FDD EVENTS

Bolstering America's Cyber Diplomacy Capabilities

Keynote remarks by Representative Jim Langevin
Featuring Laura Bate, Mark Iozzi, and Chris Painter
Moderated by RADM (Ret) Mark Montgomery

MAY: Hello, I'm Cliff May, FDD's Founder and President. Thanks for joining us today. For those of you who are not familiar with us, FDD is a non-partisan 501c3 research institute focused on national security and foreign policy. I'm pleased to welcome you today to an event called, *Bolstering America's Cyber Diplomacy Capabilities*, hosted by FDD's Center on Cyber and Technology Innovation. CCTI seeks to advance U.S. prosperity and security through technology innovation while countering cyber threats that seek to diminish it. CCTI promotes a greater understanding within the U.S. government, private sector, and allied countries of the threats and opportunities to national security posed by the rapidly expanding technological environment.

Today's event will discuss the role that cyber diplomacy plays – or should play – in U.S. cyber strategy, and the organization and resources needed at the State Department and elsewhere for effective cyber diplomacy. We have a great group of experts lined up to discuss the authoritarian threats we face in maintaining an open, transparent, and reliable internet and what steps Congress and the administration can take to ensure our cyber diplomats have the tools and capacity to execute their critical role in defending U.S. values and interests in cyberspace.

I'll provide brief introductions of our panel, but please visit our event webpage for their full biographies. Laura Bate is a Senior Director for the congressionally mandated U.S. Cyberspace Solarium Commission. Prior to joining the Commission, she was a policy analyst with the Cybersecurity Initiative at New America. Mark Iozzi is deputy chief counsel for the U.S. House Foreign Affairs Committee, where he previously served as counsel and as a professional staff member. He also previously served as a legislative fellow at the U.S. Senate Foreign Relations Committee and a legislative aide for Senator Maria Cantwell. Chris Painter is a globally recognized leader and expert on cybersecurity and cyber policy and diplomacy. He has been in the vanguard of U.S. and international cyber issues for over twenty-five years—first as a prosecutor of some of the most high-profile cybercrime cases in the country and then as a senior official at the Department of Justice, FBI, the National Security Council and finally as the most senior cyber diplomat at the State Department. Finally, my colleague Mark Montgomery will moderate today's event. Mark serves as senior director of the Center on Cyber and Technology Innovation. Prior to joining CCTI, Mark served as the Executive Director of the Cyberspace Solarium Commission, where he remains as a Senior Advisor.

Before we jump into the expert discussion, we are pleased to first hear from Representative Jim Langevin. Congressman Langevin is a senior member of the House Armed Services Committee, and has been Chairman of the emerging threats, newly named cyber subcommittee. A national leader on securing our nation's technology infrastructure against cyber threats, he serves as a commissioner on the Cyberspace Solarium Commission and is supporting the Cyber Diplomacy Act, which will be discussed today.

We hope you enjoy today's conversation. I encourage you to learn more about FDD, and check out our recent events and analysis at fdd.org. You can follow us on Twitter @FDD. I am now pleased to turn the floor over to Representative Langevin.

LANGEVIN: Hello and thank you all for joining us for a vitally important discussion about the need for strong U.S. cyber diplomacy. With the explosion of virtual events like this as we continue to battle the COVID-19 pandemic, I think we all have a better appreciation for our reliance on cyberspace. So, I want to thank the Foundation for Defense of Democracies, and particularly, my good friend and fellow Solarium Commissioner Dr. Samantha Ravich, and our Commission's Executive Director, Mark Montgomery, for organizing today's event. The panel that they've assembled for you today is superb. Chris Painter helped catalyze efforts on cyber diplomacy as our inaugural State Department's Cyber Coordinator. I regularly call on him for his wisdom and sage advice. Mark Iozzi has been working these issues for former Chairman Engel and now Chairman Meeks for years and is widely respected by members of both sides of the aisle for his

deep expertise in this domain. And Laura Bate helped develop many of the principles underlying Solarium's Pillar 2, as a key member of Task Force Three.

So, mindful of the fact that I'm keeping you from the real experts, I thought I would just provide some framing remarks about why I'm so passionate about reinvigorating our cyber diplomacy, and why U.S. leadership, in particular, is just so critical. First off, I think it's important to reflect on how we understand the cyber domain. For instance, I chaired the newly chartered Armed Services Subcommittee on Cyber, Innovative Technologies, and Information Systems. And in that context, we often think about cyber as the "fifth domain" of warfighting. But, obviously cyberspace is also used for commerce and to support national and critical functions so, we cannot only think of it in a militarized sense. What's more, while you'll often hear me say that there'll never be a war without a cyber component going forward, I'm also first to point out that there's no such thing as a "cyber war." Cyber tools, of course, will be used alongside other tools of conventional warfare. So, we cannot think of a cyberattack as demanding a response only in cyberspace. But, the focus on cyber warfare and cyber operations that would rise to the level of armed conflict misses a huge component of the cybersecurity challenges. So, cyber tools, certainly, will be used in warfare going forward and they undoubtedly can be quite effective. But, where cyber really shines is in the grey zone – below the level of armed conflict. And it's here that norms or responsible state behavior, international law, and other diplomatic concepts are so vital to maintain stability in cyberspace.

In the Solarium Commission's report, one of the elements of a strategic vision of layered cyber deterrence, is shaping adversary behavior. So, we aim to do so by implementing our "Pillar 2" recommendations, many of which build on the concept of taking action when nation states violate norms. After all, these are norms of behavior, so, "Do as I say, not as I do," just won't cut it when we're building a body of precedent about how countries should respond to malicious actors. So, Solarium invests a lot of effort in ways that we can reduce the time between offensive action and response, since diplomatic acts never happen in vacuum. You can understand that if we announce sanctions for an act that took place three years before hand, our adversary may very well wonder if that's the true motivation, or, if some more proximate offense is the real reason for the sanctions.

But, our single most important recommendation in this area is the creation of the Bureau for Cyberspace Policy at the State Department. As I mentioned at the outset, cyber crosses many equities from human rights to arms control to economic growth. So, in order for the United States to lead on the global stage and advance our vision of an open, interoperable and secure Internet, we need to be able to break down the silos that can exist within these often-desperate areas of diplomacy.

So, what's more, we need to appropriate resources to diplomatic activities. So, I was a big fan of Rob Strayer while he was at State, but, he was really a one-man band with a small team, though they did quite a bit with the limited resources that they had. But, our adversaries took advantage, whether by calling for the creation of a new cyber-crime treaty, or by starting the Open-ended Working Group at the United Nations to compete with the group of government experts. Creating a Bureau with an Ambassador-ranked leader is key to ensuring we have a holistic strategy and pushing back against anti-democratic forces looking to use cyber as a means of oppression against their own people, and as a way to counter our interests through proxy operations.

Thankfully, Congress is on the case. Thanks to the leadership of my Congressional Cybersecurity co-chair and co-founder Congressman Mike McCaul and House Foreign Affairs Committee Chairman Greg Meeks, the House will soon advance the Cyber Diplomacy Act. So, this bipartisan legislation will create a Bureau of International Cyberspace Policy. It's important that this bureau will need to be placed on the Undersecretary for Political Affairs or the Deputy Secretary, ensuring that it can guide diplomacy across all the diverse areas touched by cyberspace.

So, I have full confidence that this organizational change will best position the United States to reclaim its role as a global leader in cyber diplomacy – a need that's particularly urgent given the ever-increasing array of cyber threats and other challenges that we face. So, I hope you enjoy the panel discussion today. I want to thank you again for your interest in this very important topic. Thank you.

MONTGOMERY: Thank you, Representative Langevin for those comments. As Cliff May mentioned, I'm here with Chris Painter, Laura Bate, and Mark Iozzi to discuss *Bolstering American Cyber Diplomacy Capabilities*. I want to dive right into the questions.

So first, for Chris Painter. For our audience members who don't know you, and they all should, you are one of the world's first cyber diplomats, and you spearheaded the creation of the Office of the Coordinator for Cyber Issues at the State Department, an office that has continued to evolve and change since your time there. Can you talk about what you think is working, what you think is not working, and how the U.S. government is organized to manage diplomacy on cyberspace issues today? And finally, if you could comment on what you think needs to change to ensure that the U.S. is in a position to engage internationally on cyberspace issues.

PAINTER: Yeah. Thanks very much, Mark. And, and also thanks to Congressman Langevin for his kind words. You know, we really were the leaders in this; the U.S. was the leaders. We really created this, back now almost 10 years ago. My office will celebrate its 10th anniversary, my old office, next week, actually on my birthday. And 10 years is not a lot of time in any new area, and this is a new policy area, and we created it. We were the leaders internationally. We created the first dedicated office, first dedicated position to cyber diplomacy, and really raised the level of diplomacy in cyber issues around the world. There are now about 40 offices in countries around the world. Many of them are ambassador level. Others are senior officials in different countries.

And unfortunately, during the Trump administration, we took a step back. I don't think there was an understanding of why these were important issues, why these were important policy issues. The office was downgraded, its organization somewhat confused, in kind of a limbo situation. That said, the folks, my former staff there, many of them are still there, thankfully, I think have done quite a bit of good work, talking to allies and partners, talking about deterrence initiatives, trying to get countries to concentrate on shared threats. But they've been starved for resources and starved for priority, frankly. I mean, they're down in the organizational chain, they don't have the clout or the resources to do the job that they need to do.

So, President Biden, when he came in, said this is something across the board that he wants to make sure it gets attention, cybersecurity, in every level of the government. Both Tony Blinken and others at the State Department are people who understand these issues, which is good. So, it really needs to be re-elevated. We need to make sure we're engaging the world and have the resources to do this across the board. And that's something I think is a real priority. This part of the overall cyber issue, and how we counter threats, and how we build partnerships, is a core part of it. And if we don't have that covered, if we're not leading on that, we're less for it.

MONTGOMERY: Thanks, Chris. That's a great setup, but now we'll go to the Hill, for Mark. If people don't know, you're the Deputy Chief Counsel for the House Foreign Affairs Committee. And I know you've been closely involved in discussions on the Cyber Diplomacy Act. Can you give the audience a brief overview of the proposed legislation and its status and where can we expect to see some movement in the near future? And where do you see we might have obstacles in getting this done this year?

IOZZI: Let me just unmute here and say, Mark, absolutely, thanks for having me. And I think the legislation ties in really well with the comments Chris made about the history of this issue with the State Department, where the U.S. has been in the past and where there's opportunities for us to go with this in the future. The legislation has a really long history, the Cyber Diplomacy Act. It actually started when Chris Painter was still at the State Department, but with this sense that America had been leading in this space, but there was really a lot more that we could do. And that cyber policy really should be something that is viewed as a crosscutting, national, diplomatic foreign policy priority that touches security issues, economic issues, and human rights issues, and really needs to be treated as a foreign policy priority, and not as a side issue.

In that time, I think a lot has happened within the U.S. government and around the world and how we engage in cyber diplomacy and how our adversaries engage on it, and our allies engage on it. But really, not enough has been done structurally within the Department to not just recover from the downgrading of Chris's old office that he talked about, but to actually bolster this issue, which was the initial intent of the legislation when we drafted it. And so what the legislation does, what the Cyber Diplomacy Act does, in a nutshell, is establish, in the current iteration, a bureau, but initially it was just an office that could be elevated to a bureau, that is in charge of leading this crosscutting issue of cyber diplomacy at the State Department, from the security issues, to the economic issues, to the human rights issues, to elevate those issues and to coordinate them across the inter-agency and the State Department.

Unfortunately, I think it got bogged down in some bureaucratic in-fighting about where this new bureau should be structured in the Department. The past administration, after downgrading Chris's office, I think realized their mistake, I think, responded to the introduction of the legislation by saying that they did in fact want to create a cyber bureau. I think the problem was that the work wasn't put into, from Congress's perspective, from a bipartisan perspective in Congress, the work wasn't put into really understanding what the mission of this new bureau should be, and how that mission-driven focus should dictate where it's structured in the Department.

And so, we ended up with a couple of proposals that Congress couldn't figure out why they were structured the way they were from the executive branch. One proposal to focus on economic cyber issues, and then another proposal to focus on security cyber issues, and really none of those responding to the intent of the legislation or what outside experts, including the Solarium Commission have identified as this need to have a crosscutting prioritization of cyber policy within the State Department.

So, we didn't really get past these structural issues with the Department. And we've been bogged down in that disagreement for far too long. Going forward, I think we're going to reintroduce the legislation very shortly, with a hope to get past the bureaucratic structural issues and to really just push forward with authorizing a cyber bureau at the State Department that will deal with again, the security, economic, and human rights aspects of cyber diplomacy. So, hope to see movement on that very soon out of our committee.

MONTGOMERY: One quick follow up on that. Is this legislation bipartisan in nature, or is this just one party pushing over the other?

IOZZI: Yeah, absolutely. So, it's always been bipartisan. It started out under Chairman Royce, a past Chairman of the Foreign Affairs Committee, and then is currently led by Ranking Member McCaul.

My past boss, Chairman Engel, was the lead Democrat on the bill, and going forward it will be McCaul and current Chairman Meeks' legislation, along with other bipartisan co-sponsors, Mr. Langevin and others, is our plan for introduction now. So, it's always been a bipartisan, bicameral issue. It's never been a partisan issue.

MONTGOMERY: Well, great. In today's environment, that's an excellent validation. All right. Let me turn to Laura. About a year ago, the Cyberspace Solarium Commission, which Mark referred to, and which you and I are members of, released its final report to Congress and called for the creation of an Assistant Secretary of State dedicated to cybersecurity issues. How did the commission drive this recommendation? How do you view the Cyber Diplomacy Act in comparison to the CSC's proposal? And do you think the Commission will end up fully supporting what's going forward, and potentially going forward in the Cyber Diplomacy act?

BATE: Yeah, thanks. And thanks very much for allowing me to join you. It's a remarkable panel for being able to pick apart and discuss some of these issues. In answer to your question, I think the Cyberspace Solarium Commission, back in our very early days, we're talking like summer 2019, had a series of briefings to cover a lot of the issues we knew we would have to address. And Rob Strayer came in for one of those and talked to our commissioners. And I think, at the time, he was Deputy Assistant Secretary for Cyber and was able to talk us through what his office was doing and what some of the challenges were that they were seeing.

And I think, even from those early days, as you heard from Congressman Langevin, it was very clear to the commissioners that there's enormous amount of value for enabling State Department's work, and for implementing the structural changes that allow us to do that. Again, echoing the same trends that you heard from Mark Iozzi, a lot of bicameral, bipartisan support from the Commission to make sure that we were setting up State's team. They're doing monumental work, but they're limited by position, by resources, by staff size.

So, when this came down to our staff, to the CSC staff, to my colleagues and I, we started picking apart some of the goals that would help bring greater elevation to that position. And one of the first ones was looking at the leadership structures that are set up. As you said, Mark, our recommendation was to establish an Assistant Secretary at State that would report to the Political Affairs Bureau. So, picking that apart first, and the Assistant Secretary and the placement of political affairs. We wanted to elevate, as I think Chris, you started out by saying, that you were sort of buried in the bureaucracy. And we wanted to make sure that the position was really elevated to a leadership level that both reflected the importance of the issue, but also allowed some of the crosscutting authorities that would really make the position a success.

In our original report, we talked about an actual Assistant Secretary of State. Now the number of Assistant Secretaries given to the State Department and allowed to the State Department is set in law. It's a capped number. So, as we started to look into it and dig into it, it did become apparent that the way State Department works with this cap is to recognize that a number of positions, like for example, the Coordinator for Counterterrorism has a position with the rank equivalent to Assistant Secretary. And that we feel addresses a lot of the things that the commission looked at, and a lot of the things that the commission was trying to get out of that. One of the real non-negotiable and really important parts in the elevation of that leadership is that the position should be an ambassador-level position.

And then looking at where the Cyber Office sat organizationally, I think that you heard from Mark that we really wanted to start with the mission at the commission as well, and think about what we wanted this office to do, that we needed the office to be able to establish an open, interoperable, reliable, and secure Internet. And that in doing that, you need to be able to address a broad range of issues. You're talking about Internet governance, you're talking about digital economy, privacy, surveillance, in addition to the more bread-and-butter cybersecurity norms, capacity-building, those types of things. So, that was the basis for our suggestion, that that position report to the Undersecretary for Political Affairs or higher, to allow some of that crosscutting ability, the ability to gather together a range of different issues to really address in a fulsome way what we know this Cyber Ambassador will have to confront.

Comparison to CDA. The CDA provides for an ambassador-level position, so I think looking at the nuts and bolts of what's laid out, I think that there are a lot of similarities. The location within the administration is the same there as well. One of the things that CDA has that the commission's recommendation doesn't lay out quite as coherently or quite in the same way is a policy for how to engage internationally in cyberspace. We don't use the same words that CDA does, but we rely on a lot of the same basic principles. We talk about the same call out for cybersecurity norms. We talk about the same importance of rule of law, the same emphasis on collaboration with like-minded partners and allies. So, where the CDA has a little bit more explicitly written some of those priorities, the commission is very much there in spirit. So, I would say there's a lot of similarity between the two.

MONTGOMERY: Hey, thanks. I think I want to dive now into what it means for our cyber diplomacy activities at the State Department. But before I go there, I got to bring up another question with Chris cause, because Mark referred to this. And at the end of the last administration, really the waning moments, most people were taking a knee. We turned around, and former Secretary of State Pompeo established a Bureau of Cyberspace Security and Emerging Technologies at the State Department. The move's come under criticism from lawmakers and some panelists on both sides of the aisle. I'd like your opinion. What are your concerns associated with the manner in which this was established by the former Secretary of State, and how could you see a Cyber Diplomacy Act charting a different course, that can help address some of these concerns?

PAINTER: Yeah. Happy to address that. And I've been one of the critics, as you may have alluded. So, I would say, first, to step back, this shouldn't be a partisan issue. When I was at the State Department, and when I was in the government, at Justice or the White House, this has never really been a partisan issue. It's been a bipartisan issue, and it should be. This is a core issue for all of us, and we should try to maintain that. So, it's good that this is a bipartisan effort and bill. The other thing I'd say is, the advantage I had in my position is I reported directly to the Secretary. So, I wasn't buried in the bureaucracy. Unfortunately, what they did to the office, which unfortunately for Rob, is they made it a Deputy Assistant Secretary level, who reported to an Assistant Secretary, who reports to the Undersecretary. It's pretty nested down, and had that in the economic session, where the other rest of the office was still under the Secretary. It was very confusing.

But, if you look at the office, or the bureau, the things you want are, position, like who did this report to? So, it has that power. Scope, crosscutting, so it has that authority across the different bureaus and areas. And I had cross-cutting authority. We worked on cybercrime, norms and international cybersecurity, worked with the cyber terrorism, on cyber terrorists in the Counter Terrorism Bureau, worked on Internet governance issues, worked on human rights issues with DRL. We had a broad sweep, because all of these issues are interdependent. They're not silos. They depend on each other. When Russia, for instance, or China talks about Internet governance and having the state control and more, they're doing that as a proxy to controlling speech and controlling what they think is destabilizing, so as human rights dimensions, but also as a security dimension. So, if you look at these two, these narrow straws, you don't really understand the problem. I think other countries have recognized that as well. So, turning then to Pompeo, literally as the door was hitting him on the way out the door. And I think literally, the day after the Senate confirmed President Biden's presidency, he releases his plan. Which, although it had been around for a while, doing that the last minute, didn't seem to make a lot of sense after starving this area of resources and position for four years to suddenly do this.

And the plan itself has a couple of flaws that I think are pretty critical if you look at those pillars. In terms of position, it reports to the Arms Control Undersecretary. Now, that's a good person, certainly, but that only covers one part of the mission. It probably covers the stability area to some extent, some of the cybersecurity area, but not clear, it's a new area. The legislation has it reporting to P or higher. So Political Undersecretary is the third highest in

the Department. Traditionally, also has the strength of the State Department because all the different bureaus that are involved, all the regional bureaus. Higher would be the Deputy Secretary or the Secretary, like I reported to. So, it placed at a higher cross cutting position so you're not in one stove pipe. I think the first proposal was to put it in the economic bureau. It would make no sense at all because those issues, although they're important, certainly don't cover the vast range of these issues. So that's one issue, placement.

The other is scope. And I think the real problem, my biggest problem with the proposal is the scope is very narrow. It's dealing with the kind of security elements of new technologies and cybersecurity. And if you look at all those other issues, the human rights issues, internet governance, now doesn't mean internet governance anymore. It means everything. If you go to the UN discussions on this, the Internet Governance Forum is not about the technical workings of the internet. It's about the broad sweep of issues. And to have several different voices at the State Department who have competing voices on these issues, it's just a recipe for disaster. I mean, we're not talking with one voice, we're talking with many voices. We're not having a unified approach, we're having a splintered approach. And that doesn't make sense in terms of our own policy or what other countries are doing. So, I think that, at a minimum, we have to rethink what that structure is. If that makes sense, if that scope makes sense.

And the third thing is coordinating authority, with that additional scope, wherever you place this, they have to have coordinating authority over the other issues that are involved, whether they be human rights online or internet governance and other issues, or some of the economic issues. That doesn't mean you have to move everything into one bureau, but they have to have that coordinating authority. I had the authority of working in the Secretary's office so I could cajole people, but having some direct authority that the Cyber Diplomacy Act provides, I think, is very useful. So, in short, I think that's what the failings of the current structure are. And I think those can and should be addressed so that we don't end up with something that just balkanizes us this issue.

MONTGOMERY: Thanks. You gave me two thoughts when you say that. First, the term cross cutting. In so many ways that, the Cyberspace Solarium Commission in our recommendations to the federal government, the executive branch was figuring out how to elevate things out of stove pipes, and get them cross cutting. So, I think that's as true at the State Department as anywhere else. And I love that you called it nonpartisan, or bipartisan, so did Mark. I'll say, inside the Cyberspace Solarium Commission, Senator King would say, "This is bipartisan, nonpartisan. I don't know the politics of the people in the room," which I questioned when it came to like Representative Gallagher, Senator Sanders. But broadly, I used to put the one corollary, there's a word. If you put the word election in front of rainbow unicorn, it's partisan. So maybe election cybersecurity is partisan but I think everyone –

PAINTER: Mark, as you know, unfortunately I think the Russia situation complicated the area and made that more partisan than it needed to be, because that was a link. And that's partly why I think President Trump just did not prioritize or care about this issue, which is unfortunate for all of us.

MONTGOMERY: That's a good insight. Well, Mark, I did say I wanted to get down into the nuts and bolts of what cyber diplomatic activity is. So, I'll dive in here and say, one of the responsibilities outlined for the head of the office, or Bureau, potentially created in a CDA relates to encouraging the development and adoption by foreign countries of internationally recognized standards, internationally recognized policies and best practices. So, really standard setting. And this has received a lot of increased attention over the past several years in the context of our competition with China. Why are technical standards and bodies important? And what role would the State Department and our diplomats play?

IOZZI: Yeah, you're absolutely right that this is an issue that's received – international standard setting – it's received a lot more attention, especially in Congress, than it has in the past. And I think it goes from, sort of, America's tradition of approaching standard setting is largely an industry-led and multi-stakeholder approach with government involvement, in some aspects of it, but not in any way, government-controlled in the way that some of our foreign state adversaries see it. And I think that there's, what we need and what there's a clear path forward for and what the legislation envisions, is that America still has its multi-stakeholder approach, but that we engage on this as a diplomatic, economic, and security and foreign policy priority for the United States. The problem that we've heard about, and I'm sure many other people are familiar with as well, is the Department has a small capacity to do this, but not nearly the same amount of resources or structure or rank of officials that countries with a very different view of how standards should be structured have.

The Chinese show up with a much larger delegation and very different priorities than the United States shows up with far too often. And that's something that is a structural problem for how we've organized our diplomacy and something that is really a fundamental part of what the legislation sets out to address. And so that means that the State Department should be meeting at a similar rank with a similar amount of engagement to further our conception that I think is really well-founded about how standards should be set, how the internet should be structured and governed and how technology should be structured and governed in a way that prioritizes our conception of security and privacy and human rights in a market-driven approach, and that is going to serve America's national interests, but also these cross cutting interests of democratic societies. And if we don't engage at that level, we're going to miss that opportunity, and we're going to be saddled with internet national standards that don't serve, I think, those fundamental interests of having an open and interoperable and fundamentally democratic Internet.

I'll also take this opportunity, I think maybe to just pile on to what Chris said about the proposal that Pompeo pushed through right as he was on his way out the door. And that was fundamentally a proposal that I think wasn't set up to meet this need. I think that's one of the concerns of looking at cyber diplomacy as a security issue. As essentially as an arms control issue, which it's fundamentally not. And that we, in response to the Pompeo proposal, which had been on the table for quite a while, without, sort of, our concerns being resolved, one of the things Congress did was asked GAO to look at the proposal. And what they identified was that in coming up with the proposal, Secretary Pompeo had not consulted with any of the other government agencies, some of whom are very important in standards setting, or consulted with relevant parts of the Department, or as GAO put it, made a decision based on data and evidence. And I think making an evidence-based decision was really Congress's fundamental role with that. That I think we are open to different ways to structure the reporting requirement, to structure the reporting of the bureau at the State Department. If we're not stuck with stove piped policy areas that don't address the cross-cutting nature of cyber diplomacy. That's the fundamental requirement here. And if the department's ultimate proposal is evidence-based. I think one of the things that we're going to be looking forward to in moving the legislation is solving those policy issues without being bogged down in whether there's reporting to one undersecretary or another undersecretary. And it's my hope that we're in a position to do that and move forward now.

PAINTER: I just jump in to say, critical to that is what I was saying about having that authority to deal with cross cutting issues. If you don't have that, your loss. And the State Department is really not architected for cross cutting issues. It's not the way they were built originally, but it's something that needs to happen going into the future.

IOZZI: The last thing I'll say on this is it's Congress's expectation and understanding that the Pompeo proposal isn't being rolled out as written, again, as GAO found without any evidence or data to support it. And that that's being reviewed. And our hope would be that that review in conjunction with moving the Cyber Diplomacy Act will solve it.

MONTGOMERY: Well, thanks. That's a great discussion. I would commend to the audience a series of [Government] Accountability Office reports. Several on State Department, which I think hit right at the issues that have come up here, but also more broadly at the federal government's implementation of cybersecurity that the whole cross-cutting discussion was the subject of an unfortunate GAO report in the sense of a very critical report of the executive branch's inability to integrate its cybersecurity efforts. And you remind me of one other thing. You gave a great description that could be cut and pasted into a discussion at National Institutes for Standards of Technology, or NIST, for their budget appropriations to support these international standard setting bodies. I think they'd have the technical expertise, they have the mission. So, they're a little different than the State Department is right now. And that in terms of clearly stated out in an authorization. But what they don't have are the capacity and the resources to fully support what I hope will be a State Department-led effort to really get at this. Great.

Laura, kind of break into a different type of diplomatic activity. The Cyberspace Solarium Commissions kind of broader strategy for preventing, withstanding, and responding to a cyber incident or cyberattack, places heavy emphasis on the value of building a coalition of allies and partners. I know some of this work has been underway since Chris was at State, as well as under Rob Strayer. But if you could give me some examples, how the increase in use of joint attributions of cyber-attacks that we could try to accomplish among the international community and how we could use that. And then how do you see that word growing? And what's it going to take to get to where the Commission wanted to be? And why do you think the Commissioners value this?

BATE: Yeah, absolutely. And I'll preface my comments by saying we studied it, but Chris, you've done it. So, feel free to jump in there, if there's anything I'm missing here. But sort of speaking to how we saw it on the side of the Commission and looking into these issues. You mentioned work underway. I think part of what we were looking at there is joint attribution. And I mean, it was fascinating because even during the time that the Commission was meeting, we were seeing the drum beat of joint international attribution really increase, not just in frequency, but in the number of countries participating and in the rapidity after an attack with which you'd actually see that attribution come together. So, to give a couple of examples, the U.S., UK, Canada coming together in 2020, talking about COVID vaccine development, hacking of COVID vaccine development.

One to probably North Korea. There's a really standout case as well. In 2020, we saw joint attribution, international joint attribution, of an attack that occurred in 2019. A Russian cyberattack on Georgia. And in the end, there was something like over 20 countries who had signed on to that joint contribution. And there is a really interesting, reasonable, rich academic discussion about the value of naming and shaming in terms of attribution and what value that has in shaping behavior, but sort of setting that aside, independently of that, this kind of joint attribution does two really, really, really important things in terms of international engagement. One, it sets a baseline, it communicates that the international communities, or at least a large coalition of partners and allies, can come together, can be united on recognizing not just that an attack occurred, but who did it and what it looked like and that we all agree that these are the basic facts.

Being able to communicate that allows us as a community to say, "If an adversary is picking on one of us, they need to be prepared for a response from all of us." They're risking engaging a larger group. They're risking a response, whether it's just calling them out or whether it's sanctions or whether it's some other step. That kind of response from a larger community of nations by picking on one. The second thing that I think that this does, it's really important, is that joint attribution allows us to establish a baseline to take that further action. If we all do agree that X happened and Y was responsible, then we as an international community, as a group of coalition of partners and allies, can move forward with other steps.

And what those steps are, obviously, you're going to vary significantly – whether it's legal or economic, whether we're talking sanctions or whether we're talking something else. Being able to establish collectively that this happened is really, really an important first step. So, talking about growth and what that can look like. I think a big step is simply figuring out what those responses are. Like whether they're legal, whether they're sanctions, whatever comes afterward. I think being able to work with our partners and allies to determine what their legal framework allows, what ours allows, and how we work around some of the challenges sort of bridging from one to the other is really important. Bringing more countries into the fold is really important. Research is very clear that when you have joint action, say for example, sanctions, the more countries that participate, the more effective those are at shaping adversary behavior, shaping anyone's behavior. So being able to connect with that coalition of like-minded allies and partners becomes really critical in having an effect.

The other step, I think, is getting faster with that kind of attribution. If an attack happens, the lag until we attribute that attack has a lot to do with being able to establish communication between international counterparts, whether someone in the FBI can work with someone at EUROPOL to be able to establish basic facts and go through that kind of work. And that comes from building muscle memory, right? That's practice. And that's a lot of legwork on the part of our cyber diplomats and on the part of our government across the board, being able to figure out how we can establish these pathways, establish this communication, establish patterns and protocols, and be able to do it quickly under pressure.

Getting there, because this can be a really labor-intensive thing, it takes hands and it takes investment over time. The State Department needs to have the bandwidth to be proactive and address some of these issues beforehand, but also the agility to be able to field an effective response, if something does happen. And that agility comes from being able to cut across stovepipes and here again, we've said the word cross-cutting a lot, but that's really where a lot of that agility comes from.

PAINTER: Yeah. And I might just add to that. Yeah, absolutely agree with everything you said. I'll just say that indeed, the folks in my former office have tried to continue this to try to build those alliances, to advance this idea of a deterrence initiative, to talk about what costs can be imposed. We have been terrible, both as the U.S., with also the community of countries at actually taking that next step. You're not going to name and shame Russia or North Korea by naming them. But as you said, it has other value. We have to take that step in making sure that this is going to be costly to them and we're taking action and we're doing that with partners. And I think that's really going to be the challenge going forward. We've seen some good action out of Europe already, but we need to do more of that.

MONTGOMERY: And if I can add one thing on attribution, I'd say it's speed too. And one of the problems in the United States, we still, I mean, I'm not a hundred percent sure to the degree to which we pin the tail on the SVR for SolarWinds and certainly tweets that claim it might be China in the middle of your description of the problem don't help, but we need to take attribution from a month's long process to an hour's long process and kind of skip the weeks and the days, along the way and get there. And there's a process inside the United States, intelligence community, law enforcement, data information sharing network, to get to that, and then get it in a way that's releasable rapidly to a key allies and partners. And I think once we do that, we'll show the kind of trust that might engender faster movement on some of the what do we do about this now points?

PAINTER: Well, and we have to be in a position to even if it takes us months to arrive at that, what we did NotPetya, it took six and a half months to say it was Russia. And we did that and we said, and there will be consequences in the future. Now, if you're going to wait six and a half months, have something ready to go then. So, we have to synchronize much better than we've had in the past, I think too.

MONTGOMERY: That's a great point. So, Mark, moving on. GAO has come up a couple of times in our discussion and at least in older versions of the bill, and I think in the current version of the bill, that could have become a Cyber Diplomacy Act, it requires GAO to submit a report to Congress a year after the signing of the CDA that assesses U.S. cyber diplomacy and how the creation of the bureau has impacted related efforts. Where does Congress, or what's the House Foreign Affairs Committee hoping to see from this assessment? In other words, what do you think the status quo could be a year after the CDA is signed?

IOZZI: So, yeah, so GAO has come up a lot because I think one of the real challenges that we were setting out to solve was a concern that at a senior level in the Department, I mean, to be totally frank, especially after Chris left, there was a concern that the Department was failing a little bit and trying to figure out what cyber diplomacy even was. And that was evident in a number of conversations where they would present to us their plan and completely misdescribe the problem that they were trying to solve. And I think that there was just a real disconnect between some sort of stretched very thin officials within the Department that knew what they were doing had been doing it for a long time and just not – in a senior leadership, especially under Secretary Tillerson, who was trying to downsize the Department as whole – just this real disconnect about what cyber diplomacy was.

I think there's now a much clearer conception of what the whole point of a bureau and agreement and consensus that there needs to be a bureau. So, I think that that initial problem has been solved. Nonetheless, I think it really remains to be seen how well a new cyber bureau will be implemented and how successful they will be. And I think that's really where GAO can come in and be very helpful and has already been very helpful. And that is in identifying what are the best practices and what are the metrics for measuring success within an organization, and how do we measure whether or not we've achieved that? And they have a capability to do that in a more concerted way and to sort of augment congressional oversight with sort of various specific findings and recommendations that we found very helpful on cyber policy and other areas up until now.

So, I think the bill included one aspect of a GAO investigation, but that's just a small part of sort of our overall work with GAO to augment Congress' oversight in assessing whether or not this bureau is achieving all of the things that we've set out right now, right? Engaging in the cross-cutting aspects of cyber diplomacy, setting metrics for success, and then whether or not they're actually successful in coordinating and leveraging diplomatic power to show success in those areas. So that's the sum total of our large project. The GAO is an important part.

MONTGOMERY: Thanks. And as I said, all props to GAO and the reports they've done, I think it really has made a difference. And I would extend it beyond State Department again, DOD some of their reporting there has been really groundbreaking in helping DOD establish itself properly. So, I think going to GAO in the Cyber Diplomacy Act is absolutely appropriate use of the skillset of that team.

So, Chris, you're President of the Global Forum on Cyber Expertise and Foundation Boards. And as you can tell, I hope that maybe that's not your job in a few months, but you work directly on issues related to cybersecurity capacity building. Can you talk about the importance of that as the building to the U.S.? Why is it critical that we aid other countries in building their capacity? And kind of during your time at the State Department, how did the U.S. engage in this capacity building effort? And what barriers did you find that stood in your way?

PAINTER: So, I found capacity building, I still find capacity building, especially in my new role, as foundational to everything else we're trying to do in cyberspace. Countries need to have the capability, both the technical capability, law enforcement, computer emergency response teams, policies like national strategies to be able to engage in this area, but also on the policy side. To be able to engage in, for instance, UN and international discussions around these issues,

around norms for instance. Or to engage with the U.S. on these partnerships we're trying to build to go after shared threats. So, it's really important for lots of countries to be able to do this. And unfortunately, lots of countries don't have the capacity to engage in these things, and it helps the U.S. ultimately, if they do, because they can work with us on these issues.

And it's really something I've heard in the UN context and in the, what's called the Open-ended Working Group. Multiple countries, really every country that talked either said how valuable and important capacity building was or that they desperately needed it. So, if we're trying to, I think, really take the high road and help those countries to help us, but also trying to win those countries approval for our view of the internet, our view of cyberspace, the open interoperable secure world, and not the world of more closed systems, more controlled systems. Then I think it's important for us and really valuable for us to do this.

Now, this was a founding pillar also of my office at the State Department. One of the things we did from very early on was to do regional capacity building in Africa, for instance. That was one of the core things we did. And the State Department has continued to do that. It hasn't been resourced appropriately. It hasn't gotten the resources it needs, and it does need resources. We have – the U.S. has been playing and my organization, the Global Forum on Cyber Expertise, has about 60 countries. It has civil society. It has a number of private sector entities. It's a true multi-stakeholder group that is focused on coordinating these issues. So, it's been active in that organization and doing some of its own programs, but it needs the resources. It needs the people to be able to actually do this. And I think that that's going to pay dividends for the U.S. going forward again and again.

And it also helps us in another way, which is, one of the enduring issues is to mainstream this issue as a core issue of national security and economic policy, and ultimately of diplomacy, of diplomatic policy and foreign policy around the world. And the capacity building helps us do that too, including capacity building to help countries mainstream it within their own governments, within their own departments of state or their own foreign ministries. One of the things we did was worked with then Political Undersecretary, Wendy Sherman, have each of the regional bureaus do regional engagement plans around this, which included capacity building. To mainstream this as an issue. So, it really, I think provides this overall foundation for all the other good things on cybersecurity, on human rights, on economic policy we're trying to do around the world.

MONTGOMERY: Thanks. That's a great description. Laura, so we've talked about organizational structures, we've talked about strategies at State Department. We've talked about working with partners and allies in capacity building. What else is there out there that we should be thinking about? And specifically in the State Department, and maybe outside the State Department, to make sure that U.S. cyber diplomacy is positioned for success?

BATE: Yeah. So, there are two things in particular that I want to talk about, but before I do that, I want to just pull the thread on capacity building a little bit, because the Commission had a couple of recommendations there that I want to pull apart a little. As Chris said, and I can't emphasize that enough, the importance of capacity building just cannot be understated. We talked earlier about the value of building a coalition of allies and partners. Well, the stronger our partners are, the stronger that coalition becomes, the stronger we all become.

It is vitally important that we're enabling our allies and partners and enabling international governments to really practice good cybersecurity. It benefits us all. But one of the challenges that we encounter in the United States in capacity building is that our funding structures aren't really set up to give us much agility or flexibility with funding these activities. Internationally speaking, civilian cybersecurity agencies grew where they are planted. Their location speaks

more to the history of their development than it does any particular planning on where they sit or what they do. So oftentimes you see genuinely civilian cybersecurity functions housed within law enforcement or military structures, and a lot of the constraints on some of our capacity building funds, particularly the Economic Support Fund that enables a lot of these activities, is constrained in so far as it doesn't let expenditures go to programs that sit within those departments and agencies internationally.

So, what you see happening is this weird cobbling together of different funds to make sure that we're able to empower our partners and allies the way we need to, the way that we're able to build capacity, but pulling from this combined mesh of things. It works, it gets the job done, kind of, but it doesn't really give the agility that becomes so important to effective capacity building, which is really a critical national security function. So, one of the Commission's recommendations was to either figure out ways to make the Economic Support Fund, in particular, more adaptable to that, or if that's not possible, and legislatively that runs into some real challenges. The other option is to create a fund that really allows consolidated cybersecurity capacity building. It's a really important need.

But moving on from that, two of the things that I want to hit on before we wrap up today, one is resourcing. This comes up when we talk about the State Department's activities time and time again. Our cyber diplomats are providing the basic building blocks on which so much of the rest of our national security and our national cybersecurity is built on. It's just really not the place to cut corners on funding. It's not the place to cut corners on resourcing or on elevating the position. If we're going to do it, we've got to do it right, and that means not just setting it up effectively, but making sure as we go forward that these positions, these structures, and these people are resourced in keeping with the importance of the mission that they're facing. And last point for me is that the functions that we're seeing out of State Department really also touch on a lot of issues of coordination across government.

Interconnectivity of the issue areas has been a theme throughout this conversation, and we really do see that what is true in one department or agency touches on something in another department and agency. And so, a lot of what's happening outside of State Department impacts State Department's equities. With that in mind, it's really important that the White House is keeping those international engagement equities in mind when they're doing decision-making. The Cyberspace Solarium Commission emphasized, and has pushed for, and has argued and has really been supporting the position of the National Cyber Director, and this is part of why that's so important to us, because when you're talking about cross cutting issues across departments and agencies, being able to coordinate those equities at a White House level becomes really, really, really important.

So, as we look forward, as we look into the future, as the administration meets their legal obligations set out in the last National Defense Authorization Act to fill the position of the National Cyber Director. This will be one of those really important roles that that person fills, to make sure that that Cyber Ambassador is looped in and that State Department's equities come into those big decision-making roles across government.

MONTGOMERY: Thanks. One other thing I'd probably mentioned there is I think right alongside and integrated with the State Department is the Cyber Assistant Legal Attache, the Cyber ALATs, that are overseas. And I think we recommended an increase from six to 22. I think we've got it up to about 12. I don't know if there's just 12 out there yet. I think there's 12 appropriated. Getting that number up to provide that technical expertise to support our diplomats at the key posts overseas where it's needed would be another part of that.

PAINTER: Yeah, and let me just jump in on that too. I mean, that's on the law enforcement side, which is critically important. But also having, and this is something else we did during the time I was there, a cadre of trained diplomats at

posts who at least one of their jobs is to do cyber issues. And we were very successful in creating that and training people like Vint Cerf, Toomas Ilves, the former President of Estonia, talked to them, really giving them a background in it. But that network is really important because this is becoming a key issue around the world.

IOZZI: If I could circle back to Laura's point on resourcing also before we move on, because I think that it's just a really fundamental point, that we can create a new bureau, but the risk is that we create an unfunded mandate to do a whole range of work that frankly didn't exist in any way the same need the last time we even authorized the State Department. And so, the State Department, unlike, say, the Department of Defense, hasn't been authorized in over a decade and a half. So, if you think about how different the internet and technology looked a decade and a half ago, there's a whole lot of room for improvement in our engagement and it's a whole new need for diplomacy.

And I think we've been really hard pressed to a point at a pressing issue in foreign policy that's disappeared over the last decade and a half, but it's really easy to see this whole new area that has expanded. And that means that either we're not going to engage in that space or we're going to have to put more resources on the table, because it's hard to figure out where we take from and the internet didn't exist in the same way the last time we authorized. And so, I think it's, really, the challenge for Congress is going to be whether we can get consensus around funding this new foreign policy priority. And I think once a bureau is created, that's the first step, but how to resource it is going to be the second step. And I think that's probably going to be the bigger challenge.

MONTGOMERY: That's a great point. And I think the Department of Defense would say it is both a benefit and a burden to be reauthorized every year.

IOZZI: Fair enough. As a former authorizer, I think you can –

MONTGOMERY: So final question for Mark, and then Chris. And so, in your final question, any last comments you had, as Laura did already, that'd be great. So, Mark, you've already referred a little bit of this, but the Cyber Diplomacy Act, if it's passed, would require the Secretary to outline a strategy for how the U.S. engages internationally on cyberspace policy. Now, what sort of goals or plans would you be looking for in this?

IOZZI: I think the main point of the strategy is to ensure that the new bureau is thinking about, again, we said cross cutting over and over again I think in every answer to this, but that they're thinking about the full spectrum of what cyber diplomacy is and setting goals and objectives in each one of those spaces, and then coming up with a plan to achieve those goals. And that's really, I think, if you're not planning for what you're going to achieve in a new bureau, then you're going to be a little bit lost. And the lack of really foresight and planning was one of the things that we felt like has been missing for a long time. Without that planning, you can't engage at the right level to coordinate even within the Department, never mind with the other agencies.

So, I think it's about across all three of those aspects of cyber diplomacy, the big buckets of security, economic, and human rights, setting clear objectives for what we're trying to achieve in the diplomatic space, a clear plan to get there, and then assessing whether or not we're structured in a way and resourced in a way that's showing results. And if not, that's going to be a signal that we need to come back and revisit the authorities and the mission of the organization. So, I think we often talk about how, lament, maybe is a better word, how we're constantly tasking the Executive Branch, as Congress, we're constantly tasking the Executive Branch with coming up with strategies and reports for us to take all this time. But if you don't have a strategy for what you're doing, you're really lost as a bureau. And so, this shouldn't be an additional burden. This should be basic good governance.

MONTGOMERY: Thanks. That's great. So, I'll come here now to Chris. I'll have you close this out. Final question from us, and then any thoughts that you had. The question would be, part of FDDs work at the Center on Cyber Technology Innovation focuses on cyber-enabled economic warfare, and one of the norms it explicitly called out for in the legislation relates to the wrongfulness of cyber-enabled theft of intellectual property. In addition to diplomatic efforts, what tools do you think the government has and what role would the State Department have in an inter-agency of bringing these tools to play for underscoring the wrongfulness and the illegality of this kind of behavior?

PAINTER: Yeah, thanks for that. And that is a core norm, in my view, something that we really advanced and pushed in the agreement we reached in 2015 with China. Now, you can argue certainly that, that had an impact for some period of time, and that now has gone away. But we got that also endorsed at the G20, which I think is important, that theft of intellectual property to benefit your commercial sector is not allowed. But you also have to enforce that, and when we talk about any of these norms, any of these things we're trying to advance, this has to be not just thought of as this boutique cyber issue. We have to use all the tools we have to be able to achieve it. What I think helped in that case was then-President Obama said, "Look, this is not a cyber issue. This is a core issue of our economic and national security, and we're willing to take friction in our overall relationship with China because of it."

We need to be doing that with our relations with every adversary country, and even with our friends, saying, "Look, this is so important. We're going to lift it out of this cyber realm, which some people claim to not understand, and put it on the national security agenda. And we're going to make sure, we're going to use whatever tools we have with countries, with our partners, with our adversaries to make sure we get there." And I think that's going to be important. So yes, the State Department can play a critical role in that, to be sure. I'd also go back to Laura's comment about essentially having a seat at the table. One important thing that this role has to do I think, is to provide that diplomatic perspective to the inter-agency discussions. DOD, DHS, DOJ, all have lots of representation on these issues. Those are all critical parts. They even have some overlaps. DOD does a lot of things internationally. DHS just came out with an international strategy.

Great, but we need to be able to work together and coordinate those activities. That's something I used to do. I had inter-agency meetings once a month. But we also have to make sure that State has a strong voice when things are considered. When we're talking about response, do we respond using diplomatic tools, economic tools, military tools, or a combination? Well, it should be a synchronized combination, but State, again, has an important role to play there. And I just go back, Mark, to how I started. This is not this technical issue anymore. This is not this boutique issue anymore. This really is a core issue, not just in the future, but now for our economic and national security, and we have to treat it that way.

And so, part and parcel of that is creating this strong position at the State Department, mainstreaming it throughout the Department, making sure it's a recognized priority in our government, and the State Department has a significant role to play in those discussions. So, certainly, welcome to any efforts to achieve that. As I said, we're the trailblazers in starting that now 10 years ago. And it's unfortunate, I think we've fallen behind some other countries and we need to catch up. And we cannot just catch up, but, I think, spring ahead and re-assume that leadership role that we once had.

MONTGOMERY: Well, thank you very much. That wraps up a comprehensive review of what ought to be done in cyber diplomacy, both at the State Department and on the Hill. And I want to thank Laura Bate, Mark Iozzi, Chris Painter, and, of course, Representative Jim Langevin for their participation.