Center for Strategic and International Studies

Online Event

"Lessons Learned from a Cyberattack: SolarWinds Conversation (Part 2 of 2)"

Part 2: The Path Forward

RECORDING DATE:
Friday, February 26, 2021 at 12:00 p.m. EST

FEATURING:

Lieutenant General (Retired) Edward Cardon,
Senior Counselor, The Cohen Group;
Former Commanding General, U.S. Army Cyber Command

Jeanette Manfra,
Director of Government Security and Compliance, Google; Former Assistant Director for Cybersecurity, Cybersecurity and Infrastructure Security Agency (DHS)

Congressman Michael McCaul,
Ranking Member, House Committee on Foreign Affairs; Member, House Committee on Homeland Security; Co-Chair, House Cybersecurity Caucus

CSIS EXPERTS:

John J. Hamre,
President and CEO,
CSIS

Suzanne Spaulding,
Senior Adviser, Homeland Security, International Security Program,
CSIS

Glenn S. Gerstell,
Senior Adviser (Non-resident), International Security Program,
CSIS

Transcript By
Superior Transcriptions LLC
www.superiortranscriptions.com

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

John J. Hamre: Good afternoon, everybody. My name is John Hamre. I'm the president here at CSIS. And we are delighted that you are joining us for this very, very interesting conversation. I want to thank Suzanne Spaulding for creating this serious look into SolarWinds and what it says about America. And I will quickly turn to Suzanne. But I just would like to make just preliminary remarks.

It was now 23 years ago when I was the deputy secretary of defense. I disclosed to the American public that we had a serious cyberattack. Now, in retrospect at the time it was very naïve and innocent, but it was a serious issue for us. And my boss was pretty unhappy that I did that, but I knew there was no way to mobilize a department as big and complicated as the Defense Department to take it seriously. And it's gratifying to see how well we have advanced. But we still have massive issues and problems in this country and we're going to explore that today.

And so, Suzanne, thank you for leading this. And we look forward to hearing all of these wonderful panelists.

Suzanne Spaulding: Dr. Hamre, thank you so much for that introduction and for providing the historical perspective on today's conversation – reminding us how long we have been wrestling with this seemingly intractable issue. And thank you also, as always, for your strong support for these important conversations. Very much appreciate it.

Welcome, everyone, to part two of our conversation about the SolarWinds hack and related events. I am Suzanne Spaulding. I'm the senior advisor here at the Center for Strategic and International Studies for homeland security. And I lead the Defending Democratic Institutions Project. So part one of this program took place at the beginning of this week on February 22nd when I had the opportunity to talk with SolarWinds' new CEO Sudhakar Ramakrishna, who provided some interesting insights into how this hack played out in SolarWinds, what steps they took upon learning about the hack, and what subsequent steps they've initiated to reflect lessons learned so far.

He also provided some specific examples about the way government could more effectively work with companies like SolarWinds when they're subject to malicious cyber activity. If you missed that conversation, I'd

encourage you to go back and watch the video. I thought it was really enlightening.

After our conversation on Monday at the start of the week, throughout the week Sudhakar had several opportunities to testify on Capitol Hill, along with at least one of the hearings with Kevin Mandia and Brad Smith, and others through the week. So today we close out this week, and we hear from policymakers and experts about what they think are some of the important takeaways so far, and what we need to do differently going forward. It's a great panel and it includes two people with whom I worked closely when I was the undersecretary at the Department of Homeland Security – Congressman Mike McCaul, who was then chair of the Homeland Security Committee and still co-chairs the Congressional Cyber Caucus; and Jeanette Manfra, who was the assistant secretary for Cyber. Great to see you both.

Our panelists will get a fuller introduction from our wonderful panel moderator, Glenn Gerstell. But I get the pleasure of introducing Glenn. Glenn, I am really pleased to say, is a colleague here at CSIS. We were lucky to grab him. He is a senior advisor for the International Security Program. He has already written and spoken widely about the intersection of technology and national security and privacy.

Glenn, of course, served as the general counsel of the National Security Agency from 2015 to 2020. Before that, he practiced law for almost 40 years at the international law firm of Milbank, LLP, where he focused on global telecommunications and served as the managing partner of the law firm's Washington, D.C., Singapore, and Hong Kong offices.

Glenn served on the President's National Infrastructure Advisory Council, which falls within the organization that I used to lead at the Department of Homeland Security. That body reports to the president and to the secretary of homeland security on security threats to the national infrastructure.

He's a graduate of New York University and Columbia University School of Law. He's an elected member of the American Academy of Diplomacy and a member of the Council on Foreign Relations. He is a recipient of the National Intelligence Distinguished Service Medal, the Secretary of Defense Medal for Exceptional Civilian Service, and the NSA Distinguished Civilian Service Medal.

We are lucky to have him here at CSIS, and Glenn, I look forward to this panel discussion. Over to you.

Glenn S. Gerstell: Thank you very much, Suzanne, and thank you so much, Dr. Hamre, and to CSIS for this, and Suzanne, that was an excessively long introduction. We'll discuss it later.

One of the aspects about this panel is it couldn't possibly be more timely because just minutes ago, for those of you watching currently live, the House Oversight Committee and Homeland Security Committees just concluded seconds ago a hearing on this very topic, the SolarWinds hack. To address that in greater detail, we have three terrific panelists and I have the pleasure of introducing them. I'll try to do that in alphabetical order.

We'll start with Lieutenant General – retired – Ed Cardon, who is now a senior counselor at the Cohen Group. He retired from the United States Army as a West Point graduate and after 36 years of commanding troops around the world. I had the good fortune of overlapping with him when he served as the commanding general of the U.S. Army Cyber Command. And after that – undertaking that command, he had an exceptional job in the United States Army as being in charge of the transformational unit that set up Army Futures Command, one of the most important organizational changes in the Army in a period of decades.

Our next panelist is Representative Mike McCaul, whom I've also had the pleasure of working with when he was – when I was at NSA and he was the head of the House Homeland Security Committee. The congressman, who just suffered through, I guess, what, five days or so of freezing weather with no electricity and water in his home in Austin, is now in his eighth term representing the district in Texas that includes Austin.

He started his career in the United States Attorney's Office, was in the Department of Justice in Washington and the state of Texas State Attorney General's office, all of which gave him a long background in national and homeland security matters. He currently serves as the ranking member of the House Committee on Foreign Affairs. He's a member, as I mentioned, of the House Committee on Homeland Security and, as Suzanne also mentioned earlier, is the co-chair of the House Cybersecurity Caucus.

And then another former U.S. Army member, Jeanette Manfra, is the director of government security and compliance at Google Cloud. After serving in the Department of Homeland Security in a variety of significant senior cyber policy roles, she was appointed as the assistant secretary for cybersecurity at CISA, the Cybersecurity Infrastructure Agency. She left there at the end of 2019 to join Google, as I said.

So, with that, we have terrific panelists, and let's jump right into the questions. And maybe we can just start with the fact that we've all read the news. We've seen so many articles about this hack apparently caused by Russia, although there's been no formal government attribution to that. We just saw hearings a couple of days ago from the Senate Select Committee on Intelligence, holding a rare public hearing on this topic with representatives from cybersecurity firms, from SolarWinds and from Microsoft – actually, the heads of those organizations. And as I mentioned earlier, we just also concluded minutes ago hearings by the House on the same topic.

So with all this background, what we've learned so far – and we've learned a lot – I'd like to ask the panelists, do you feel that this particular hack has changed anything? Is this just something bigger, but it's more of the same? Is this qualitatively different? After all, no bitcoins were stolen. No blueprints appear to have been stolen. No data appears to be corrupted. So is this really something the same as what we've been seeing before but just on a bigger scale, or is this really different in some way? And, if so, how?

General Cardon, maybe I could start with you on that.

Lieutenant General (Retired) Edward Cardon: Thank you for the introduction, Glenn, and it's an honor to be here with all of you today.

Three points, maybe, on what you just said. First is, I do think it's different. We normally don't see software supply-chain attacks of this scale. The way I look at it, one intrusion, that's an incident. Eighteen thousand intrusions, that looks more like something very different. That's the first one.

The second thing, though, that I'm encouraged about is the information sharing, but it's also pointing a number of holes in the way we do this. So no one can see all the data. The government sees their data. DOD sees their data. Private industry sees their data. And there's all kinds of restrictions on this. So no one can see it all, and it's been quite an effort, both public and private, to put this together.

And the last one is, of course, these tools that started all this – (inaudible) – came forward in December. Given with all the other tools that have been taken over the years with these tools, what does that bode for the future?

And I'll stop there.

Mr. Gerstell: OK, good.

Congressman, your perspective from the government?

Representative Michael McCaul (R-TX): Yeah. And thank you, Glenn. Thanks to CSIS. I remember co-chairing the famous report that we came out with on cybersecurity. Gosh, it's probably like a decade ago. And what a great exercise that was.

Suzanne Spaulding, I just want to give a great shout out for her service at DHS. And her leadership on cyber was extraordinary, and it helped me to elevate the cybersecurity agency within DHS and authorize it into law. And I think it has really stood up as a great organization. Chris Krebs, of course, I thought, did a phenomenal job, who's now working for SolarWinds.

I have a little bit of an attachment to SolarWinds. They're in my district in Austin. And so when the breach first occurred, I was one of the first ones I

think they contacted. And I talked to, you know, the new president and CEO, Ramakrishna, about what happened.

And I think what is different about this, to the previous witness's point, the scale is so massive. And we still don't know what the damage is to this day. Also the type of malware itself was very sophisticated and very deceptive. It could literally enter into the system and leave without leaving any trace or fingerprints, if you will. The intrusions initially occurred in March of 2020 and lasted through June. It was not fully detected until December of 2020, at which time Microsoft developed the kill switch to basically take down the malware within two days, which was extraordinary, but by that time the damage has been done.

I don't think it was destructive in nature. I think it was more of a theft espionage type of exercise. And by all accounts, without getting into the classified side of things, I think Russia is – talk about attributions – very good assumption this is coming from Russia. And so there's so much more to talk about in terms of how we respond to all this. And I'm also – you mentioned Army Future Command. We're so delighted to have that in Austin, Texas as well. They're doing a phenomenal job.

But that's kind of my short take on SolarWinds.

Mr. Gerstell: OK, thank you, Congressman.

Jeanette, your perspective now that you're in the private sector?

Jeanette Manfra: Sure. And again, thanks for having me. Nice to be here with my former boss, Suzanne. And I think this might be the first event I've done with Mr. McCaul where he wasn't asking me questions from the dais. So – (laughs) – like him, this is less stressful.

Mr. Gerstell: And you're not under oath.

Ms. Manfra: Exactly. (Laughs.) So, you know, I think to your question about whether it's qualitatively different, I think it may be a little bit too soon to tell. This isn't the first supply chain attack. It's probably not going to be the last. I think what – for my perspective, what's significant about it, similar to other, you know, big incidents that the government has had to deal with, is it's a moment to shine a light on challenges in the – what I'll call the overall system. And you know, there's been – there's been a lot of talk about, you know, why our defense is, you know, there with information sharing. Why can't we detect these things?

And I think that's really important to talk about, like, building better cyber defenses. But I think for too long that's been sort of the exclusive focus. And there really needs to be more talk about, like, why is the system overall not more secure? And this is really one of the reasons, when I decided to

leave government and what attracted to me to Google, is, you know, the notion – both that obligation but also that opportunity to drive modern security architectures, to make sure that our overall software ecosystem was more secure.

And so I think, thinking about it, you know, from the government as a consumer of IT services and products, is what could we be doing to better modernize those systems to make sure that, one, technologically to have more of those security capabilities – those modern security capabilities, but also from an operational perspective. How the government thinks about risk overall needs to better include the risk of technology. And I think this is a really important moment when – that highlights that lack of – the lack of integration as government, and not just government but, you know, companies.

Everybody is sort of thinking about their dependency on software and infrastructure and being able to mature their understanding of how do they manage that risk not just from the technological perspective but from the entire organization's mission perspective. So I would say I'd love to see more of that conversation. And I think this really highlights – and is a moment where people can start to have those questions and those conversations across the public and private sector.

Mr. Gerstell: Thank you.

Well, all three of you have raised lots of good points, that – each of which we could probably spend half an hour or an hour on. Let me draw your attention to just two of them. During the hearings that we've had in the – in the Senate and the House, the witnesses talking about the SolarWinds hack made a point – they made two points, which I'd like to ask you all to comment on. One which – one is that during the course of the hack they were not able – they didn't think the private sector was able to quickly get threat intelligence information into the hands of government and the private sector quick enough to do something about it. So this hack persisted, evidently, for months. Of course, it was only discovered in December, apparently. But even then it was slow to really get dispersed. It took a matter of weeks.

And a number of the witnesses at these hearings have said, gee, we need some kind of mechanism to share threat intelligence in a very quick way to prevent a hack of this size from spreading. And then, secondly, the hearings brought out the point – and also the CSIS interview with the CEO of SolarWinds – brought out the point that although some 18,000 customers of SolarWinds evidently were potentially – had the malware implanted, or used the SolarWinds update to implant malware and sort of get a backdoor into company systems, only a much smaller number, perhaps just a handful of government agencies – still important – and perhaps 100 companies actually were victims of further exploration and exploitation, where the

attackers – again, presumed to be Russia – not only entered but then were able to roam around, so to speak, withinside the networks. And the point was made, normal cybersecurity programs and protocols could have stopped that further exploration.

So I'd like to ask the panel – and Congressman, we'll start with you on the government side – do you think the laws need to be tightened up, one, to require mandatory breach notification or to permit early threat intelligence warning without liability? And do you think we should have minimum cybersecurity standards of the sort that might have prevented further exploitation of this hack?

Rep. McCaul: Well, and thanks for the question, Glenn. That's actually one of the precise questions I asked the CEO of Microsoft, and it's the issue of breach notification and mandatory breach notifications.

When we set up CISA, it was done in a civilian space to be the – sort of the central clearinghouse for threat information as a civilian agency with the private sector. We had that bubble chart back in the day. We had NSA and DOD Cyber Command offensively, defending in a time of warfare; FBI investigating; and then DHS being the information-sharing mechanism. Brad Smith, the CEO – or president of Microsoft, agreed with me that he thinks it's time to have a mandatory breach notification system. Jim Langevin and I have always teamed up on these issues. We introduced, or are planning to introduce a bill on that, and I think that would go a long ways.

Now, some of this was, you know, reported early on, but some companies don't report this at all. And it's important we have that threat information to share it across – not only with all the private sector, where about 80 percent of this resides; across all of the departments within the federal government. And this can be done very easily, like what we do when we sanitize threat or classified information. You know, we take out sources and methods and we take out certain names. We would take out of the name of the company because the fiduciary duty to the shareholder and really just have the threat information itself: What is the malware itself? What are the ones and zeroes? What can we share that will not compromise the company who notifies the government about the breach?

I think liability protection is also something that we should be looking at so that there's – it's very clear that there will not be lawsuits. And that would encourage even more information sharing with the Department of Homeland Security and the federal government.

So I think this is going to – this is really ripe for legislation. And to get – to get that on the record from all of the witnesses being supportive of this law I think is a great step forward.

Mr. Gerstell: Thanks. And do you – do you feel we should go a step farther and also have government impose or industry impose in some kind of self-regulatory way minimum cybersecurity standards? Or should we leave that up to the –

Rep. McCaul: You know, I always like it to be more voluntary. You know, but we have the NIST standards. When they become just more of a check-the-box exercise, I don't think it's very meaningful. So if we do have a list of standards that companies would have to comply with, we'd want that to be very meaningful. And then I guess to your point – and I'd like to hear from the private sector as well – I'm sure they would prefer it to be voluntary, not mandatory.

But look, this world's getting more and more dangerous in the cyber space. And if the private sector can't do it on its own, we may have to look at mandating it.

Mr. Gerstell: Yeah. I think that's a – that's a great point, Congressman. I think the issue from my sense and talking to some of my colleagues is that voluntary standards are probably going to work for the very large, sophisticated companies that have the resources and talent – cybersecurity talent within the company to deal with that, but when you get into smaller companies, mid-sized companies – who, again, are part of the supply chain for the bigger companies, so it's still a vulnerability we need to address – I think that's where the problem is. And I worry that industry self-regulation alone may not be sufficient. The economic incentives probably aren't all that strong. It's not a profit center to spend lots of money on your firewalls and configuring your systems. So I think that's a problem that our – that the private sector needs to grapple with.

I'll just ask quickly, Jeanette, if she has a perspective on that now that she's in the private sector, and then we'll move on to other questions. And in fact, let me just mention to the audience that there's a Q&A function at the bottom of your screen, not the chat function. If you want to submit a question, we'll try to get to them at the end. But you can put your questions in the Q&A function at the bottom of your screen.

Jeanette, back to you.

Ms. Manfra: Yeah. I would say, as Representative McCaul mentioned, there are mechanisms for information sharing. And so there's, you know, some – maybe some potential to learn from it – you know, why aren't some of these mechanisms maybe working as well as they should? But they do exist. And so I think it's really incumbent on the private sector, and particularly large companies that have that visibility to continue to develop that relationship, as well as the government, of course. You know, my former agency has spent a lot of time working on building that out. And that, you know, there's maturing that needs to happen. And I know that new folks there are going to work on that.

You know, from my perspective, both from the government and from this side, information sharing is a little bit too broad of a term to get real action. And so, you know, really trying to drive down to, you know, what's the outcome – you know, what specific thing are we trying to avoid, and who has that information around intelligence and can get it to us, and really building those pathways so the government and the private sector are not just sort of having broad, general conversations about threat intelligence. Because there's really no sort of overall incentive, on either side frankly, to share much specific. But if we can talk about – you know, we're talking about specific scenarios here that we want to prevent, these are the types of companies that have that information. Let's build a model to get that information flowing back and forth.

So that's kind of on the information sharing side of things. I would say sort of the part about, like, talking about a little bit more on supply chain and minimum cybersecurity standards, I think that the standards are very important. And as you mentioned, oftentimes it's the very large companies who are able to fully implement that full breadth of the standards. But not exclusively. There are very small companies who are – you know, really prize and value the differentiation that security provides. I think we need more of that. But we need to also have it on the consumer side. So the government is a very large consumer.

They need to be, you know, driving what those security standards are that they want to see – through their procurements, through their, you know, whatever sort of mechanisms they have to purchase IT. And so I think it's really important to think about the economics and how do we drive more security through the – sort of the existing processes of, frankly, these large procurements. And I don't think, to Representative McCaul's point, there is – there's a bit of, like, checking the box on some of those things. And we need to – we need to mature that function so that, back to the risk point, is that you have your procurements thinking about the risks that that could introduce, and you're driving standards through those. But, yes, voluntary industry global standards I think are really crucial to solving some of these problems.

Mr. Gerstell: Thank you. Let me pick up on your point about incentives, which you mention in the context of the private sector and turn to Ed to talk about the government military side of things here for a second. There don't seem to be any real incentives – or maybe I should switch it the other way – there don't seem to be many disincentives for countries such as Russia to stop this kind of hacking. Let's assume, for argument's sake, that they were responsible for SolarWinds. But if it wasn't this one, they're responsible for others. And we certainly know from the five-volume bipartisan Senate report what they – what the Russians were up to in the 2016 elections.

So my question, Ed, for you is, one, if this is just espionage and nothing was stolen, nothing was deleted – let's assume that for argument's sake – so no physical, real-world damage, so to speak. And it presumably is the kind of thing that maybe our own intelligence community would like to do to the Russians. We can leave that unstated or unspecified for a minute. But what should our response be? Should we retaliate? How do we impose costs on them? And otherwise, they're free to do this with impunity.

And then an allied question, is it right for the private sector to bear the burden of foreign nation-state attacks? We certainly – if Russia sent over a missile, we'd know what our reaction would be. Why is it OK to let the private sector suffer a cyberattack? Ed, do you want to pick up that and then maybe then we'll go to the congressman? And, Congressman, I understand you have a vote coming up in a few minutes, so when you need to step out, by all means let us know. But if you would comment right after the general on this, that would be great.

Gen. Cardon: Thanks, Glenn. So maybe I'll start with the second one first, in that it's my belief that most private companies cannot effectively defend themselves against a nation-state, because the nation can – the nation-state can bring resources, time, other intelligence to bear that there's no way a private company can defense against. Many have done well, but if it's a determined actor and they have a lot of time and they're determined – as, you know, we often talk about, defense has to be right 24 hours a day, seven days a week, 365 days a year. Offense has to just get lucky once. And so that's that part. So I think there has to be help from the attribution side.

Now, to your other question about –

Mr. Gerstell: Can I interrupt on there for a second? One of the things that some companies talk about is the right to hack back. How do you feel about that?

Gen. Cardon: I worry about the second- and third-order effects of that, because I think one of the challenges we're having – and even in the discussion here – is we put the espionage in what I would call a 20th century frame, not a 21st century frame. And I'm not sure that, you know, we say, well, it looks like espionage. It looks like espionage, but it may take us years to figure out, OK, in these companies what are they, how does that impact others, what part of the government are they in, how long is it going to take us to find out? And then if something happened, it can turn into a destructive attack at the worst possible time. And then we'll have to say, well, that was a bad decision four years ago.

And so we struggle with this. I mean, I know numerous administrations have talked about retaining all options. Each one has to be looked at on its own merits. I think the FENN (ph) Board is a start. But I think one of the challenges we have is, you know, like, even SolarWinds, widely reported to be Russian. Still working on a sure attribution, right? And so there is an

element of truth to this. So I think, picking up on what Jeanette said, you know, info sharing is a pretty broad term. But just, like, just simple things like, for us, worldwide collection of DNS logs. I mean, it's amazing how if we could just do that, we could do a lot with attribution. But often those are missing, they're not collected, etc.

And so I think each case has to be done on its own merit. But I don't think that this could be looked at in solely an espionage frame, because you're making assumptions forward that it will not evolve into something else. You're almost trying to prove an unknown unknown.

Mr. Gerstell: Right. Well, thank you.

And maybe I can just jump in with a quick comment before we go to Representative McCaul. But I think that if it's just purely espionage, so to speak, traditionally we've dealt with pure espionage in spy channels. In other words, if we catch one of their double agents, we kick out one of ours – or, we kick out one of theirs. And so the retaliation occurs within intelligence channels. That seems to be a little different in the cyber world. And I notice that Brad Smith from Microsoft the other day in the hearings, as well as some government officials, have started to delineate a little bit of a difference in this particular act, even if it is – even if it turns out to be pure espionage, by talking about the broad scale of it and the reckless nature of it.

Namely, using a supply chain mechanism in a sort of indiscriminate way to get into a very, very large – in this case tens of thousands of companies. And somehow that's a little different from tailored, targeted espionage. So maybe there's a legal basis for creating an ability to retaliate against this kind of, quote, "espionage," as opposed to old-fashioned just snooping around. Congressman, do you have any thoughts on that, and whether it's right – back to my earlier question – for the private sector to bear some of this foreign nation-state burden?

Rep. McCaul: Well, I agree with the general. If it's a nation-state – a foreign nation-state adversary, I think the United States government has a duty to assist and respond. You know, these questions, interestingly, going to – we discussed this with Jim Lewis at CSIS, you know, 10 years ago. We don't have a definition for cyberwarfare. What is cyberwarfare? What constitutes an act of cyberwarfare? What really is cyberespionage? Why don't we have any international norms and standards out there?

I think in this particular case it would make sense to coordinate with our European and NATO allies, and for us to look at sanctions. But this gets – this subject matter gets a little tricky, because as you know, there are certain things that we do in the classified realm to get information about our adversaries. So when you get into this international framework – and this is precisely – and it's great timing. And I passed just yesterday my

Cyber Diplomacy Act bill. The missing piece is always – you know, we had DHS and CISA defending the nation, and DOD in a time of warfare standing up, and FBI investigating, and CISA sharing the information. What's always been missing, though, is this sort of ambassador-like position on cybersecurity that can negotiate with other countries, and allies particularly, certain norms and standards within cyberspace. We don't have that right now. And that's what the bill is designed to do through the State Department.

I think it will deal with the issues you've raised. And I think there are certain points of you're crossing the line too far. I think certainly a very – highly destructive attack, like the NotPetya attack, I think that's getting closer into cyberwarfare. But we have to define that legally as well. And I think a destructive attack like some that we've seen would warrant a proportionate response if there is a cyberwarfare attack and cyberwarfare, and kinetic response as well. And I think some of that was defined under the Obama administration about a proportionate response to the attack. And I think when you get into espionage, it does get a little more tricky because, you know, we're engaged in certain activities ourselves and we don't want to weaken those strengths that we have.

But this is all so cutting edge right now and still not well defined. And I really think this is the area that CSIS – would love to continue to work with you on this, because this is the really undefined area both of the law and also internationally, where we need to have certain standards and norms internationally, and right now we just don't.

And so, like you said, Russia with impunity can attack us. China can, you know, steal all this intellectual property. That's why we shut down the Houston consulate, because they're stealing, you know, the vaccine. They're stealing research from Texas Medical Center, NASA, with impunity and with no response. Remember, they stole 23 million security clearances from OPM and there was no consequence to that action.

You know, my five kids, bad behavior, there are consequences. In the cyber realm internationally, when a country does this and there are no consequences, then the bad behavior continues. And I'm afraid that's what we've seen. And it's getting worse.

Mr. Gerstell: Thank you. I agree with your comments and I also applaud the moving along of your cyber-diplomacy bill. I think having an ambassador-level person at the State Department to help coordinate the international aspects of this will be key.

Let me ask the congressman, just if I can stay with you for just one more second – I'll ask Jeanette to comment as well – do you think the U.S. should join the Paris Call or take other steps in a formal way in international law to outline what exactly should be illegal in cyberwarfare? And do you think

that's a good approach, or should we keep it sort of informal and you know it when you see it, giving us more flexibility to act when we want? What's your sense of that, sir?

Rep. McCaul: You know, I think this is such a cutting edge and so ill defined, if you will, that we need better definitions. And I do think a more formalized process like a Paris Accords type, you know – I mean, we did this with climate change. Why aren't we doing this with cybersecurity?

I would like to, when we pass the Cyber Diplomacy Act, be able to have the State Department and DHS and the Cyber Command within the DOD all come together with our – starting, really, I think, with our NATO allies, because our NATO allies are under threat every day from the same foreign nation-states, particularly Russia, China, Iran, North Korea.

And that would be a great starting point to come forward with some of these definitions and some of these standards and norms that then eventually we can put in MOUs and agreements with – and I think starting with our NATO allies is a good place to start so we can have some standards and norms and agreements, and possibly even negotiate treaties with countries down the road. That may be something that we'll be looking at down the road as well. But I think it's way overdue, and it is high time.

And I think SolarWinds is another wakeup call, and it's not going to be the last one. You know, we're going to continue to see this as long as we don't have any consequences to these bad actions.

Mr. Gerstell: OK, thank you. I completely agree. And I note that the United States is an outlier in that it has not joined the Paris Call. I understand the rationale was in part that if we signed and countries like China and Russia did too, we would be obligated to honor that, and we would. But those countries wouldn't, and so we'd have an asymmetry there. That's certainly an important point. We'd want to make sure we didn't tie our hands back and unilaterally disarm. But by the same token –

Rep. McCaul: And that's why I get back to the espionage question. That's precisely, I think, the issue at hand on the espionage. I think that you're right, that would be more difficult.

Mr. Gerstell: Yeah.

OK. Jeannette, I wanted to come back to you.

Ms. Manfra: Yeah, that was a lot. I think I want to sort of – back to what General Cardon said, the notion that we're trying to use 20th century mindsets and thinking and strategies to apply to a 21st century problem, and what the – and Mr. McCaul talked about and sort of the definitions is, you know, we do seem to be sort of stuck in a – and, particularly, I think, the government often is,

well, this is how we thought about airspace and this is how, you know, we thought about the Navy, and then we're going to – we're just going to apply that to cyberspace.

And I would venture to bet that, like, if you put five people in a room together and asked them what the definition of cyberspace was they would all have different definitions. So even at that level is, you know, what are we talking about specifically is – can be sometimes a challenge. And then it's – cyberspace is not some separate domain that exists outside of, you know, our physical reality. And so, but it is unique, and that part of the uniqueness of it is we can't just apply this is how we achieve strategic air deterrence, let's, you know, apply that to this new domain. And that requires a lot of creative thinking and a lot of different approaches.

It also – and it just requires a level of, like, coordination and, like, joint operational almost with nongovernment entities that is really challenging to actually execute to any success. And I still think the government and the private sector, they need to continue to reorient around a new relationship in kind of jointly managing the – you know, frankly, the sustainability of this technological ecosystem that we've built.

And so I think, and I love that, you know, the cyber diplomacy work. I think that's so important and, you know, thinking about, like, what are, like, norms of behavior in this sort of 21st century world and how do we encourage others to participate in that. But I also think, you know, the U.S. has to – has an obligation to be a leader there as well, and I still think there's a lot of work to be done inside of government in terms of balancing intelligence, operational, and defense priorities, that it's really got to be sorted out and before, you know, the private sector can kind of come in and help.

But that being said, the private sector has a tremendous amount of, you know, opportunity, I will say, to be able to provide a more secure foundation upon which the rest of the world can be operating on. And so I – you know, I think, at Google we take that very seriously and we pushed, whether, you know, through open source or other sort of – or other forums or through our own products, and we want to see more of that. We want to see everybody be able to take advantage of the investment and the modernization that the large, you know, tech companies can do for security, and have less and less of the onus on smaller organizations or individuals.

It's a long journey. But I think this – you know, this could be a moment – this, combined with, you know, elections and, you know, the various other things that have happened, is I think you're starting to see people really wake up, is we have to think differently and, like the general said, we have to have a 21st century mindset in how we're solving this.

Mr. Gerstell: Great. Thank you. Lots of good points.

Congressman McCaul, are you still with us for another five minutes or so?

(Pause.)

I don't know if he stepped out. I know he had to vote.

Rep. McCaul: No, I'm here.

Mr. Gerstell: You're here. OK. So let me just quickly go to you and then to – and then to Ed, just to take advantage of the fact that you have to leave in a minute.

Do you – do you sense that the executive branch is organized the right way to deal with the threat we've now just been describing for the last half hour, this vast threat? We've got a new national cyber policy director as a result of a provision recently enacted into law. The Biden administration has not yet – I believe not yet nominated someone for that. There are lots of cyber – senior cyber roles scattered throughout DHS, the Department of Commerce, the Pentagon – we're going to come to Ed in a minute on that. Is the executive branch organized the right way? And then, just quickly if I can sneak in a second question, how do you feel about Congress on that point?

Rep. McCaul: Well, you know my views on Congress. I mean, the Committee on Homeland Security, I came very close to fixing the jurisdiction of that committee. And as Suzanne will tell you, it takes an enormous amount of time from the Department of Homeland Security to appear before the hundred-plus committees and subcommittees, and it's absolutely – you know, and I came very close to fixing it.

But moving on to the bigger question, I do think this is all, really in the time that our report came out with CSIS, has really been evolving. And you know, clearly-defined roles I think are important. We did recommend a position in the White House to elevate the cybersecurity mission in the White House. CSIS did in their report, and that was very important with Langevin, Jim Lewis, and myself. The Obama administration, to their credit, elevated it and put that position in there. Unfortunately, the previous (sic) administration took it out. I'm pleased to see that the Biden administration is putting that position back in to elevate the cyber mission within the White House to oversee.

But again, I think, you know, going back to the original what they called the bubble chart – I'm sure the people in pioneer days, what is the role of the federal government? What is DOD's role? Some people thought NSA should be the information sharer with the private sector, the defense industrial base pilot program. And then we had Snowden, and then we thought, no, we need a civilian agency so we don't have those kind of optics, and DHS was the obvious go to.

And then we created CISA. And I think CISA has really risen to the occasion. It was pretty rocky in the beginning. They had a lot of learning curves. But they have really come a long ways in their sophistication.

And again, I think the missing piece that I see within the federal government is the cyber diplomacy mission; and our ability to negotiate and coordinate with our allies, and particularly NATO; and, you know, what can we do within the global framework to our enemies when a very destructive attack occurs. And those parameters need to be set forth. They need to know that if there is a destructive attack against the United States there will be a proportionate response back, not unlike what happened yesterday when the Shia militias were bombed in Syria.

You know, they hit our embassy in Iraq, and if we don't respond then we're – you're operating out of weakness, not strength. And I'm always for a strong response to a strong threat, and cyberspace is no different. If we have a strong attack against the United States or our interests, then I think they need to know and we need a framework that's international that the response is going to happen and you're going to get hit back. If you steal all these security clearances, there will be a response. There's not going to be just a meeting; there will be a response. If you – if you destroy the power grid and shut it down, there will be a response to that. And that's what's uncertain right now in the global – in the global perspective that I think we really need to focus on right now.

Mr. Gerstell: Good. Thank you. I very much agree with your comments.

Ed, let me turn to you for your perspective as a former military officer. But how do you feel about the issues the congressman has just raised? And in particular, what really should be the role of U.S. Cyber Command and NSA in addressing this? Should they be in the background? Should they have a – more of an aggressive position? As you know, NSA over the past year has a new cybersecurity director which is working quite closely with the defense industrial base to help secure them. Should that role be expanded? What's the role of the military in this picture?

Gen. Cardon Originally, when Cyber Command was created, you know, it was very much focused just on the military, DOD. And when we set up Joint Task Force Ares against ISIS, it started to expose a lot of cracks in the way that this was organized. But I will say to the congressman and to Jeanette's point that there has been huge growth in this area, and the Solarium Commission also did a lot of work in this area.

So back now to the role of Cyber Command and NSA. I think their role is spelled out, but, much like we have with the National Guard in this country, you can provide military support to civilian authorities. And so they can ask for help, because one advantage the department has is it has a Cyber Mission Force, right. CISA doesn't have a Cyber Mission Force. They don't

have 6,000 people that can be deployed for very unique, specialized situations.

Now, the rules to do that, how that will be done, all that would have to be worked out. But I think clearly this goes to – there's not a defined line between government and commercial networks. I mean, many government networks are commercial networks. So this idea of, oh, it's very easy to describe this, it's not so easy. And this is why we tend to evolve down more to how do we share information and then how do we share that protection.

Rep. McCaul: Hey, Glenn, I'm going to have to unfortunately leave. But I want to thank you for having me.

And to the general's last point, you know, when I was meeting with my Texas Guard in Austin at Camp Mabry, what I think is really a really interesting idea is you have these tech – you know, they're like, you know, daytime techies, you know, that work in the IT sector, but they joined the National – they joined the Texas Guard.

So I think what the general is talking about is really kind of another cutting-edge thing that's happening right now within the military where you have basically full-time – because they're the civilian Army, essentially, right. Their daytime job is doing tech, but they're part of the Guard. And I think that's an excellent role for them to play.

And so – but I apologize. With that, I'm going to have to do my constitutional duty.

Mr. Gerstell: OK, thank you so much for joining us. We appreciate it.

Ed, were you – did you have a further comment on that, or no?

Gen. Cardon: No, I was –

Mr. Gerstell: OK. OK, we've got a couple of – we've got quite a large number of questions coming in. And again, there's a Q&A function on the bottom of your screen, not the chat function. I'm going to try to consolidate a couple of these questions into one or sort of pick out a few.

There's a couple of questions having to do with one of the recommendations of the Solarium Commission, the Cyberspace Solarium Commission, about having some kind of mandatory equipment or software certification system to help deal with the supply-chain vulnerabilities, and a related series of questions about how private-sector companies can manage a multiplicity of third-party cybersecurity vendors and how that needs to – how that needs to be addressed.

Jeanette, since you have the advantage of being both in the – both at CISA as well as now currently at Google Cloud, what's your sense of what we need to do in terms of equipment and software? Do we need something equivalent, like an underwriters' laboratory, before we plug anything into the internet?

Ms. Manfra: So I would say to – I think we kind of need to separate the different types of technology we're talking about. On your point about the underwriters' laboratory in particular, I would say sort of like consumer devices; you know, your nest in your home or, you know, the various different – your smart refrigerator, all those sorts of things.

I do think that it would be useful – and it's something I worked on when I was in the government to try to make some headway there – of, you know, being able to make sure that what is sold to the consumer for these, you know, sort of – the digital device that, you know, you could have some sort of physical consequence, if you will.

You know, I think it gets much more complicated when you start talking generally about software and even some of the underlying infrastructure. I think it's – I think it gets much more complicated to contemplate, like, a mandatory set of things that anybody and everybody who builds software should do, part of which is because you're going to shut a lot of people out of the market. And one of the great things about, you know, our technology industry is all the innovation and really is, you know, allowing the United States in particular to benefit economically for all of that innovation.

And so I don't think you want to shut that down. I think instead you want to think about how do you encourage secure software-development life cycles. And NIST has published some work around here. And, you know, it's something that at Google is just, like, amazing to me to see, like, how that is really just, like, designed into the entire process. And I know other – you know, other companies do the same. But, you know, what is it that, from a say NIST perspective as a well-respected standards organization globally, you know, there's, like, potentially opportunities to drive more security best practices, I think, maybe even standards might be too strong of a word yet. But how do get more of those best practices?

And I know I keep harping on this but, like, we need to have, like, the buyers demanding these things. And, you know, right now you have a lot of companies that they just don't see the need to invest in having that security. When a bug is identified they'll patch it, they'll fix the bug – or maybe not. And so we need to have a much stronger sort of demand on the buyer's side. And the government is just in a really powerful position to be able to do that, just given how much they acquire. All governments, really.

So those would be kind of some of the things I would think about. There's also, you know, sort of a broader resilience of the entire system question.

The internet and how it was able to flourish, and the many great things that enabled that, are also many of the reasons that we have these problems. And so thinking about how do we understand those points of fragility in how the internet is designed, talking previously about how, you know, an attempt at espionage could have potentially destabilizing impact. WannaCry, another example where, you know, the adversary may not even have the intent of having a deep destabilizing impact, but just the way that things are glued together is that is increasingly a problem and as more and more organizations become dependent.

So I think, you know, thinking through how do we, you know, incentivize more security software development, how do we start to, you know, think about if you're a smaller company, I'll be honest, like a lot of companies need to be outsourcing more of their capabilities and not trying to, you know, build and run everything internally. So think about how you can reduce your costs and improve your security by outsourcing more. Those are some of the things I think I would say off the top of my head.

Mr. Gerstell: All right. All good thoughts.

I certainly think you're right that we need to either provide economic incentives or regulatory requirements in order to change behavior. I think given the relative newness of all this technology – after all, the internet is sort of fundamentally about a generation old, under 20 years old, right? The iPhone is 13 years old. I don't know, YouTube is 14 or 15 or so. It's no surprise that this started off with light regulation, and we're now – as we – as problems become manifest, we move into a position of heavier regulation of technology. That's always been our pattern of regulating technology.

Let me ask – I'll ask Ed just to comment generally on these points. But let me – given that we're out of time, unfortunately, because we could spend hours on each one of these points – let me just ask Ed to comment specifically on what we've been talking about, but then go back to him and then to you, Jeanette, for a wrap-up question of – which I'm going to try to wrap up a number of the audience questions all having to do with the theme of: Are we just doomed to this type of problem? It's a cat and mouse game, or an arms race – cyber arms race – pick whatever metaphor you want. And we're just doomed to it because of the inherent nature of the internet? Or is this something we will be able to surmount and get a handle on? And if so, how?

A big question, but, Ed, let me turn to you, back to Jeanette. And then we'll have to, unfortunately, wrap up the program there.

Gen. Cardon: OK. I don't think we're doomed. I don't think that – I do think it's a competitive space. And as long as we keep that in mind – but I see the defense getting a lot stronger. I think there's a lot of new technologies and

concepts on the horizon. I mean, NSA just announced today the zero trust document. If you haven't seen it, I mean, that's going to help a lot of with ransomware to shut it all down, if everybody actually did it. So those sorts of things, I see that better. But the idea that it's going to go away, that it won't be competitive, I don't think that's going to happen. But I think we're not doomed. I think there's a lot of exciting things on the horizon here that could help.

Mr. Gerstell: Quick question, do you see us developing an alternate internet, some other – some other more secure, authenticated thing? Or are we living with the one we've got?

Gen. Cardon: I'm actually more worried about it splitting apart because of what China's doing and what we're doing. I sort of – all of what Eric Schmidt talked about, right?

Mr. Gerstell: Right, on our way to the splinternet.

Gen. Cardon: Yeah.

Mr. Gerstell: Jeanette, very quickly?

Ms. Manfra: I do not think we're doomed.

Mr. Gerstell: OK.

Ms. Manfra: I think we are – we're putting too much on the defenders, and they're defending something that's nearly indefensible, and so we've got to build a better mousetrap, if you will.

And so I think that on an alternate internet, you know, I think – I think the internet is undergoing a pretty drastic evolution right now. And I think to the point about splintering or not splintering, that is – it's undecided, and I hope it doesn't. And I think it's really key for the government to understand what the economics of the internet ecosystem is and how can they shape it to a way that kind of gives us – keeps all the things that we love about it while building it more secure and safe.

Mr. Gerstell: Well, I'm sure the audience appreciates that we've only been able to skate across the surface of a very wide range of topics with some fabulous experts today. So let me thank our panelists. Thank you and the audience for your attention and your great questions. I wish we could have gotten to more of them, but I know we'll have more programs on this topic.

Suzanne, let me hand it back to you with gratitude to you, Dr. Hamre, and CSIS for organizing this.

Ms. Spaulding: Glenn, thanks so much. That was terrific, and I want to thank our wonderful cyber leaders for this great conversation. I learned a lot this afternoon, including, as Glenn said, one of the things I learned is that we didn't leave enough time. We didn't schedule enough time for this great conversation. But I'm encouraged by Congressman McCaul's request that CSIS work with him on things like international norms; Jeanette's suggestion that we need to do a better job on defining our terms, working on a lexicon; and General Cardon's optimism about where we're headed.

So we have our marching orders, and we will absolutely continue these conversations. And thanks to all of you who have joined us this afternoon. Take care.

(END)