Resiliency Against Large-Scale Cyber Attacks:
Recommendations from the Cyber Solarium Commission

Featuring Rep. Mike Gallagher, Tom Fanning, Dr. Samantha Ravich, and Suzanne Spaulding. Moderated by Christopher Bing.

MAY: I'm FDDs founder and president, Cliff May, and many of you know this but I'll repeat it anyway. FDD is a nonpartisan institute, founded and focused on national security and foreign policy. FDD conducts actionable research prepared by experts and scholars from a variety of backgrounds and provides policy recommendations. We take no government, no foreign government, or foreign corporate funding whatsoever. We're pleased to co-host today's events with the Cyberspace Solarium Commission. As you also know, the Commission is a bicameral, bipartisan, and intergovernmental body developed to think strategically and to provide a plan for defending the United States against cyber-attacks of significant consequence. Today's events will focus on one component of the commission's mission, the resiliency of America's critical infrastructure. We're joined today by CSC co-chair, Representative Mike Gallagher, who he chairs the commission with Senator Angus King, as well as commissioners Tom fanning, Samantha Ravich, and Suzanne Spalding.

Our speakers will preview findings and recommendations from the Commission's forthcoming report and that'll be available on March 11th. I want to express my gratitude and my admiration, not for the first time, to my colleague Dr. Samantha Ravich. More than four years ago, she joined the advisory board of FDD's Center on Economic and Financial Power, and came to us with the idea of socializing – in the age of Bernie Sanders, I hesitate to use that word, sorry about that – the then new concepts – I should stick to my script – of cyber enabled economic warfare. She has pioneered this field for our institution, founding and leading FDDs Transformative Cyber Innovation Lab and our Center on Cyber and Technology Innovation. Her leadership within FDD and in her growing number of prominent affiliations is truly making an impact on critical areas of American national security.

Before we begin today's program, I want to note this event is one of many that FDD hosts throughout the year. For more information on all our work, our events, and our areas of focus. We encourage you to visit our website, www.fdd.org. I'll also note that today's event is on the record and its being live streamed as well as recorded. Do please silence your cell phones if you haven't yet. Finally, I encourage you to join in on the conversation and you can do so on Twitter. It's just @FDD. With that, I'm pleased to introduce Representative Mike Gallagher. Representative Gallagher has been a member of Congress since 2016, representing Wisconsin's eighth district. Among his many qualifications, he served in the U.S. Marine Corps as an active duty counter intelligence human intelligence officer. He was twice deployed to Iraq, and served on General Petraeus' central command assessment team in the Middle East so I and we thank him for his service.

I should note, and I note this proudly, Representative Gallagher is also a longtime friend of FDD, having joined FDDs National Security Network. He was a National Security Fellow in 2011, before his political career started. Members of this group are selected because they are promising they are their various ways. We know they're going to have futures in national

security in various ways and we are very proud to have Representative Gallagher, whom we recognized early on as an exceptional leader as part of this network and he's a part of the alumni network to this day. Please join me to welcome Representative Mike Gallagher.

GALLAGHER: Thank you Cliff. Is this working, am I good? It's great to be back at FDD. As Cliff mentioned, I am a proud alumnus of the national security fellows program. I was encouraged when earlier they said that there are members of that program that are now running for Congress, although I understand that there are two that are running against each other right now. You may have sort of gone a little bit overboard on encouraging people, but an incredible program. My legislative director, Chaz, who's here, is also an alumnus of the program. So FDD has really distinguished itself as a hub and a place where you really have invested in the next generation of national security leaders, and that's, that's critical. And in fact, I was struck throughout the Commission's work at, you know, cyber gets very technical very quickly. We talk about algorithms and you know, a bunch of nerdy stuff, but at the end of the day, all of our problems are human problems and our solutions will be human solutions getting the best and the brightest to work on these tough problems.

And that's why it's been an honor to co-chair the Cyberspace Solarium Commission, to work with such wonderful people like Dr. Samantha Ravich. You are blessed to have such a, not only a great national security leader, but an innovative thinker here at FDD, and she's been a great friend for a long time. And thank you Samantha for your leadership on this Commission. Also Tom Fanning really occupied a unique space on this commission as a representative from, from the private sector, as CEO of Southern company really injected an invaluable and unique perspective into the Commission's work, but also in an industry that has to work and partner with the federal government and has to navigate all of the complexities that come with that. And I can tell you, Tom has a very demanding day job, but he has been at almost every single Commission meeting. He takes an enormous amount of time out of his personal schedule to interact with a ton of officials here in D.C. that need his expertise and his advice and really just as a citizen, thank you for being willing to sacrifice on behalf of this country.

I see Suzanne Spaulding in the back, who's one of our Commissioners. Mark Montgomery, who's our executive director. I may have to leave for votes around 10 that's actually a real thing. It's not just ‘cause when the hard questions start coming in, I want to pass it off to someone else. But if you see me slide out the back, it's not because I'm afraid or angry at anything anyone said. It's cause I occasionally in Congress you have to vote on things. So I want to give you a preview before we get into the discussion which be far more interesting of what we might have to vote on should the work of this Commission sparked some interest among my colleagues. Obviously we are facing an immense challenge in cyberspace. The Commission is inspired by a time of strategic uncertainty in the late forties and early fifties when a lot of smart men and women had to step back and think what is the right strategy for the United States vis-a-vis the Soviet Union.

And in many ways built the national security apparatus that we still operate under today. And in the last decade we've seen Chinese cyber operators steal hundreds of billion dollars of intellectual property, accelerating China's military rise, undermining our military dominance. We've seen Russian operators and their proxy’s damage public trust in the integrity of our

elections and our democratic institutions. China, Russia, Iran, North Korea have probed our critical infrastructure with impunity. And so, look back to the early days of the cold war, I would argue we faced a similarly exigent strategic challenge where the risk threatened to rapidly outpace the country's ability to respond and counter it. And in response to the nuclear threat from the Soviet Union, President Dwight Eisenhower developed the nation's first continuity of operations and continuity of government planning processes to ensure that the government would continue to function in the aftermath of nuclear war. These measures included the construction of facilities to protect the government from nuclear attacks like Mount Weather in Virginia and the Raven rock mountain complex near Camp David in Maryland.
The goal was to send a message to our adversaries. Whatever you throw at us, the U.S. will maintain its strength and its ability to respond, and if necessary, retaliate. To borrow the immortal words of Green Bay legend Vince Lombardi. Perfection is not attainable. However, in other words, we must be prepared for that situation in which we fail. Eisenhower understood this in the strategic context and we have incorporated his wisdom and the wisdom of Lombardi into our work. Resilience, which we're going to talk about today, which we define in our strategy as, "The capacity to withstand and quickly recover from attacks that could cause harm or coerce, deter, restraint, or otherwise shape U.S. behavior is the key to denying adversaries the benefits of their operations." We have to become a harder target. As United States has become more technologically advanced, the systems and assets, our critical infrastructure that support elements of our national power such as a strong military, a strong economy, have come under increased risk of cyber-attack, placing their continued function in jeopardy.

Therefore, in an American strategy to build resilience must take a risk based approach. The U.S. government must be able to regularly identify and secure the systems, assets and private entities that are most critical to U.S. national power. This means securing what we call systemically important critical infrastructure or infrastructure whose disruption can have cascading widespread impact across the nation. This is going to require consistent engagement across all sectors and greater capacity in government and the private sector to identify and reduce evolving risks in cyberspace. Under the leadership of the cybersecurity and infrastructure security agency, the U.S. government has made great strides at understanding this national risk, but we must continue to evolve. We in Congress must make sure the government maintains rigorous, codified and routinely exercise processes for identifying, assessing, and prioritizing risk, and then translating that into strategies, budgets, and resilience programs.

Furthermore, while the United States has developed and tested mechanisms and processes to respond to physical and natural disasters, the same rigor has not yet been applied to understanding and responding to cyber disasters, and continuity planning has missed a crucial pillar of U.S. national power - the economy. We in Congress must make sure that the largest and strongest economy in the world can continue to function in a crisis and withstand any attempt to disrupt or undermine it. Additional gaps in resources funding and authorities hamper the U.S. government's ability to respond and recover. The U.S. government must ensure it has the speed to quickly mobilize response regardless of the size of a cyber-attack. And we in Congress must equip the executive branch to be a more mature partner in cyber response and recovery resourcing and enabling them to play an additive role not only in times of emergency but also in times of distress.

To go back to Vince Lombardi, and I once wrote a memo to my staff that without Vince Lombardi, America would not exist. The idea if you go to Lambeau field, the clock is 15 minutes fast, Lombardi time. If you're on time, you're 15 minutes late. The reason our government exists as it does is because James Madison got to the constitutional convention before everyone else did and was able to shape the battlespace. Vince Lombardi has enduring wisdom for all of you. But while he said that perfection is not attainable, whether in football or cyber defense, the broader quote was, "If we chase perfection, we can catch excellence." That is what we have tried to do on the Cyberspace Solarium Commission. That is what we are here today to discuss. I want to thank my fellow commissioners for your work. I want to thank Dr. Ravich, Tom Fanning, and Suzanne Spaulding for being here. Thank you FDD for hosting us, this and I very much look forward to the discussion. Go Packers.

BING: My name is Christopher Bing. I'm a cybersecurity reporter with *Reuters* news in Washington, D.C. where I cover nation state hacking. We have a great panel today. I'm really excited for this conversation. We already heard some bios, but I'm just going to run through them from left to right real quickly before we get started. To my right is Suzanne Spalding. She's a senior advisor for Homeland Security at the CSIS international security program. She previously served as under-secretary for the national protection and programs directorate at the Department of Homeland Security. To her right is Mr. Tom Fanning, chairman and CEO of Southern Company, a leading American energy company. He's co-chair of the Electricity Sub-Sector Coordinating Council, which serves as the principal liaison in between the federal government and the electric power industry. Next is a Dr. Samantha Ravich, the chairwoman of FDD's Center on Cyber Technology Innovation. She also serves as Vice Chair of the President's Intelligence Advisory Board and on the Secretary of Energy's Advisory Board, and our opening speaker representative Mike Gallagher, who's co-chair of the Cyberspace Solarium Commission and currently serves on the House Armed Service Committee and Transportation Infrastructure Committee. To get started, I like to bring representative Gallagher back into the conversation. While historically the concept of nuclear deterrent is well understood. What does deterrence look like in cyberspace to you? This is a key point of the report. So what are the differences and why is deterrence in this domain particularly important?

GALLAGHER: Well, I think while we, we start from this question of is deterrence possible in cyberspace? I emphatically answer though it is difficult. It is possible, because we're not attempting to deter cyber, some sort of amorphous thing or domain or capability. We are still attempting to deter human beings, right? Occasionally those are Nation-states, which theoretically are easier to deter in some cases, occasionally those are cyber criminals, which may be more difficult, but in contrast, a nuclear deterrence which has a very small margin for error, right? In other words, you, you don't want deterrence to break down and the whole point is to avoid war. We entered this discussion from a recognition that in some sense right now deterrence in cyber is constantly failing. And in order to restore some semblance of deterrence and it won't be perfect deterrence, we need to at least have three layers of deterrence.

One, we need to capitalize on a lot of changes in authorities and changes in strategies that we've made in the last three years whereby we've adopted a forward posture in cyberspace, the DOD cyber strategy in 2018 called for defend forward. I would argue to you that that is having some success and if we can build on the defend forward concept, become a better ally around the

world, working with like-minded partners, we can perhaps spread that concept across the entire federal government and over time build norms of respectable behavior in cyberspace. Secondly, we have to be prepared to impose costs. I think it's fair to say that below the threshold of military force, there is some ambiguity about whether the United States government will respond. If you, for example, mess in our elections or hack our critical infrastructure. It is my belief and the commission's belief that we need to have a clearer signaling strategy that says, below the level of force we are prepared to strike back quickly with speed and agility while still retaining flexibility in terms of the precise nature of our response.

And then finally in the third layer we need to become a harder target. As I alluded to, I would nest this within the concept, not of strategic deterrence by punishment, but conventional deterrence by denial, right? In other words, in the same way the national defense strategy right now is calling for us to shift from deterrence by punishment to deterrence by denial. For example, an endo pay comm. The same is true in cyber. How do we ensure that we are harder to attack and that even if our adversaries are able to get past our defenses, we can be back up online with speed and agility? So that's three layers layered, cyber deterrence and I think the Commission report, which will come out next Wednesday, mark your calendar will build in how, while cyber deterrence is not perfectly analogous to nuclear deterrence, we have learned some lessons from nuclear deterrence, but we were also trying to make this concept relevant for 2020.

FANNING: If I could just add to this notion of nuclear deterrent, you don't want somebody to push the button, right? You want to do everything you can not to get there. In the cyber realm, corporations in America are getting attacked, each major company, millions of times a day. And when we go to machine to machine capabilities, it could be trillions of times a day. The waves of cyber-attacks are hitting the beach all the time. And so this notion of deterrence is an idea that helps shape behavior, impose costs, remove the benefit of this constant drumbeat of attacks. So that's, you know, from our standpoint, 87% of the critical infrastructure is being hit all the time. And so that's what we have to do and work within. It's a really different concept. I think the nuclear deterrent

SPAULDING: And implicit in that is the idea that with an unclear deterrence, you either have to turn it or you haven't, I mean, it's a pretty binary choice. With cyber, you're deterring, you're trying to reduce the level of malicious cyber activity. This is not going to be as both Tom and Mike have said, this is not going to be a – we're going to eliminate cyber. This is all about mitigating the consequences and mitigate and reducing the level of activity.

FANNING: And reducing the reward of the activity is a big deal.

BING: Representative Gallagher started to touch on these different levers of national power that the federal government has to deter adversaries. But for Suzanne and Samantha, what are some of the preemptive steps that can be taken to reduce and identify risk ahead of time?

SPAULDING: Yeah, so we spent a lot of time in the report emphasizing this risk management approach and in fact if you look at the six pillars under which we group our recommendations, we've got a lot of recommendations, but we really tried to bucket them under these six pillars. They match pretty, pretty nicely up against the traditional way you think about

risk assessment and risk management. That is, there are a couple of pillars that go to threat that's around the norms and preserving instruments of military power and, and figuring out how to use those in a deterrent effective way. There's working on improving the cyber ecosystem, which is really, if you think about it, it's really about removing or reducing vulnerabilities both in the technology and the people and processes. And then this one, which is on resilience, which again goes to really focusing on consequences. And so as you're – and part of that is starting with assessing your risk, right?

And so looking at it as a factor of threat, vulnerability and consequence. And what we emphasize in the report is how important the consequence piece is. In our cybersecurity discussions, typically we tend to focus a lot on threat actors and we focus a lot on vulnerabilities and reducing vulnerabilities and not nearly enough understanding the consequences which help you both prioritize is what you really care about is the function that's enabled by this networked world and by these computers and assets and systems and networks that you're worried about. It's really the function. So what you care about is the consequence if that is disrupted in some way, if the confidentiality, integrity or access cannot be guaranteed or protected. And then it helps you with managing risk because you could look at not just deterring threat actors and reducing vulnerabilities, but how do we reduce the consequences? And one of the things we talk about in the report is that that may not be a high tech solution, right? That may be in what we call an analog solution. Think paper ballots as a way of addressing and vulnerabilities within our election infrastructure, for example.

FANNING: Or the electric system in the 1950s

RAVICH: So one of, one of the most impressive parts about the, the Commission's work, which you'll see when the full rollout happens next Wednesday, is we really met the charge that was given to us, which is not just to think about the strategic future and how we were going to deal with the strategy to protect the country in this new battle space, but actually recommendations to make it so, right. I mean it is very, the, recommendations on all the different parts of layered deterrents that we've touched upon come with real recommendations, the steps we need to take. And one of them, as we were talking and Suzanne was mentioning, understanding the threats you can mitigate it, relies on data, right? How are we going to get the data we're going at, we go into very specific steps on how are we going to get the data? Working with the private sector.

Because again, and it, we really were so, so appreciative that that Tom was part of this commission and you know, came to, we had 28 meetings, 28 meetings since last summer. Two hours, most Mondays, right. Four members of Congress came too as well, most of the co-chairs came to every single one of these meetings. Tom flew up from Atlanta to come to every, almost every single one of these meetings. Suzanne and I and the other commissioners, I mean this was serious work we took on and we debated these issues carefully and we recognize that we can't just hand wave and talk in, you know, big picture. We must have a strategy, but how are you going to actually do that? So these recommendations are very specific in a number of a number of instances. But on the, on the data, you know, again, as Tom was mentioning, so much of, of what we need to know resides in the private sector. And until this point in time, you know, there's been a disconnect between the what the government, how they think about the threat and

how they prioritize what needs to be done about it and how the private sector is battling its way in this battle space with frankly, not all the tools it needs to be able to protect itself and the citizenry. So there are, you will see very specific ways we walk forward into this.

FANNING: Yes, let me just hit this real quick cause you're hitting on some very important points. It's not just how the private sector interacts with federal government, how federal government can work better within itself. It's how we realized very quickly. I've been leading the electricity sector in the cyber realm now for about six years. Very quickly we learned that living within the silo doesn't work. We are truly interdependent with other industrial sectors across America. And so one of the things we've done I guess starting about three years ago and now we're really getting there now as former tri-sector group which puts together finance, telecom and electricity, having a joined threat matrix where we understand likelihood by magnitude of problem of cyber threats. And really starting to think about things we can do together from an analytic standpoint and whatever. 'Cause you know, it isn't just about be fired upon and fire back, some of the most important work we can do is understand the nature of the battlefield. And the more we can illuminate situational awareness among and between the federal government and private industry and Oh, let's not forget about state and local governments. That is such a key, because when we get into the notion of resilience, there will have to be boots on the ground. They're going to have to deal with the aftermath. So all this has to be integrated and it's an enormous issue.

BING: In a new relationship paradigm between the federal government and the private sector on cybersecurity. People who've been following this space for some time know that there's been arguments for a centralized cyber agency of some kind in the federal government. But I understand the report has a different type of approach. So I wanted to ask you about sector specific agencies and what role they would play.

SPAULDING: Yeah, so we've reached a point, if there was ever a time that we could have pulled all of cyber would have made, might've made sense to pull all of cyber into one department or agency we are long past that. I'm not sure it ever existed, but it certainly isn't the case today because it again, like it permeates every aspect of our lives, it permeates all throughout the government and it requires just as going back to the risk management approach and the focus on consequences as to both prioritize and then mitigate, you really need deep sector expertise to be able to do that. You're a – I always say, you know my cyber ninjas at DHS, they were fabulous, incredibly smart, really hardworking, committed people, but your IT specialist can no more tell you about the impact on your business if you're from a, from a significant cyber incident, then the electrician can tell you about the impact on your business if the power goes out for an extended period of time, right?

You need those, that sector specific expertise. Most of it resides in the private sector and, and I can't emphasize strongly enough how, what a delight it was to work with Tom Fanning for those years that I was at DHS, somebody who really understood it and why the Electricity Sector Coordinating Council is one of, if not the best private sector coordinating council in this. But it also means that the departments and agencies like the Department of Energy, the Department of Treasury for financial services have to be key players in that as national risk management experts, as sector risk management experts because they, they have, and one of the advantages

that DHS and CISA, previously NPBD had is that we had all hazards approach both physical and cyber with the mission of strengthening the security and resilience of our nation's critical infrastructure. Our sector specific agencies need to similarly take that holistic approach.

RAVICH: But we know that not all of the sector specific agencies are as robust and good as they should be. Right? I mean clearly the ones that Tom works with, you know, are amongst the best. But when we look at let's say water versus power, there are great disparities in terms of how, for instance, the EPA, you know, is able to deal with its sector specific agency to deal with water. I mean the utilities, the water utilities, there are about 3,000 electric utilities across the country. There are 70,000 water utilities. In California there are 3,000 alone. And, and while you might be able to exist for a couple of days in the dark, you can't exist for a couple of days without water. Right? So when we look at getting the sector specific agencies up to snuff, there are some that have not had the attention that they need, potentially resources, but certainly, you know, no pun intended, getting a fire lit under them, to do what they need to do.

GALLAGHER: Can I just add really quickly, I agree with what Suzanne said, though we did debate a variety of different structures. You know, do we need a cyber-specific agency? Do we need this? That while a lot of our specific recommendations remain embargoed, I think you, I think I'm allowed to say this while I'm a coach here, so I'm just going to say it.

If you're an FDD fellow and you want, you know, if you want to be more reckless, just get elected to Congress. The overall approach we ended up taking was to figure out how do we elevate and empower existing agencies, develop sort of clear left and right lateral limits for agencies. And sector risk management agencies, but also have an environment where people want to play nicely in the sandbox. So I think you will see a lot of recommendations that are, geared towards giving the very dedicated professionals at, you know, NSA or CISA or take your pick the tools they need in order to be a proactive, responsible partner with the private sector.

FANNING: You know, and in thinking about that, we can't boil the ocean. So we have to start with a very clear notion as to where the priorities are for national resilience. That's a very hard but important first step. And so therefore, if we understand where those assets reside within the United States, the private sector can work with government to help develop strategies. Now, we got into a lot of discussion about words like “sharing” and words like “cooperate”. My view is, we must collaborate. We must share the obligation. Now if you think about it, private industry and government in the United States had lots of law and regulation and precedent that really doesn't support that. We're very separate as apart from say, China. What we have to do is figure out for the good of national security where we should start to make a much greater collaboration between the private sector and government, whether it's the intelligence community, whether it is in any sector specific agency.

I love working with Suzanne and our model back then was to say under Homeland Security, private industry prepares for and ultimately responds to the hold accountable piece I think is central to what solarium was all about. You know, when we think about is Mike, Mike's a great historian. When we think about the 1953 solarium and you know, there's model of here's the Soviet Union, here's Western Europe and here's this tank battle on the plains of Poland, not a nuclear war. The nature of the battlefield is on the telecom networks and the electric grid, and

our financial systems. We know them better than the government does. And so therefore we must join in this effort and bringing the department of defense and cyber command and the FBI and Secret Service and whoever else needs to play to hold the bad guys accountable is some of the most important work the solarium commission has produced.

BING: Much of cyber policy making today involves planning for possible scenarios that may not have occurred before, and yet just over the last several years, we've seen truly the destructive force of massive cyber-attacks such as Wannacry and Notpetya. I know the commission report deals with this issue of a catastrophic cyber-attack and how the U.S. government would deal with that and plan ahead of time. For Dr. Ravich, what can be done to ensure the continuity of the economy and this type of catastrophic cyber incidents?

RAVICH: Yeah, so this is an area that the Commission really focused upon. Let me just back up, my work here at FDD, since 2014 has really focused on cyber enabled economic warfare. The use by adversaries using cyber means to undermine key components of our economy in order to weaken us strategically and militarily. Because we are the number one military in the world, and because we're the number one economy in the world. And by undermining our economy and you can undermine our military strength. So imagine a cataclysmic cyber-attack during a time of overseas crisis. Right? How would you rally troops, you know, if you can't even get them on the planes, the buses, the trains. If you know, the Walmart shelves were depleted and soldiers had to leave their loved ones at home without baby food or, medicine. Now you can imagine the toll that would take on our military.

So, you know, in the past it was worth writing about the strategic aspects of this, but it took the Cyber Solarium Commission and the hard work of all the commissioners to say, all right, well how do we actually not think the unthinkable, but plan the unplannable. Right? And that's what continuity of the economy is about. Yes, it does kind of leverage the understanding of coop/cog, continuity of operations, continuity of government, but continuity of the economy really focuses on a number of aspects. One is if there was a major cataclysmic cyberattack, what is the most important seed data that has to be protected from critically important, strategically, systematically important critical infrastructure so that they hold it offline in a secure place, maybe here, maybe overseas at a friends or friend or allied nation so that we could reconstitute the workings of major economic components.

Another aspect, think about, you know, the blinking interconnected, woven network of our economy, right? You know, you, you can't have the banks function without the electricity grid. You know, part of the electricity grid runs off of oil and gas and coal. Okay, so all of these things are connected. What are the key nodes and where are they? So that in the immediate aftermath of an attack, you could flow resources, but that has to be planned before you can't do that when the lights go out. Right? So the planning of it, the thinking, the prioritization, and, and let me be clear, not everything is going to be prioritized, right? So making those hard decisions beforehand and being more – exercise it where the Defense Production Act needs to come into play and letting the American people know that frankly, not every place is going to be prioritized. So there has to be resilience in the American people as well. But this is kind of the bread and butter of continuity of, of the economy. And, and it is both a major piece of resilience in and of itself, right? So that we can reconstitute an attack by an adversary won't take us down,

but the adversary needs to know very clearly that if they try the next day, they will feel our wrath, right? They need to know that that is deterrence.

SPAULDING: So Samantha made a number of important points. But one of the things I want to emphasize that is I think the Commission was particularly I would say brave, courageous about, is this notion – and Tom drove a lot of this of systemically important critical infrastructure because it has, I bear the scars from my time at DHS. We love all of our children. There are 16 critical infrastructure sectors. They are all important and they are all important when we talk about that cyber ecosystem. I mean we all, and we all know, you know, Home Depot was hit through its HVAC vendor, which you wouldn't, nobody would probably put that on necessarily on their list of systemically important critical infrastructure. Nevertheless, this effort to identify national critical functions that DHS has been undertaking for the last few years that focuses less on a specific sector or entity but looks at cross interdependencies and cross sector reliance for what are the key functions that the American public relies upon has helped us get to this notion that, you know, you know, there are some that from a national perspective are more, are more vital. And where we need to focus resources and efforts. It doesn't mean that we are ignoring the rest, but, but surprisingly just even saying that that there are that some are going to be prioritized in our efforts here. We'll get some pushback on that, but I think it's an important step forward and it, and it helps you move then along on a number of things including some discussions about a more robust intelligence sharing, for example.

GALLAGHER: One of the bigger recommendations to come out of the report and my hope is it will generate a discussion among all the smart people in this room about, okay, how do you actually plan for the continuity of the economy? Incidentally, I have my staff ask the Congressional Research Service this week. What happens if we cannot physically go to D.C. because there's, you know, a coronavirus outbreak for example, and you might need to pass some appropriations. I haven't gotten an answer on that yet, but anything I can do to avoid going through O'Hare would be fantastic.

FANNING: But you know, in my industry, this is stuff we do all the time when there's a hurricane or something. How we think about restoring electricity depends upon a very clear sense of priority among our customer base: hospitals, things like that. So we have a model that we started with but boy a boy, the work that I think Chris Krebs has done at CISA and some other things. Taking that down when we evaluate systemically important assets in the United States and the layers of resilience we have to have, whether it's electricity or telecom or water or whatever it is, this is some of the most important work in front of us and will make us better as a nation.

BING: Short of a true cyber war. The type of instinct catastrophic gets into that. We're talking about there's a gap between routine technical assistance that the government provides. There's a lot of space between that. In terms of the reports, recommendations, what are some of the initiatives or programs that can fill in that space right now and improve that type of assistance?

GALLAGHER: And I, I want Mark or someone to start doing this vigorously if I'm getting into embargo territory here, so you can imagine the Stafford Act sort of governs and calf

and distress and all that stuff. Okay. There is, you could imagine it's theoretically possible if there were a no kidding, catastrophic cyber-attack where there was physical disruption, potentially death. You could imagine a president invoking the emergency authorities that he already has, right? In order to unlock a lot of funding and things like that. However, there's a lot going on right now in between that and nothing for which you might need a in between authority to unlock additional funding. And so, we have at least two if not more recommendations that tries to get at that gap that we've identified right now. For example, giving the executive branch the authority to, okay, I'm going to say this last chance, ah, okay. To declare a cyber-state of distress, which would then unlock access to cyber response and recovery fund. So you could imagine if an election where no kidding hacked and a state election authority needed access to the National Guard or something else for which there's no clear a suggestion right now that it would be reimbursed. And in fact that's blocked cooperation in many instances, this new mechanism creating a cyber-state of distress, unlocking access to a cyber-response and recovery fund would allow States local, tribal and territorial governments access to enhance federal expertise and resources that they currently don't have right now. So that's one way we try and get at that.

RAVICH: And you know, it's an important point because again, unlike the nuclear, it's not binary, right? It's not mushroom cloud, no mushroom cloud. The Pentagon has written a lot about persistent engagement. And we talked a lot about persistent engagement. We are in a cyber-war. It is constant. You know Tom talked about and Suzanne talked about the, you know, how much we are in this war. So it is not just waiting for, you know, the event, the event is happening, it's, it's upon us. And you know what, we really worked hard as, as a Commission really, and again, I have to call out, you know, the, the fearless leadership of, of, of Congressman Gallagher and Senator King is our co-chair and the amazing staff, no one who came into that room would be able to tell who are the Republicans, who are the Democrats. There was heated discussion, but it was about substance and content. So it was, it was such an honor.

FANNING: So let me just add, it wasn't bipartisan either. In my view, this thing was nonpartisan and I actually get that sense walking around the Hill and Congress – I was up there yesterday fooling around.

GALLAGHER: Me too.

FANNING: This is an issue. It's a really tough issue we were describing before we came out here. I was on Maria Bartiromo's show at one time trying to describe it with her. And it's like, I invite you all to join me to go watch the cyber war. Let's go out on the beach. And it's as if we're watching a battle of submarines. All we see is the ocean and nothing happening. Very often that's what's going on in cyberspace. It's happening all the time. It is on us and it is lethal. And so we only see something when something cataclysmic happens. This joining of effort is critical in order to forestall the worst of circumstances. And you know this, there is an element of national kind of cyber hygiene to the public. Remember Smokey the Bear and remember don't be a litter bug and all that? There's more we can do as a government to create cyber hygiene among the populace. But here again, at least where I start and what I think we're talking about here, and this is not about punk thugs and criminals, even though those are always important to somebody, we're really talking about the existential threat. Someone interfering with the American way of

life. And I think there's a lot we can do coming out of this report to stop that bad day from happening

RAVICH: And this report was not written in a, in a bubble either in terms of just the commissioners and, and when I say just the commissioners four sitting members of Congress, six outsiders of whom we were three, four sitting members of the executive branch. An amazing staff, dozens and dozens of meetings on the outside with private sector entities, other governments, allied nations to kind of stress test some of the recommendations that we're putting forward. You know, what the, what's the pushback going be? Now we heard pushback on some of them and some of them we were able to then, you know, take that into consideration and, and be able to craft the recommendation in, in perhaps a slightly different way. But some of them, we heard the pushback and frankly we said, you know what, it's time to kind of belly up to the bar. Like, you know, we, we've got to do things that might not be easy and, and some might not like it, but it has to be done anyway.

GALLAGHER: Yeah. I think, sorry to jump in. Though, you know, I mean not everyone on this stage agrees on everything. Certainly the Commission didn't agree on everything. Everyone was willing to make compromises because we were united by recognition that the status quo is not getting the job done and to, to come on Tom's point. I, I do think, and I've only been in Congress three years, so what do I know? But there is a genuine sense among members on the left and the right that we need to figure this thing out. I think there's a genuine, you know, it's interesting. I would actually say regardless of who wins the election in 2020, the new consensus position on foreign policy is a hawkish position on China, which is remarkable to me if you think about it. In other words, I always tell a story that I think it illustrates it. In the wake of the NBA scandal, when Daryl Morey got slapped by the NBA commissioner for tweeting and support of Hong Kong, we sent a letter to the NBA commissioner and the cosigners of that letter were Tom Cotton, Ted Cruz, friends of FDD. On the one hand. And AOC on the other hand, right? Like show me another issue in American politics that unites that wide range of. I think there's a lot of genuine bipartisan energy around how do we shore up our defenses in cyberspace and make sure that the Chinese communist party doesn't outpace us. Russia doesn't outpace us, et cetera, et cetera. Now, there isn't a lot of deep expertise. I mean I don't, it's hard. You can't have any.

FANNING: I'm the only a CEO in my industry. I think that was a CIO in my career. You know what that means, chief information officer most days I thought that meant career is over. I'm telling ya, this notion of depth is a real issue and so with the, with the, you know, the, the riches that we have up here on the commission and everywhere else, boy, I think we've got something we can work with now as opposed to dumb books that go out by people that attended a conference.

BING: I think that's a good optimistic point to end it on. I'd like to, we have about 30 minutes right here. I'd like to open it up to the audience for questions. We should have some microphones going around or if not, yeah, right over here. Yes sir. Right here in the red tie. Yes.

O'CONNOR: Good morning. My name is John O'Connor. I'm with James Whitney. Like many of you ate longstanding labor in the trenches. A couple of quick questions on a lightning round if you will. Do you acknowledge that we're not only in a state of conflict but we're losing,

point one. Point 2 is will your, will your recommendations extend to clarifying Tom your words of obligation and cooperation to a point of requirement on the part of critical infrastructure companies to provide, maintain and allow continuous and immediate access by authorized government entities in their network to be able to instantaneously mitigate and retaliate if possible. That's question number two. And question number three is would you support an amendment to Sarbanes Oxley? And I say this as a member of a public company audit committee to put the same requirements on me with respect to cyber as I wear for financial integrity today. So are we losing, are you going to finally confront the hard question in the room is will you allow at the Southern companies continuous and widespread access by government entities on an on a line speed basis and are you going to bring the board into the picture?

GALLAGHER: I'll try it first and then I'll pull out the hard ones to you guys. With the caveat that unless conflict is a term of art and while there is a debate about the threshold use of military force when you're in conflict or not, we are very blunt in the report about the fact that we are, I mean it's so Wild West right now. It's game on, right? If we're, yeah. The whole reason for the Commission is that the status quo though we've made significant improvements and Nakasone has done some great work and all this. The status quo is leading, I think we describe it to a slow surrender of us power and responsibility, or that's how the chairman describe it in our, in our very colorful chairman's letter.

FANNING: But wouldn't you say, Mike, I want to parse your question and weave it in in one respect. It's not capability. It's choice to act. Our capability is fabulous. Okay, so then it becomes a matter of policy. What do we think about Defend Forward and Persistent Engagement? Well, you know, whether we're winning or losing our capability is fabulous. All right. Let me leave that one there.

GALLAGHER: You could say we live in the glassiest house is probably –

FANNING: Maybe, maybe, maybe the other one that this obligation, okay. I hate to do this but we can't say right now. There are specific recommendations about that. I want you to tell you my opinion and I'm not going to go to the heart of your question, but rather the principle and that is as a matter of national security, critical infrastructure providers have a special obligation to the government, to the nation.

RAVICH: So I think it's fair to say and looking at that relationship, we, I think – I think it's fair to say we place a lot of faith in and reliance on the market. Our preference is for effective market solutions to drive improvements in cybersecurity. And so you start with that premise and you look at what is preventing the market. The market is not working today to do that. Why is that? What are some of the reasons? And so one of the things we looked at are things like cyber insurance, right? Which can help make a more effective marketplace. So you'll see some things in there around those issues. You know, other access to information can help make markets more efficient in driving appropriate behavior. But we recognize that in some instances the market is just not going to get there either because you've got already regulated monopolies for example, or because in many instances you've got externalities that are harms to the public that you, that it's not reasonable to ask a business to. There will never be that business case. Right? And so in those instances we looked at both carrots and sticks

FANNING: Benefits and burdens, right?

RAVICH: So, so again, we can't go into specific recommendations that, that a lie at the heart of your question, but I give you just a little bit of color on the conversations and the debates that we had in, in the Commission that led to some of the recommendations you'll see next Wednesday. And as Suzanne was saying, you know, it was, there are market forces that need to be aligned, you know, better to allow the companies themselves to do what's needed or be told to do what's needed. But also, you know, for the consumer, right? I mean, you know, the, some of the conversations and some of these meetings where, how, how do, how would I, and I'm in this field, how would I possibly know whether this device is safer than that device? Right? How can I possibly vote with my pocket book to be more cyber secure or my mom or you know, or my cousin or, and the, the consumer themselves can play a real role in this if they knew what they were voting for or buying. Right? So, so getting, so there was a lot of conversation about that. How do we get broader market forces aligned to make this country more safe and secure? But as Suzanne said, then recognizing there are gaps between even in the best case the market getting to where we need and where government potentially has to step in to align those more purposefully.

MAKRIDIS: Thank you so much. So my name is Christos. Coming from an economics background, one of the, I think this is kind of like a framing question. One of the additional very large benefits I think of the suggestions that you're making are that because critical infrastructure typically requires such large investments and investments tend to be lumpy. People don't like to make them at a continuous nature and in public infrastructure, energy, roads, everything. There has not been overhaul for a long time. And so I wonder if you can also frame this opportunity to move forward on the cyber side as an opportunity to really push ahead on some of the fundamental infrastructure challenges, country faces with roads, energy, I mean all sorts of infrastructure, including even 5G.

FANNING: I think you're spot on. Look, we've been, we've been arguing, at least in our sector, that resilient as apart from reliability. Our industry is built on engineering, economics and reliability. What is the cost of an adage? And therefore we build up to the point where you get the biggest bang for the buck. Resilient in reliability is how your system operates under a normal day. Sometimes the generating plants don't run sometimes and transmission lines don't work, but otherwise we'll build to that standard. Resilience is the notion of how your system operates under abnormal conditions and what is the cost of that? And we had been arguing, if you want to go look and Georgia Power, we do an integrated resource plan and do them all over the United States. For the first time, we argued about resilience within the context of that plan. So, I think there's absolutely that argument to make and it's a darn good argument. And then when we think about kind of the national infrastructure, we should include cybersecurity as part of that piece of the pie.

GALLAGHER: I would say one of the challenges in the report though, frankly, was, I mean, as you guys know, cyber can quickly become everything, right? Yeah. We're in a hundred pages about 5G and Huawei and ZTE and everything. And while we have 5G analysis and certain recommendations that get at it, you know, we had to be very diligent in terms of not allowing this report to expand. But, Tom is absolutely right. I'd finally, I'd say before I sneak out,

is I'm sure when this comes out, there's going to be people that say, no way we could do all these recommendations. Then there's going to be other people that say, you didn't go far enough. Maybe we got to just write. Maybe that's evidence. But I would say that we started from the premise of, I say this as someone who spent three months at the Eisenhower library, a good deal of my late twenties early thirties studying the original project, Solarium. We started from the premise that you can't recreate that magic, right? That that was unique to Eisenhower, unique to the moment our commission had a different makeup and different strengths as a result, right? This combination of House, Senate, executive, legislative branch, outside experts, private sector is really a unique forum that at least in my experience was the military and in Congress and the intelligence community, I've never experienced before. And so we hope that we've produced a document that will at the very least, generate a ton of debate and discussion and so we really hope you'll read it and I'd be just will finally say that's the biggest thing people get wrong about the original project, Solarium. It's there's this mythology that's built up saying, in July of 1953 you know, they emerged from that room with the new look fully formed, not the case, right? We continued to debate key aspects of containment until the Soviet Union collapsed, so for decades, and so we recognize that this is not the end of a process but the beginning of a broader process. And so with that I'm just going to sneak out and thank you for allowing me to be here.

FANNING: One other metaphor, just picking up on that concept, I always use the metaphor of the old sixties lava lamp.

RAVICH: I don't know where this is going.

FANNING: But that's kind of how you should think about the threat. It's always changing. It's always mutating. So you can't have fixed defenses. We're not building the Maginot line. So some of these recommendations are not determinative in and of themselves. They will set up a process or set up a relationship that by its nature will modify over time.

RAVICH: Yeah, Mike kind of alluded to this, but we want this report to be read. The chairman's letter is written in an extremely readable, accessible tone and we want the American people to start demanding some of these recommendations get, or all of these recommendations, most of these recommendations, the legislative ones get passed through Congress, the executive ones get operationalized. The private sector ones get adhered to quickly because you know, this is not, again, just a creature of Washington where we can solve all problems. It won't happen.

SPAULDING: Yeah. I will say having been involved with a number of commissions over the years, you know, their, commissions can decide whether they're going to be pragmatic or they're going to be really up here, aspirational blue sky. And one of the unique things as, as Mike pointed out, is that we had executive branch folks at the table with us in addition to our members of Congress, that that executive branch participation was really unique in my experience. But it kept us grounded and very pragmatic. And so that was clearly the approach that we took. Even though, you know, we've got some pretty far reaching things in there. They are all we believe, maybe one or two exceptions, really doable and the most, I think amazing thing about this report is again, unique is that, and I think we can say this, when the report comes out, I mean the staff is already working and has been first quite some time now on legislative language to implement recommendations. So we are not up here, you know, just sort of throwing stuff out. These are

things we really believe need to be done and we are doing everything we can to make sure that they get done including putting draft legislative language out there.

RAVICH: Cut and paste in the appendix for the recommendation so that Congress can literally cut and paste it and put it into the NDA. And hopefully people will call for that type of action. Both here in Washington and in the private sector again, that we went out and talk to, they know that, that there are things that must be done, state, local, territorial, tribal as well. Because, look, we're only as strong as our weakest link and if, if they don't get the flexible funding, they need to ramp up capabilities, you know, it's not going to be good for any of us.

SPAULDING: SLTT: state, local, territorial and tribal.

FANNING: Oh, also international we dealt with, that's another tough one. You know, there's three from the private sector perspective too, and I'm one person, but there's three kinds of companies in the world, right? There's birds of prey, moving prey and roadkill. It's pretty clear to me that people that are roadkill have lost their ethos. Think Enron, you know, they, they can't make things work and they lie and steal about it. The difference between birds of prey and moving prey really deal with your perspective on short and long-term success. How do you define success? And we've seen lots of moving prey companies. These are the people that will do everything they can make next quarter's earnings per share. What they said it was going to be, and sometimes sacrifice their long-term viability to make that happen. I think this report balances some very important tactics that we need to execute on, but I think it will also see within this report some very important aspirations and a very big idea is a different relationship between the private sector and government.

BING: We'd be remiss not to just touch on elections a little, a little bit more. Given that Super Tuesday was just earlier this week, and, Samantha you were talking to about the accessibility of some of the language in the report and in these recommendations, how can the government push through more resilience just in the public to disinformation operations, foreign cyber-attacks surrounding the election?

RAVICH: And I'm going to turn over Suzanne since she has just led panel on this.

SPAULDING: Well it's a, I'm glad you asked the question Chris. The – our election related recommendations are contained within that resilience pillar and that was very intentional. I mean we had a number of conversations about where should these go in the report because the most important thing is that resilience. So I talked already about the notion of, for example, why paper ballots and a paper auditable trail is so important for resilience. And that gets to what is really the greatest risk in our concerns about our elections. And that is public trust and confidence, right? What is really fundamentally at the end of the day all about is does the public believe that the process was legitimate, such that they will accept the outcome and preserve our peaceful transition of power and our democracy? And so that what we look at when we look at information operations, they are geared toward undermining public trust and confidence in our democratic institutions that in our democracy elections is one piece of it, but it goes much broader. I mean, Russia, particularly other countries are, are going to get increasingly involved, but Russia is engaged in a broad based campaign to undermine public trust and confidence in

democracy and our democratic institutions. So we have to do all the kinds of things that you hear about in terms of working with platforms and et cetera. Teaching media literacy is important, but, but really to build public resilience against that pernicious messaging, we need more robust civic education and engagement. At the end of the day, Americans need to understand what our democracy is about, what our democratic institutions are supposed to do. How they as individuals can hold them accountable, right? So to fight back against the messaging that's coming out of the Kremlin, that they are irrevocably broken and that we should give up and despair and disengage and stay home and not vote. That's the message. And we need to counter that message to say democracy is important, it is worth fighting for. It is under attack and we must all fight for it and we can't give up. We can't despair and we have to vote. Well that's my little speech but, we've captured that notion in the report.

CLINGMAN-JACKSON: I have two questions that talk about two key audiences that I don't think we've talked about as much. One, the international community, how you see kind of our allies tapping into this resource both as key stakeholders but also as like information sharing, et cetera. And then the second, you kind of mentioned a little bit about of creating a public hygiene for cyber. If you can talk a little bit more about that and what that looks like as cyber can be so big, it can really encapsulate every aspect of our life. So how do you kind of see us focusing and being able to be a little bit more strategic and targeting with that?

RAVICH: Yeah. I'll just take the first question a little bit. So it was interesting last week I was over in London and gave a talk at the Royal Uniform Service Institute. RUSI. Great people, a couple of members of the House of Commons and the House of Lords as well as the defense establishment and gave them a little bit of a preview of, the commission. Now the staff and some of the commissioners had, again over these last seven months, done extensive outreach to our friends and allies about some of these recommendations. Because everything from, as I mentioned on continuity of economy, the thinking of where do we hold the seed data. They were really interested on their own end is would we potentially think about hosting their most critical seed data so that it ties us even closer, you know, together we've got one another's back, right? But the other thing, and this isn't really as much on the resilience piece, which we're here to talk about today, but we do have a section on international norms and engagement and on that, you know, last week I talked a bit about like pieces of paper are worth less than even what you know, the signature on them. If you can't verify, you can trust. All right, so kind of turning trust and verify on its head. And as we look forward into the future of new international norms, new cyber treaties and obligations, do we have the technical capacity needed to monitor verification? Right. We'll, we're going to have to not only make sure we have that critical technology capability to, you know, quickly, quickly know if a, if a treaty is being undermined or, or purposely manipulated, but that people trust our technology showcasing that. Right. So it is, it is a bit different than, you know, our investor going to the UN and saying, here's the picture of the missiles in Cuba. You know, nowadays people will say, is that photo doctored? Right? So we not only have to have the technology to shore up these international norms that we are engaging in, but the trust that people will, will believe it. They'll leave the other two to answer on the second.

FANNING: Yeah. Let me hit the international thing too. Several years ago I went over to visit with some folks in parliament to talk about what we were doing in the US versus what's going on in the European Union and in the UK and a variety of other things. And there's lots of

good models around, okay. If you think about it, a lot of international kind of doctrine is based off the five i's, et cetera. We have to reach beyond that to think about how to collaborate. One of the most important outcomes of this obligation to join is the illumination of the battlefield. So that can't be just a domestic enterprise. We have to really understand how that works. We also know that the attribution issue is an exceedingly difficult issue that requires international cooperation. We have to cover that base from a physical standpoint. So we do the war games in the electricity sector. Suzanne was great with that and we call it GridEx and I guess we just finished GridEx 5 maybe. Anyway, this latest scenario was essentially interfering with the electricity grid in New York, the state of New York. So we took out New York City. We also took out Toronto, and so one of the things that we actually tested in conjunction with Canada, we had the equivalent of the ESCC of Canada. There was how do we stand up the system who gets priority? And it was very interesting how that worked. You all may know that the electricity grid is a network grid between the United States and Canada, particularly in the Northeast. And so these are real issues that we have to work on. When Suzanne was at Homeland Security, we intentionally populate the ESCC and non-classified space and in some cases in classified space, in a very controlled environment, Canada with America. So these are important issues that have to be dealt with. The last one is just this idea of Smokey the Bear and you know, don't be a litterbug, but this is important stuff. Dual factor authentication, how should you manage your own resources? You know, and it's funny, I'm just going to guess, I mean I'm kind of a doof on all this stuff compared to say my kids. The youngest generation probably gets this pretty well. It's probably the generation beyond the youngest up to people like me that need the most help. Okay. The other thing that we have is there's such a benefit in the world of unlimited potential and information everywhere and unlimited access and all that. We just have to be mindful of the cost and the danger of being too open. So these are messages that we can get out and it's something that that you'll see a little bit of.

SPAULDING: So just picking on your very good second question and, and on what Tom was saying, CSIS every year has a, has a project called "bad ideas in national security." Last year my, my essay for that was creating a department of cybersecurity. This year my essay on that was talking about "cybersecurity" is a bad idea in national security. And I put "cybersecurity" in quotes. I think the term cybersecurity for, for you know, the reasons that you state it has become a pretty useless really the term covers too many things. It's too broad and so it intimidates, it confuses, it does not particularly illuminate or help advance the conversation. And I think back to the years that I was the legal advisor at CIA for the folks who worried about WMD, weapons of mass destruction, and we couldn't figure out why we couldn't get traction. This was a hundred years ago. And we finally realized, you know, because we keep talking about this as if WMD was one thing, right? Nuclear weapons are not the same as chemical or biological or radiological. They have some things in common, but they are susceptible to different kinds of approaches. They're different. Theft of PII is not the same as an attack on an industrial control system. And yet we talked to the American public and our policymakers as if this is all one thing. And so we've got to start dis-aggregating that term. We've got to start being much more specific. We need to talk to our policymakers, in particular American public about what it is we're really talking about in each context. And I tried to, you know, convey this to our editor in the report and where I could give, you know, my wherewithal to try to be as specific when we go through the report and not just use the term cybersecurity. And I think if you're sensitive to that, you'll pick up on it in the report where we talk about, you know, are we really talking about a critical

functions? Are we talking about privacy issues? Are we talking about data integrity issues? Right?

FANNING: And you all know probably cybersecurity is also a bit like your human body, right? There's a whole lot about your body that keeps the bad stuff out, but a whole important function in your body is what do you do in the bad stuff, gets in white blood cells, et cetera. This notion of resilience, personal resilience in a household has to deal with those issues as well.

BING: So we have time for one more question from the audience. If anyone is brave enough to end it. There we go. Brave man in the back.

ANDREWS: Rich Andrew's National War College. So I had a specific question. Is there anything in the report about the role of the, of the U.S. military in any of these issues?

RAVICH: Yes, we have a whole section and so layer defense layer deterrence. As we were talking about, this panel was focused specifically on the resilience piece and specifically on resilience on in the private sector, but there is a third of the report on persistent engagement, defend forward. You'll be very interested to see how we talk about defend forward a little bit more broadly then has been in in a pure military doctrine. But yes, there's a whole section of the report.

FANNING: And really great people, guys that weren't on the Commission but were very helpful. Paul Nakasone does NSA and U.S. Cyber Command just to reflect people and people. I've grown up with a little bit over recent history. Keith Alexander, guys like that. The idea of aligning the military, but let's just not leave it with the military and U.S. Cyber Command. I would go to FBI and Secret Service and others making sure that the hold accountable stream is integrated into the whole notion of a whole of society approach layered approach to this effort

SPAULDING: An acknowledgement, you know, the reference to the solarium project where they were three sort of conflicting approaches that were being advocated and, and the, you know, teams were set off to develop their best advocacy for each approach. And ultimately of course it was a blended approach. Well we jumped started by moving to a blended approach. But having said that, there's an acknowledgement that there is sometimes tension, for example, between the emphasis on norms and an emphasis on persistent engagement. There may be times when there are attentions there that need to be reconciled. And the question about international engagement and building trust with our international partners, persistent engagement and defend forward is the idea that we are going to not sit back and wait for the adversary to come, but to engage in that space between us. Between us and between our and our adversary. Well that space is often going to be space that is owned by our allies, by other countries. And so one of the things we are, we are very, you know, open about in this report is that we are going to have to make sure that we have robust consultation with other countries around those issues.

FANNING: Right. And every great last question finishes with a link to the first question and it really goes to the idea. I'm building – my company is building the, the only nuclear plant in a generation of Americans. And you say, Oh well do you want these guys on your system? Yup. Because if anybody's going to interfere with this multi-billion-dollar decade long thing, I

want to make sure that the guys that will hold the bad guys accountable know about it when I know about it. Now that's a single instance. But projecting that forward to systemically important infrastructure is an important concept.

RAVICH: And again, let me, let me just say very quickly on your question, and not to give away the big reveal next week, but clearly in the, in the military context, thinking about, you know, do, do those elements have that need to be engaged in this battle space, have the right authorities, do they have the right capabilities, they have the right personnel. And just on that last piece, as we think about the personnel requirements going forward in this battle space, I'll just give you a brief insight into one of the really good conversations that we had over these 28 meetings. There's a lot of discussion about, well, you know, do we need more reserves, cyber reserves? And someone brought up, I thought, and I had never considered this before, maybe Suzanne and Tom did. That when you think about reserves, you think about, well, they're going to be in the private sector knowing that capacity, right? They have that knowledge. They're, you know, they're, they work for the CTO or the Cisco or operational technology or, IT calling them up. Yeah. But if there is a national cyber emergency, most likely we're involved in an overseas contingency. So you know, thinking through, do we want these people, you know, to be now with the military deployed overseas, when we have rolling outages, we know maybe the best place for them is still working for Tom in OT or IT. Right? And, and because this is such a different battle space than we tend to think about one call up the reserves, send them over to the Middle East. The battle space is here.

SPAULDING: Yeah. It's an issue with that when you think about the National Guard as well, and you just have to be careful not to double count.

BING: Yeah, I think that's a great place to end it on. Please join me in thanking our panelists