrial base as Commissioner Ravich laid out. I think there are just a few ways in which we can do that. I mean, I do think we're going to have to find a way to sort of draw a moat around foundational technologies, sustain independent supply chains, provide transparent capital markets. That's probably the lowest hanging fruit, and all of that is bound up in this broader effort to ensure our freedom from economic coercion.

Rep. Mike Gallagher Whether there are historical precedents ... You know, it's interesting. I actually yesterday sent an email to some smart Cold War historians, and I asked them for what are the best books on the economic relationship and economic history of economic warfare of the Cold War in terms of us versus the Soviet Union. I'm starting to build that list myself, but I think what makes this competition much more difficult in some ways than our competition with the Soviets in the Cold War is precisely this point. It's that we didn't have to decouple from the Soviet Union because our economies didn't really interact that much. We are so, at least since 2001, we've become increasingly intertwined with China that we're discovering how difficult it is to decouple. But that's going to be something we have to figure out over the next decade.

Martijn Rasser: Oh, thank you for that. Mr. Inglis, do you have any thoughts on this particular topic?

Chris Inglis: So, I think that's all extremely well covered. I think we might have some questions to get onto, and so I'll leave that on the table as it has been described. Well done.

Martijn Rasser: Okay, excellent. Thank you. One final question before I turn to audience Q & A, and this is for the panel as a whole. We've talked a lot about the challenges we face with China. Where do you see room for engagement? What opportunities do we have to have a constructive dialogue with Beijing on these matters? If anyone ... Samantha Ravich, do you have any thoughts on that particular issue because there should be hopefully some areas where constructive dialogue can take place or perhaps you don't see it?

Samantha Ravich: Let me just say, I mean, there are things to explore so that where we are now doesn't get into something that resembles a hot shooting war, right? No one wants that, and but you can put your mind to it and see how it could be stumbled into. Whether it's South China Sea contingency, or it's something having to do even closer to our own hemisphere or where we're [Inaudible].

Samantha Ravich: Pharmaceuticals are something that we absolutely need for the protection of the homeland. So, making sure that the kind of where the boundaries are, and some of it will take place in establishing those boundaries through dialogue. Some of that establishing those boundaries

will take place through persistent engagement on the cyberspace, and we also talk a lot about that. But, as we become more robust in our pushback, which I think every commissioner aligned with on this, it will open ... I think open the door to a better dialogue, especially for us.

Samantha Ravich: We've been in dialogues in the past with the Chinese, and we haven't been able to enter it through a position of strength. So, what the Commission really focuses and certainly in one of those parts of deterrence, will allow us to open that dialogue from a much, much better position than we have for the last two decades.

Rep. Mike Gallagher Can I add a quick point on that? So, and I'm sure there are areas of cooperation, but let me invoke Mattis. Not Jim. Peter Mattis has a great argument on this, and he talks about and really chronicles how those advocating for engagement with the PRC, have typically pointed to four areas where it's in our interest to cooperate. WMD proliferation, economic interdependence, stability on the Korean peninsula, and environmental issues. But if you go down the list, we failed to make meaningful progress in all four areas.

Rep. Mike Gallagher For example, Chinese promises that would build export controls to monitor dual use technologies never translated into action. We expanded economic ties, but at the cost of widespread technology transfer and course of trade practices. China has consistently helped undermine North Korean sanctions, and I would argue destabilize the Korean peninsula in the process. And obviously, perhaps most obviously, China's environmental track record has been abysmal or mixed at best.

Rep. Mike Gallagher So, I'm sure there are ways to engage going forward and the avoidance of great power war is always a good idea, but even on those modest terms, engagement has failed to produce its desired outcomes.

Samantha Ravich: And if I can add one final piece on this, which is, I guess for those that really want to lean forward into international norms, trust but verify requires that you can verify, right? There's a lot of work that we need to do as a country and with our allies to get better on our technological capacity to verify before we commit to more quote international norms that require trust, because there is ... We are not in a position, let me say, to sign up for more international agreements where we can't verify that our interests are being secured and that the other signatories are living up to their commitments.

III. Audience Q&A

Martijn Rasser: Excellent. Well, I think this is a great point to turn to audience questions. We already have some coming in. Just a reminder, you can use the Q & A feature if you're on your computer. If you're on your phone, just hit *9 and we'll be able to take your question that way. The first question which I will read to everyone is from Joe Nye. He says, "I like layered deterrence, but how far can we shape Chinese expectations in the first layer? We clearly do not want Huawei in 5G, but what can we reasonably expect them to agree to? Our Global Commission on the Stability of Cyberspace suggested eight norms including noninterference with the basic structure of the internet. What do you think is feasible?" That's an open question for the panel, so whoever would like to jump in, please go ahead. Go ahead, Chris.

Chris Inglis: Yeah, so I think the answer in part builds upon what Congressman Gallagher and Dr. Ravich just said, which is there are three ways to engage China in this regard. One is in dialogue to ensure that they are clear about our expectations and the consequences of not meeting those expectations. Two, to our actions. How we build, right? The sort of systems that Joe talks about. What standards, what sort of resilience, what sort of robustness we build in such that we have kind of lived out our own expectations. And then finally, the consequences that we impose both positive and negative on those who don't live or abide by those expectations.

Chris Inglis: There's a range of remedies that we can bring to bear, not simply for the Chinese, but for anyone who impacts the global infrastructure on which our society and other societies depends. We've not been coherent or consistent in imposing consequences, positive or negative, on those who depart from those norms. Carrie's quite right, or I'm sorry, that Samantha's quite right in saying that we need to actually understand who's doing what in this space. We need to improve the alignment between attribution and those consequences, but if we do those three things, then we have a fair expectation that China will be held accountable for how it operates in this space, and that we might in fact, if we invest in the resilience and the robustness, define and insert into this space those systems that we would prefer to use.

Rep. Mike Gallagher Can I just add that particularly when it comes to 5G, I think, over the last three years we've tried to play aggressive defense in order to begin the process of setting standards. We're seeing some progress. Our friends in Australia and New Zealand led the way. More recently countries like Vietnam and Japan have joined in making important decisions, but obviously we've seen some disappointing news in the UK. In Germany, I think it's still a jump ball. There's a growing alliance in the Bundestag pushing for standards that would exclude 5G suppliers subject to influence of a foreign country. There may have been changes. I haven't been following German politics that closely, but I think that might be the sweet spot.

Rep. Mike Gallagher It'd be great if other countries join the chorus in warning about Huawei, but ultimately what matters is that they craft regulations that lead to its exclusion and the preservation of competitive global markets. Also, the preservation of interoperability of our networks. If countries are more comfortable landing on a universal standard that bases eligibility for the future of telecoms on interoperability, freedom from extrajudicial state direction, and strictly enforced rules of the road such as intellectual property standards, that's an end state that we can not only live with but I think favors the free world.

Chris Inglis: If I maybe just add to that. There's another Mattis, Jim Mattis, who was alleged to have said when asked what keeps him awake at night, he was alleged to have said, "Nothing." He keeps other people awake at night. Whether that's true or not, but there's a kind of merit to that thought, which is that trying to blunt the activities of China or another bad actor in this space is important, but essentially mobilizing our own, harnessing our own industry innovation. Flooding the zone as it were, is going to be equally if not more important. We need to focus on the supply, the innovation, the security that we would bring to bear in free and fair markets.

Martijn Rasser: Excellent. Our next question is from Susan Aaronson. Susan would like to know, "What do you think policy makers should say about private sector responsibility for large troves of data? We now understand that if stolen and crossed could have unanticipated national

security spillovers, but we need that information. What kind of policies should help beyond basic cybersecurity?"

Samantha Ravich: Well, let me jump in on that. Just at the beginning. So, we did think through all this kind of thorny question quite a bit on the Commission because again, having Tom Fanning there was great representing the private sector. A number of us have private sector experience, and the private sector is right in terms of, up until this point, certain agencies in government just want to take. Give us all your breach information, give us your data, and maybe you'll get something back on the back end to help protect your systems.

Samantha Ravich: We, from our recommendations from our commission, had to realign those market forces, right? Had to make it worthwhile for companies both to help the broader mission of securing the United States and the citizenry, while recognizing and incentivizing that it will be good for their business, right? So, some of our recommendations, for instance on cyber security insurance, right? I mean, how do we make it worthwhile? And this also gets back to, in some ways supply chain as well, to private industry that they will ... What is it? Do good by doing well or do well by doing good, that it behooves them, their shareholder price, customers that will want to buy their equipment because they are making the whole enterprise more secure.

Samantha Ravich: Likewise, on supply chain cybersecurity insurance, it could very well be that companies that have a more secure supply chain, more of the key components here in the United States will have a lower risk premium. [Inaudible]. We really did focus on recalibrating the calculus on having the private entities be able to provide key important information to the government recognizing that there has to be some protection for them if they are sharing more information to make us more safe.

Carrie Cordero: Martijn, can I weigh in on Professor Aaronson's question as well but take it perhaps in a different direction, which is that I'm picking up on what Dr. Ravich said, many of the recommendations ... And I want to speak for a minute about congressional oversight. Many of the recommendations, including some of these issues regarding private sector responsibilities, potential legislation in the area of liability or liability protection, either way, and many, many of the other recommendations of the report overall, speak to action that Congress will need to take. Congressman Gallagher mentioned at the opening of our session today that the Commission report includes recommendations for restructuring congressional oversight as it relates to cybersecurity overall.

Carrie Cordero: What the Commission Report recommends is that two separate new committees, new select permanent committees, be created. One in each chamber, that do not step on the jurisdictions of the armed services committees. Do not step on the of the intelligence committees but do stake out territory where Congress will have a vehicle to act and to potentially even regulate in certain areas that are relevant to whether it's data protection or whether it is cybersecurity.

Carrie Cordero: The mechanism to do that is more streamlined and more robust congressional involvement. The way to do that is through dedicated committees. A colleague of mine, Professor David Thaw, and I had just written a paper earlier this year that encouraged the creation of a joint committee that would and a temporary committee that would act on these issues, at least in

the next Congress beginning immediately in January of 2021. The Commission says, "No, actually we need a permanent committee."

Carrie Cordero: Whether or not it's a temporary one or whether or not we jump right to the permanent one, the point is that in order for Congress to pick up the baton from all of this work that the Solarium Commission has done, there has to be a vehicle to do that legislative work. I just want to take this opportunity because I think these data protection issues, obviously many other of the supply chain issues that we've been talking about, all of this will require congressional action and that recommendation for renewed and strengthened congressional oversight is critical to making these things happen.

Martijn Rasser: Thank you very much, Carrie Cordero. Chris Inglis, I saw you raise your hand a little earlier. Do you want to add to this question?

Chris Inglis: I'll just add to that policy maker, if they were to ask, "So, what insights do we have?" I would say two things. All of what was said I agree with, but the two things I would leave them with is there remains a distinction between what government can do with private information, information that intrudes upon the privacy of civil liberties of an individual. Therefore, there is a distinction between the government having that information and private sector holding that information. But, but even in that first observation, the private sector at scope and scale is collecting information on that heretofore was unimaginable or impossible. We need to then bring a weather eye to that to ensure that there's not some negative consequence that ensues because of how the private sector views their agility in the use of that information.

Chris Inglis: The second point that I would make is that there actually is some good news here, which is that whether it's kind of agreement by agreement. The consent agreements that various users have to sign off on or state by state, and sometimes coalition by coalition. There's the GDPR, there's the California, there's the New York legislation rules that have been brought to bear. That's the good news from the bottom up.

Chris Inglis: From the top down, what then ensues is a somewhat incoherent, disjointed space, and so we do need to bring some greater definition to what our expectations are of the privately held bodies of information. But we need to rationalize what's actually taking place there, and to some degree, make that coherent. If you're an entity, a corporation that operates across not simply 54 states and territories, but across the whole world, you probably have to respond in a different way to each and every one of those in terms of how you're meeting your imposed obligations. That makes it harder to have an expectation that they'll actually do what society needs them to do, so we need to rationalize that as well.

Martijn Rasser: Excellent point. That's an excellent point. The next two questions are from Carlos Aramayo and Jane Tang. They're quite similar, so I'll just collate them. "What is the posture and recommendation that the Commission puts forward to confront Chinese and Russian information influence operations? Who has the authority to help relevant private sector companies tackle this multilayered scenario?" Important questions.

Rep. Mike Gallagher I can start, and then ask my colleagues to chime in. We thought a lot about, I think, sort of a prerequisite for that type of pushback that the question implies is having an enhanced attribution capability at the federal level. We talked a lot about how ODNI ... We debated various constructs of you need a specific separate organization solely dedicated to

attribution. There were a variety of different constructs we debated, but ultimately we're recommending the ODNI, in partnership with the private sector through DHS and FBI, improve its attribution analysis by, for example, standardizing its attribution guidelines and its assessment timeline, establishing an attribution analysis working group ... not standing but designated which should include key private sector analysis and data to accelerate the federal government's response ... and also advancing analytic capabilities by applying emerging technologies and diversifying data sources to overcome evolving technical challenges associated with attribution.

Rep. Mike Gallagher I think it's fair to say that one of the intellectual hurdles we tried to get over and thinking through layered cyber deterrence was the unique problems that attribution in cyberspace poses or anonymity. The unique strength that anonymity gives our adversaries, and it is going to require our ability to ... It's going to require us to improve our ability to do attribution quicker. I think the federal government's willingness to share certain intelligence and push that information to the private sector in order to equip them with the tools they need to push back in cyberspace.

Martijn Rasser: Great. Any further comments from the panel on that particular question? All right, we will move on to the next question from Michele Savini. "How do you think the COVID epidemic will impact on cybersecurity in the short term as network reliance increases, and in the long-term as social distancing changes habits and makes network dependent services more pervasive?"

Samantha Ravich: Yeah, I think even at the moment we're seeing kind of two trends right now, and it's obviously too early to see what's going to bear out. Although, I think one more than the other. One is that there are actually certain vectors that are attack vectors that have been decreasing in frequency over the last week. There's a lot of theories as to why one of them might be that some of the Chinese attackers are otherwise engaged in fighting their own coronavirus, or they are being put to other tasks inside of their own country as opposed to attacking ours. There's some indicators on that. I think that is a very short term if it is even a blip on the screen.

Samantha Ravich: The other trend is that as there are more people online combined with, in companies, there's more attention diverted from IT security systems and those protecting the crown jewels in companies. There's going to be a lot more attacks. I think that is probably much more likely that that's what's going to occur for the longer time.

Samantha Ravich: As you said, as we are conducting more and more commerce online, that we are relying on it at this moment more than we ever had. It goes to even the longer term trends on where do we want this data to flow? Again, I did speak out to our British friends and colleagues.

Samantha Ravich: Think about where we are now relying on information, our most important information for our countries' health and welfare flowing over the next generation in telecommunications technology. [Inaudible] an ally, a trusted vendor? Or from Huawei and China? I mean think about where we are and think about where this is going.

Samantha Ravich: It just really proves the point that we ... And hopefully they can still revert, change their decision on this because we will become even more vulnerable at this moment when we're relying on these key technologies.

Martijn Rasser: Great. Thank you. Would anyone ... Yes, go ahead, Chris Inglis.

Chris Inglis: I agree with all of that in the near to midterm. I would say that I'm somewhat a hopeful, bordering on kind of have some evidence to support the confidence that in the longer term, that the group of people, sometimes known as a chief information security officers, but increasingly CEOs, organization heads are actually thinking strategically about the lessons of the last two, three weeks as we've had to surge capacity.

Chris Inglis: We've had to rapidly build out infrastructure from what used to be corporately owned networks to the last tactical mile into homes and other nontraditional workplaces ... Is we've had to seek information from vaults that sometimes don't exist to replicate or to install a business in a place where it hasn't been before ... That they will now be more thoughtful about imagining the agility that they need, the confidence that they have to have in a system that could on a moment's notice have to be dramatically recast, reconstructed on the fly.

Chris Inglis: I think that those should be, will be the long-term lessons as we get through this that will apply not simply to the literal practical supply chains we talked about earlier in this conversation, but the underlayment, which is the runway on which that that runs. Which is the digital infrastructure around the world.

Martijn Rasser: What can we do as far as cybersecurity workforce development? What are some of the specific recommendations that the commission made on that front that would be applicable here?

Rep. Mike Gallagher I'll just quickly say, a lot of this involves in our opinion, how do we elevate and empower the position of CISA within the federal government. And give it the ability not only to do its job of protecting critical infrastructure, really being the private sector's preferred partner, but also make it as appealing as, let's say, NSA. And allow it to compete for talent with Google, with Facebook, and win. Because there are limits to our ability to compete on salary. Certainly when it comes to the amenities of the workplace.

Rep. Mike Gallagher But we can compete on mission. As we've seen with NSA, if we make the mission interesting enough, we can attract and retain the best and the brightest. I will say retention is probably what keeps a lot of Chris's old colleagues up at night more than anything else.

Rep. Mike Gallagher But by elevating the position of CISA within the federal government, we hope that that will have a beneficial effect on his ability to recruit the best people. For example, when we talk about continuity to the economy, well says it would be the primary government agency charged with planning a restart, restore and recovery operation for the economy if it's disrupted by a cyberattack or otherwise.

Rep. Mike Gallagher We recommend giving CISA the authority to do persistent threat hunting on all the .gov networks in a way that NSA could do the same on .mil networks. We recommend strengthening the organization. There's nothing more sexy than administrative improvements, but we shift the director of CISA to a five-year term and increase their pay. We push for new facilities, resources and authorities to elevate its stature in the federal government. And give it the tools it needs to bring the public and private sector together consistently for the cybersecurity mission.

Rep. Mike Gallagher: We think that that strengthened organization at the intersection of the private sector and public sector is really a cool place to work.

Samantha Ravich: Let me add also some of the things that we talked about in this category. What CISA, as Mike had said, can do for other parts of the U.S. government. We also looked at the National Lab Complex from the Department of Energy. Labs like Idaho National Lab that are doing tremendous work on securing the grid. What can that be pushed out to help secure other parts of the government and other parts of our economy.

Samantha Ravich: So, there is a great reserve and wealth of knowledge both inside the government and obviously spread throughout the private sector that can be used and called upon in kind of new and novel ways while recognizing that especially ... We really talked about this cyber reserve. So recognizing that some of the best work is in a cyber reserve unit, could do [Inaudible] they already positioned inside the private sector?

Samantha Ravich: Again, just a call out to the kind of conversation, and dialogue and debate that we had on the commission. We had talked about the cyber reserve. One of the commissioners, or one of the staffers had brought up the point, "Yes. But if there was a major cyber event, a cyberattack, do we really want to call up reserves that are currently working in our tech sphere or in our critical infrastructure? Because they're going to have to protect the homeland during that time."

Samantha Ravich: Being able to kind of play this out to where the best effect could be was really done so thoughtfully in the Commission's work over these many months. Our recommendations on that are after that thoughtful engagement.

Martijn Rasser: Go ahead, Chris Inglis.

Chris Inglis: On the matter of the pipeline, how do you actually develop the talent that the nation needs? The report goes into some detail it's in section 1.5 but it talks about cyber education. You can parse it into three bins. Every American for that matter, our allies as well, but every American citizen needs to know something more about cyber than they do today in their traditional education, K through 12.

Chris Inglis: To me, to invest something there so that the front line of the cyber world populated by people is better able to understand what their role is, and what threats and opportunities they face. Two, there are any number of disciplines, whether it's lawyers or engineers or even coders, they don't see themselves as being part of the formal cyber workforce. Because they have some other function that drives their daily work. But they make choices that ultimately create, or don't, resilience, robustness in that digital infrastructure.

Chris Inglis: So, we need to invest in those disciplines, those professional disciplines, some more training and education about cyber. Then of course are the folks who literally have cyber in their name. By any estimate that's at least 500,000 people short in the next two years. Might be as high as 2 million.

Chris Inglis: There's a number of people that they're short, and we need to increase the incentivization or simply the awareness of the merits of those career fields at the earliest possible moment, maybe even in kindergarten. So that the pipeline gets bigger. Then we can ultimately worry about how do we incentivize and retain those once they have arrived on scene.

Chris Inglis: The report speaks to all of those things and actually points to a number of initiatives that are already in place. One of those being the National Initiative for Cyber Education under the National Institute of Standards and Technology that do great work on one or more of the elements that I just described.

Martijn Rasser: Yeah, so the human capital component is absolutely critical of course, for addressing all these issues. Here's an open question to the panel from Jameson Cunningham. "What is an underlying assumption not being questioned? What is the 800-pound gorilla that we are not addressing?" Very interesting. A provocative question from Mr. Cunningham. Any thoughts on this from the panel?

Rep. Mike Gallagher So much of this relies upon Congress' ability to read our report in particular and then act accordingly. I know Ms. Cordero talked about how we're recommending the restructuring of the committee process. I would be lying to you if I told you I think that recommendation is going to be easy to effectuate. I actually think that's going to be one of the hardest things.

Rep. Mike Gallagher Because members of Congress are not really interested in giving up their jurisdiction. I will say, however, that perhaps the most energetic proponent of that position was the one on the Commission who has the most to lose. That's Jim Langevin, who is a subcommittee chair of a committee with jurisdiction on HASC over cyber issues and felt very strongly that subcommittee chairs like him need to be willing to cede certain authorities in order to support the creation of a cybersecurity committee.

Rep. Mike Gallagher Perhaps we didn't test the assumption of whether Congress would pay attention to this, but we did try and make it easy by wherever we're recommending a Congress do X, Y or Z, we have actually been, or continue to be in the process of formulating the legislative language so that we can allow members of Congress to cut and paste, if necessary, to get this put into law. That's the only thing I could think of.

Samantha Ravich: I might add, just really quickly and I don't know whether the "we" refers to the American people, the U.S. government or we as the [Inaudible]

Rep. Mike Gallagher It was the royal we, Samantha, that's just how I talk about myself.

Samantha Ravich: The royal we ... Is this notion of we have to think through an industrial policy, right? When we started bringing this up on the Commission, everyone kind of pushed back and leaned back in their chairs. Are we really thinking, talking about an industrial policy when we are all schooled in kind of free market economics? And we don't want to look like or replicate the Soviet Union, the central planning or the Chinese government. But we are playing on a different economic field right now. And the number two economy in the world is an aggressor.

Samantha Ravich: It is beyond time that we have to kind of rethink some of these tenants that are quite uncomfortable in terms of how the U.S. government and the private sector interact. Of course, as we dug down deeper, we all realize that the U.S. has had industrial policies in the past. This is not something we've never done. But it is, I would say, the 800 pound gorilla that we have to look at and kind of say things are different. Things are different when the number two economy is China and they're gunning for us.

Martijn Rasser: Yeah, it's interesting times when industrial policy is top of the agenda for a lot of people. Chris Inglis, I believe I saw you raise your hand. Do you have something you'd like to add?

Chris Inglis: Yeah, so I think another 800-pound gorilla in the room, it's probably been in the room for 40 years, is the notion that we can be scared straight without the collective event that we all feel happened to us. I think there are 315 million of us in a boat. We all see the hole in the boat, but it's not on our side of the boat. And therefore, somebody else needs to do something about that. The degree of self-enlightenment that that might naturally accrue simply by reading the report, that's a concern. People aren't intentionally chasing insecurity in their practices, and what they build and how they operate it.

Chris Inglis: They're chasing convenience. And so, we need a fundamental change in how people believe, or how people see their responsibilities and their personal accountability for that. And that's got to be shared at the individual level, the private sector organizational level, the government level. We need to collaborate across broadly all three of those constituencies. It's not clear that that's going to come about without some more perhaps cathartic, motivating events.

Martijn Rasser: Great. Thank you, Chris Inglis. Another question here from Aki Kahata. "Sometimes national security concerns are difficult to understand for the private sector. Basically, they prioritize economic issues rather than a national security issue. What do you think is an efficient way to share concerns on national security risk, especially the risk of the relationship between the Chinese Communist Party and Chinese private companies." This is a very interesting and important question. I extend that to include U.S. academic institutions as well. Because there's a lot of espionage concerns there as well of course.

Martijn Rasser: Samantha Ravich, I know you have to leave us a few minutes early for another meeting. Perhaps you'd like to start with this and then we can have the other panelists address it.

Samantha Ravich: Sure. I think that the U.S. government, especially the U.S. intelligence community, has kind of grown up and they live in the world that unless they can talk about collection methods, and specificity of the intelligence, that it's not really worth much. So, for many reasons there have been parts of U.S. government that have been loath to share as much information as they can with the private sector to truly underscore the threat in a more comprehensible, not wave tops, not 50,000 foot level, with the private sector and with individuals to get them to understand where the threat is.

Samantha Ravich: That really has to change. I do not think, and I think many of the commissioners did not think that the private sector themselves needs such specificity of how this information was collected at the most exquisite level. There has to be a way to push more information that is useful, that is relevant, that is timely out to the private sector and not have it just held within

the arms and the warm embrace of the [inaudible] intelligence agencies. Chris might have a ... I'm sure he can answer that or dispute it.

Chris Inglis: No, I do agree with that. I think that there is some degree of a sense that this information is so special I can't share it with you. We need to get past that. I think that the spirit is willing. We haven't quite figured out how to do that. And the report goes to that point of saying that the private sector needs to be a formalized customer for the intelligence garnered by the government. Both in terms of accepting requirements from the private sector and in provision of intelligence back to the private sector. That will/can make a difference.

Chris Inglis: I think also the government needs to put itself in a position where you can't simply argue about what perils ensue from the threats in cyberspace, but it needs to provide material assistance in creating resilience and robustness that doesn't simply blunt the swords or the activities of adversaries in this space, but actually increases the business bottom lines of companies that do business in dangerous places. Not least of which, cyberspace.

Chris Inglis: Companies will immediately appreciate if you join forces with them to improve business resilience, operational resilience. The kind of bottom line of capital markets being more accessible, having more confidence that they'll work in the ways that they should. Businesses will then say, "You're a partner with me, not simply for this arcane dark art known as cyber security, but in terms of extending and getting my business in the right place." The government cannot play favorites, and so therefore it needs to do that in an even, fair minded way. And we try to recommend some ways that the government can do that.

Carrie Cordero: Just to follow up on that as well, Martijn, two areas that the Commission report flags as areas that already exist in government but that can be strengthened to better balance some of these economic and national security issues are first the role of CFIUS, the Committee on Foreign Investment in the United States. That's a long-standing process that has existed that is really a very functional, and efficient and well-functioning ... I think most people who have been involved in the CFIUS process think it's ... It's an aspect of government review.

Carrie Cordero: And so, what that is for our participants is an inner agency review process to review mergers and acquisitions of companies that involve national security aspects. When the inner agency committee determines that the risks national security would outweigh, then there's a process through which that activity can either be altered or potentially doesn't go through. So, the Commission report does include some discussion of how potentially CIFIUS can play an enhanced role on some of the supply chain issues that we were talking about earlier.

Carrie Cordero: The other area that the report focuses on, in an area of government that can be strengthened and better resourced is NIST. Many in the cyber security community are very familiar with the NIST standards, which were started for government, but then were really adopted by much of the private sector as a baseline to establish good cybersecurity practices. I think the commission does an effective job in this report of explaining how NIST is a trusted source and a valuable source of expertise and knowledge. If it were given an enhanced role, could be even more productive in this space.

Martijn Rasser: Thank you, Carrie, great points. I think we have time for one final question. This one is from Carlos Aramayo. "Market forces incentivize software products that are fast, efficient, cheap and that offer scalability. It doesn't incentivize the creation of programs that have resilience or security in mind. How do you plan to shape the cyber realm and build resiliency if the markets do the opposite?"

Rep. Mike Gallagher Well, let me just say ... And this may be the last thing I'll say, because I'll have to leave in two minutes here. I think that's why you need a balance between ... As Chris alluded to before ... Pure market forces on the one hand and heavy handed and unduly onerous government regulations on the other. We attempted to strike that balance, for example, by requiring mandatory penetration testing for companies that are publicly traded. The goal there is not to require them to air all their dirty laundry and therefore tank their stock price.

Rep. Mike Gallagher But at least to have that information on file so that in the event of a massive breach we cold determine negligence or at least learn. That information could evolve into a set of norms. For example, you could see a near future in which 1/10/60 reporting becomes the new kind of norm in various industries. That's going to come with a cost for sure. But I just would say we're in the midst of a crisis right now, whereas I see it we were caught completely unaware from a testing and response perspective.

Rep. Mike Gallagher And where had we invested ten million dollars more proactively in testing domestically, we could have avoided ten trillion dollars in costs right now. Let us not say the same thing when a massive cyberattack happens a month from now, or a year from now, or three years from now. I'm not saying open the floodgates, spend all federal money on everything under the sun in cyberspace and force private companies to do the same.

Rep. Mike Gallagher But this is going to cost some money. Resilience costs money. But the question is whether it's worth the costs. I think all the commissioners would say yes. Yes, it is.

Martijn Rasser: Well, I think that's the perfect note to end this discussion on. Unfortunately, we're out of time. This has been a fascinating discussion. I want to thank our guests for attending and for your excellent questions. I'm sorry we didn't get to all of them. But we'll make sure that we continue this conversation. I want to thank Megan Lamberth and my CNAS colleagues for all their hard work to make this such a successful event. Thank you to the Solarium staff for initiating this panel discussion and for your support.

Martijn Rasser: Most importantly. Big thank you to our panelists, Representative Mike Gallagher, Samantha Ravich, Chris Inglis and Carrie Cordero. This is Martijn Rasser signing off. Be safe, be well. Until next time, thank you.