FDD EVENTS

Thinking Forward After the NSCAI and CSC

Featuring Rep. Mike Gallagher (R-WI) and Eric Schmidt
Moderated by Ylli Bajraktari and RADM (Ret.) Mark Montgomery

MONTGOMERY: Good afternoon, everyone. My name is Mark Montgomery, the former Executive Director of the Cyberspace Solarium Commission and the current senior director of CSC 2.0. I'm joined by fellow moderator, Ylli Bajraktari, former Director of the National Security Commission on Artificial Intelligence and the current President and CEO -- a much better title than mine, I think -- of the Special Competitive Studies Project.

I'm grateful for our two speakers for joining us today to touch on the roles of the government, the private sector and academia and what they do in shaping emerging technology policy. These were two of the co-chairs of the two most influential commissions on U.S. technology policy, and they can also provide valuable perspective on the role of congressionally-mandated commissions and the decision-making processes.

So first today, we have Dr. Eric Schmidt, who served as co-chair of the National Security Commission On Artificial Intelligence and serves as the Chair of the Special Competitive Studies Project, an initiative that continues the A.I. Commission's work to make recommendations to strengthen America's long-term competitiveness in artificial intelligence and other emerging technologies.

Dr. Schmidt also has a distinguished career as a technologist, an entrepreneur and a philanthropist, nobly serving as Google's Chief Executive Officer and Chairman, as well as Executive Chairman and Technology Advisor and also later, as Chairman of the Department of Defense's Defense Innovation Board.

Thank you, Eric, for coming here today.

We're also joined by my recurring boss, Representative Mike Gallagher, who served as co-chair of the Cyberspace Solarium Commission with Angus King. He continues to serve as co-chair of CSC 2.0, an initiative that works to implement the commission's recommendations. As a secondary assignment, he works in Congress, serves as chairman of the House Armed Services Subcommittee on Cyber Information Technologies and Innovation, and more recently, as chairman of the Select Committee on the Strategic Competition to the United States and the Chinese Communist Party, and he sits on the permanent Select Committee on Intelligence.

Thank you, Mike, for being here.

This event today is sponsored by the Special Competitive Studies Project and the Foundation for Defense of Democracies. Both are nonpartisan, nonprofit research institutes here in the D.C. area. Ylli and I'll lead a discussion for about 40 or 45 minutes, and then we'll take a question or two from the audience.

Ylli, over to you for some opening comments, and then to questions.

BAJRAKTARI: Thanks, Mark, and thanks for everyone for joining us today. Representative Gallagher, thank you for joining us. Eric, always good to see you.

I'm Ylli, as Mark mentioned. I had the pleasure of serving as the executive director of the A.I. Commission.

I always like to start by saying that about four years ago, I think our Congress really understood the importance of time that A.I. was coming to us, and I think they saw this based on two trends. One was every conversation with private-sector people, to include Eric and other tech leaders, was that they saw a powerful technology coming and yet, we in Washington were not organized for this competition. And secondly, I think our Congress saw that we're facing a competitor in China that is organized, that is well-resourced, has a clear strategy. They understand the importance of A.I.

And so with those two factors in mind, they created the A.I. Commission that I was, you know, honored to serve in, and I had the pleasure of meeting Mark not just because we were physically next to each other as offices, but nobody's born to lead these commissions. You learn by doing it, and we learned so much from each other.

And I also want to think Mark for his service to our country as a Navy officer, so thank you for that, Mark.

I want to start the conversation by asking first Eric, and then Representative Gallagher on why they thought it was so important to serve in these commissions at that critical time. Eric, I always remember the story you tell about your trip to South Korea and the famous game, AlphaGo, and why you thought A.I. was such a powerful technology. And then the second question is why you thought it was important to serve in a commission like this. This was not your first serving our country. You served on the Defense Innovation Board before that, and then Mac Thornberry invited you to serve on this commission.

SCHMIDT: Yeah. So I am enormously grateful to the Congress for getting me into this position. It's strange that when the government calls, you're actually grateful that you get the call, and in my case, I really am.

I started because the Defense Department asked me to create this Innovation Commission, and I knew very little about the military and didn't particularly care for it, and I've fallen really very much in love with the people in the military, and I don't like most of the rest of what they do. So I've committed to try to, sort of, help the leaders of the military, who I have enormous respect for, to fix the internal processes, make it state-of-the-art and so forth.

Then what happened was Mac Thornberry and a number of other people asked me to work on this A.I. commission, and there was this sense that A.I. was coming along and that Washington knew nothing about it, which I think is roughly correct. And that's also because A.I. is really software, and Washington is typically behind in software. And I can talk about that.

So a simple, sort of, defining moment for A.I., which is what you're asking about, is DeepMind had come up with some new algorithms which are called reinforcement learning, and I figure they sounded pretty interesting. You know, I get pitched a lot of interesting ideas, as everybody here in the room does. And we show up in South Korea to play the best Korean player -- his name is Lee Sedol -- and they have a new algorithm, and everyone believes that the computer will lose because the computers have never beat in the game of Go, which is a very, very complicated multi-state game. And as the game proceeded, all my Korean friends who are -- became mute as it was very clear that the game was being played in a different way.

We subsequently did the same thing in China, where the Chinese, who are far more arrogant than the Koreans, I might say, were absolutely convinced that they win. And as it became clear we were winning, they actually shut down the feed to 200 million Chinese people so that they couldn't see the Chinese person lose.

Google decided after that win to simply retire. You know, when you have won everything, just stop. Because you might lose after that.

(LAUGHTER)

But it's an example of the power and the insight of these technologies today. I don't need to remind you what's going on with things like ChatGPT. And we can talk about that.

I've had the pleasure of working with Congressman Gallagher, who is, sort of, this, sort of, young force of nature in these areas, right? So I think the tie between the two groups and what we're doing now is remarkable.

BAJRAKTARI: Representative Gallagher, I think what made Cyber Solarium so powerful was your service in it and your passion for cyber-related issues. The risk in the cyberspace has evolved in the last three years. So what made you serve on the commission? And how do you see the risk evolving over time?

GALLAGHER: Well, while Dr. Schmidt's being incredibly nice and generous, but we have to be clear. Whereas Mac Thornberry and others sought out Eric Schmidt to serve because he's Eric Schmidt -- he's, like, the smartest guy in the world on these issues, the only reason I became chairman of the Cyberspace Solarium Commission is because nobody else knew that it was happening, and...

(LAUGHTER)

And Senator Sasse texted me saying, "You have to be part of this." Because he passed the legislation. And because it was called "Solarium," it evoked one of my favorite historical case studies, the original Project Solarium in 1953, which I wrote my dissertation on. So I got suckered into doing it. And then I just texted Paul Ryan, who was speaker at the time, and I said, "Hey, I'd like you to choose me to be on this commission."

(LAUGHTER)

And Paul Ryan's response was "Nobody else has asked me."

(LAUGHTER)

"So you can do it." So that was the history of how I became...

SCHMIDT: Never volunteer.

(LAUGHTER)

GALLAGHER: ... involved.

I would also note, you know, now that I chair this Select Committee on the CCP, I'm involved in this process of trying to convince people, or compel people, to testify. Eric was the rare person who was very eager and willing to testify before our committee. He did so a couple weeks ago, and it was phenomenal. I would commend his testimony and his related article about innovation power, which was published in Foreign Affairs recently.

So thank you for your willingness to engage and your leadership.

As we went through the committee's work, I think the evolution, at least for me, was -- like, if you read the opening part of the report, it talks about, I think, NotPetya -- well, it starts with a dystopian fictional future scenario that we thought would be an interesting way of bringing readers in. But then we talk about NotPetya, which reflects, sort of, the obvious focus on Russia, and then the, sort of, report then goes to talking about China as our biggest competitor in cyberspace.

And I think that's largely still true. But by the time the report and our work was wrapping up, I started to gain a more profound respect and appreciation for, and concern with, a lot of the vulnerabilities we have in terms of our critical infrastructure here domestically. Put differently, I thought that the infrastructure we had to shore up was defense infrastructure, or defense industrial base infrastructure, and it is.

But as I went down the Cyberspace Solarium rabbit hole, I became aware of vulnerabilities we have in very interesting places that we tend to ignore, like water utilities that just don't have resources that they need to defend themselves. But it could be enormously destructive if someone hacks a water utility and messes with the pH balance and thereby -- even if you just put a question mark in people's minds about the safety of the water coming out of their sinks every day, you've had an enormous destructive impact.

And then I started to think about the things I'm obsessed with from a military perspective, which is, you know, how do we deter a war across the Taiwan Strait? How do we help Taiwan defend itself?

And the more you study that problem, or the more time you spend with Mark Montgomery, because he is truly obsessed with it...

(LAUGHTER)

... the more you realize that it isn't just a matter of the anti-ship missiles we sell to Taiwan. It's a matter of the cyber resilience of key domestic infrastructure, or the airports of debarkation, or the seaports of debarkation that we need to surge men and materiel west of the International Dateline if things start to heat up -- or the cybersecurity of Guam, which would be a target in any kinetic scenario over Taiwan.

So it was a very intense process. It was a great learning process. And I'm very glad that I got fooled into sending Paul Ryan that fateful text message five years ago.

SCHMIDT: Can I add, Congressman, you're going to be doing Cyber Solarium Commission number three? Because the scale-up of offense technologies, primarily due to A.I., we can deter it for a while, but eventually we're going to have to be resistant, eventually, to non-state actors who will have extraordinarily asymmetrically powerful weapons. And so I would say that you will either drive this or you'll find your replacement. But we're not done, right?

That's what I learned in this process. It's going to get -- the defense of the nation is very important. You understand this.

GALLAGHER: I'll make a deal. If you do A.I. Commission number two...

(LAUGHTER)

... I'll sign up for Solarium Commission number three.

(LAUGHTER)

And if they sign up to be executive directors again...

(LAUGHTER)

But your point is very well taken, and very well said.

BAJRAKTARI: Thank you. I told Mark this is going to be really difficult to script this conversation because I know both of them, and they have a lot of thoughts.

But let's go back there, a little bit, to the A.I. commission and then Representative Gallagher.

You told me at the beginning you want us to write a really good book?

SCHMIDT: Yeah. What I actually said is I want a book...

(LAUGHTER)

... OK. It didn't have to be good. I wonder...

(LAUGHTER)

... if anyone has read all 760 pages.

(LAUGHTER)

I know you didn't, Ylli.

BAJRAKTARI: But reflecting on this, Eric, we have numbers of legislation being passed from this commission. Obviously, Mark and I, two years after, we still handle a lot of requests from the Hill about pieces of legislation that have not been passed. What do you think, big picture, was some of the success of the A.I. commission?

Obviously, we live now in the A.I. moment. And what do you think were some of the things that we didn't come across to a successful path?

SCHMIDT: Well, there's a specific set of things that are in the NDAA which we authored -- your team specifically authored. So one of the pieces of advice for those of you who want to do this work is you have to have a theory of action.

We had a -- one of my friends had done a Ph.D. on commissions, and I said "what are the failure modes of commissions?" And he said "most of them fail." And I said "why?" And he said "because people write a very nice report, which everyone really admires and then nothing happens."

So Cyber Solarium had a theory of change, we had a theory of change. Our theory of change was that we would effectuate it through the NDAA, and we had the idea, which I think was yours, Ylli, to write the legislation on behalf of the Congress.

This is pretty arrogant on our part but we figured, since they've asked us to work, we might as well produce some legislation candidates, and much of that, something like two-thirds of it, is now part of the NDAA.

What we learned in our commission -- and I want to emphasize this -- is that these problems are really talent problems, and talent in the sense of how do we get the talent in our country, how do we produce more talent, how do we get the talent into the government, how do we get the leadership to understand this, which includes people who -- they'll never become computer scientists, you know, they're busy being other things, et cetera.

And we've done OK, not great in that. Some highlights would be we still need to work on high skills immigration reform. The Congressman and I have talked about this many times. This is, for many reasons, a high priority.

The other problem-- it's just to be blunt and obnoxious -- the government is really bad at buying and doing software. It's true at the state government, it's true in the federal government, it's true in the military.

And the reason is that the way procurement grew up in the last 30 years, which we can spend an awful lot of time debating, is not how software is procured. I'm not talking about the fact that the F-16 -- sorry, the F-35 is a $1 trillion weapons program. What I'm talking about is that you can't get a small software team to fix stuff with enormous leverage, right, at any level. It's true. And America would be a much happier place and a much more efficient place if we could fix that problem. I encounter this every day.

BAJRAKTARI: Representative Gallagher, same question to you. I know you had a one-year time compared to -- as which -- we had two-year, and I remember Mark's office looking, like, the original Solarium project. So what are some of the successes that you have observed out of your commission and what do you think we could have done better?

GALLAGHER: Well, we were smart enough to steal some of your ideas early on, in terms of their theory of change, and your friend, if I remember correctly, briefed us very early on about the -- he did this very in-depth historical study of commissions.

There's actually a fascinating -- for anyone who's about to make the mistake of getting a Ph.D. like I did, there's a bunch of literature on the politics of commissions. This guy Kenneth Kitts writes books about it. And the finding is usually they're used by members of Congress or presidents to sort of pretend like you've done something, even though you don't actually get things done. There's notable exceptions -- the A.I. Commission, 9/11 Commission -- but it's a very interesting bit of literature.

But we similarly, based on that conversation and based on the fact that we had four sitting legislators on the commission, which was a unique makeup for these type of things, decided that our final report, that we wanted to write it in accessible prose, we chose to do an unclassified report, would be but a blueprint for legislative action.

And we, again, stealing from you, decided -- or more specifically, Mark and his incredible team -- I see many of them here -- Ally went from being a Navy fellow in my office to going to Solarium, abandoning the Navy and doing all sorts of fun things...

(LAUGHTER)

... wrote the legislation, which any time you make it easy for members of Congress, that's usually a good maneuver.

Successes and failures -- I would say some of our biggest successes were the structural changes we made to the Executive Branch, most notably the creation of a National Cyber Director. One of our commissioners, Chris Inglis, became the first National Cyber Director. He's phenomenal. I'm sad that he has not been replaced yet and that the White House is not moving with alacrity, in terms of identifying his replacement.

We created the Bureau for Cyber and Digital Diplomacy in the State Department, which is being incredibly well led by a fellow Marine, Nate Fick, who is also a force of nature and just a phenomenal asset and part of the team here.

We enhanced the role of CISA, gave it more authorities, tried to enhance the authority that the CISA Director has, and there, we have one of our red team members, Jen Easterly, leading CISA very well right now.

We -- I'd say secondarily, some of our successes were giving DOD more resources and authorities to perform their cyber mission -- acquisition authorities, more resources -- but also forcing them to do things like a cyber force structure assessment, which, you know, illustrates the obvious, that we're not devoting enough talented humans, like Eric suggested, to this problem.

In terms of failures or things where we need to do more, we, in law, required a national tabletop exercise on cyber, we required a continuity of the economy plan, and we have yet to see either of those things happen in a meaningful sense. So there, we just have to do basic oversight to make sure that the Executive Branch complies with the law.

And I would just conclude by saying I agree wholeheartedly with the comments you made about talent. I think maybe the only thing I learned in this process is that cyber, despite all of the fancy jargon and sort of highly technical nature of it, is still fundamentally a human problem, right? The vulnerabilities are human but the successes are human.

SCHMIDT: So that explains how my meeting in the State Department went so well. I showed up a week ago in the State Department, talked about A.I., and there's this guy, Nate, right? Now I understand where he came from. And there were two people in this meeting -- this was all of the top people in State -- and it's Nate and Seth Center who worked on it with us.

So I think one of the narratives that we forgot to mention, both of us, is that part of the theory of change is the people who work in the commission and then go into the government, and they are your emissaries.

And sort of a rule of business is that if you could sort of put your person in the company, they're likely to buy from you. It's the same principle.

GALLAGHER: That is a publishable dissertation right there, that idea.

(LAUGHTER)

So you're welcome, whatever grad student is in the audience right now listening.

(CROSSTALK)

MONTGOMERY: First, I agree completely. I think, of our 25 or so, you know, long term members of our commission, I think 23 went into government. Google stole one. You know, I think that really helps and has been useful.

You know, for me, I want to come back to what you -- our biggest shortfall is one you kind of alluded to, and that's we did not get to cyber resilience strong enough, and I think it's because it's a multi-year issue and it's cyber resilience of your military mobility, you know, your port systems, your rail systems, your air systems so that you can get supplies and equipment moving rapidly. And the cyber resilience of your national critical infrastructure.

We have have to remind ourselves that that -- electrical power grid, financial services, telecommunications, that provides our actual source of national power, our economic tools of statecraft. And if we don't preserve those powers in a conflict or if an adversary can demonstrate to us that we won't be able to use those -- our national critical infrastructure, our military mobility, it's going to change our decision-making.

And for me, the how you get from where we are to there, is building stronger public-private collaboration and making sure we're resourcing the -- you know, getting the agencies right and -- you know, we just put out a paper the other day at FDD, the Foundation for Defense of Democracies, about this exact issue, about how you get sectors properly resourced, authorized, organized, and then how they have the proper relationships to the private sector.

One of the things is very few federal agencies hit all four. Maybe Department of Energy, and our work showed us that.

(UNKNOWN): Yeah.

MONTGOMERY: But you know, EPA didn't. HHS didn't. So -- Agriculture didn't. So really critical infrastructures don't have the proper support network from the government, and that's going to require oversight. Because we passed a law telling them to do it, but the oversight hasn't caused them to do it.

GALLAGHER: Quick point of order. Well, one, I naively thought when I came to Congress seven years ago, having watched "Schoolhouse Rock!", that you passed a law...

(LAUGHTER)

... the thing happens. Doesn't always work that way.

But I really want to -- because I know he has to leave in five minutes. I see at least two commissioners from Solarium, Patrick Murphy, Jim Langevin -- oh, Ken Rapuano's here as well. Essential to our ability to turn report into legislation was Jim Langevin. I mean, he was the chair of the Cyber Subcommittee on Armed Services, and was indefatigable in his efforts to turn our recommendations into reality.

Sincerely -- I'm not blowing smoke. You're not in Congress anymore. I have no reason to kiss your butt, Jim, but like, we...

(LAUGHTER)

... we would not have been successful without your tireless efforts. I mean, he would harass me on the floor constantly about a letter, or this, or have you talked to this person. So Jim, thank you for your leadership. It was phenomenal.

(CROSSTALK)

GALLAGHER: Yeah. Thank you.

MONTGOMERY: All right, Dr. Schmidt, so over to me now. Recent discussions about artificial intelligence and the government role have frequently talked about the need for regulation. Do you think this is a possibility? And if so, how?

SCHMIDT: So it′s important to establish why you need regulation, and I′ll give you some examples of how not to do it. China has an A.I. act which says that if you do anything that′s against the spirit of the Chinese Communist Party, you can be arrested. It does not define what that is, so it′s not enforceable except by humans who can arbitrarily do things. That′s not a good model.

The European Union has an AI EU Act which is so restrictive at the moment that if it′s implemented -- which I hope it′s not -- it will prohibit the use of open source in any form for A.I. In Britain, they didn′t pass an online safety act after a lot of complaints which would have defined ″harmful but legal speech″ according to, essentially, the British government, which is clearly not the way their non-constitution works. So everybody is screwing it up, in my view.

In the U.S., the best way to do it is to try to identify an actual problem, and then try to work on how to solve that problem. And so whenever somebody asks me about regulations, I say, ″Well, what do you not like?″

Here in Congress, I can tell you what people don′t like. It′s social media. It′s not A.I., and the reason is that they are -- these poor people are just subject to this enormous influence campaign which is full of misinformation. And frankly, I don′t know how you put up with it, especially as a highly-educated person. You know, it′s just insane, what we′re doing to our legislators. But -- so that′s one thing.

I decided to work on extreme risk, which I defined as the ability to harm more than 10,000 people, an arbitrary target, and existential risk, which is getting rid of all humans on the planet. So that′s the one I chose to work on, which strikes me as, both, pretty important. And there are scenarios in the future where A.I. as it evolves could be such a danger. It′s not today. And so that′s what I′ve been working on, and I would suggest that we not try to regulate the stuff that we all complain about until we have a more clear target.

Like my own hobbyhorse for the moment, which is not the subject of this panel, is we′re going to have a mess in the 2024 elections on all sides because of misinformation. By the way, that′s true in every democracy. Democracies depend on trust at some basic level as to what people said, what the facts are. We need a solution for that. So that′s a problem to be solved between now and November of next year.

MONTGOMERY: Thanks. And, Mike, you know, our fellow Commissioner, Chris Inglis, became national cyber director, wrote the National -- or authored a lot of the National Cybersecurity Strategy, and in it, he said I think we′ve come to that point where a purely-voluntary approach won′t apply. We need some mix of things, including regulation. The how do you think about that?

GALLAGHER: Well, I think if you read our final report -- easier to read 150 pages than 900 pages -- just saying.

(LAUGHTER)

But we don′t have a hard cover. We don′t have a nice hard cover. So yours looks cooler.

MONTGOMERY: Angus said no book stop.

(LAUGHTER)

GALLAGHER: Yeah, that's right. You'll see the tension there, and it's almost an unresolvable tension or sort of a balance you're constantly trying to strike between regulation and incentive. I mean, there's some areas which need to be highly-regulated from a cyber perspective. Nuclear power generation is one of those, right? There are other areas where I think it's -- probably be better to pursue a set of incentives where -- I had mentioned water utilities before. They had no resources right now. So there, you need the federal government to come to them not with a heavy hand saying, "Do X, Y, Z," but kind of a helping hand of, "OK, here's the resources we have that you can leverage. Here's our expertise." And so it's a mix.

I actually think Dr. Schmidt said it best when he testified before our committee a few weeks ago, which is that we need to do it the American way. We need it to be a true partnership between the private sector and the public sector, not just a government edict coming out. That then assumes you have competent leaders in the government agencies that deal with the private sector.

And in some sense, that was the theory of the case with the national cyber director. It wasn't just sort of, to quote my good friend, Angus King, "One throat to choke for legislators." It was a person that the private sector could interact with on a day-to-day basis.

So you know, it's hard to get the balance perfectly right. We tried to strike it, but in a situation where 80 percent of the critical infrastructure is controlled by the private sector, as it is in cyber, you almost need the private sector to step up and lead, and I just don't think it's going to happen with the government saying, "You must do it this way or that way." It has to be a balance.

SCHMIDT: But just to add to your point about why you need a cyber director, the government is very confusing to normal people. I mean that as a general statement and a specific statement. There's so many points of engagement that you do, in fact, need people who can see it all and really have some authority, and that's what you created in your report. We're going to ultimately need the equivalent of an A.I. czar, some structure like that. In our proposal, we made a proposal to do this at the V.P. level in the White House because we needed something that would look over all of it. That is not yet a solved problem.

If you want something to happen at scale, there needs to be a concerted owner and a set of initiatives. Each of the divisions, an administration person needs to sort of respond to, what are they doing? They need to get themselves organized.

And in fairness to our government leaders, they have so many different priorities, right? Here's a new priority. Well, we didn't give them much money to do the previous priorities, so you have to sort that out.

GALLAGHER: Yeah.

MONTGOMERY: You know, one thing I'd add to that is that, you know, when we looked at this, we had exactly that feeling that we either had to get one cyber committee in the House and the Senate, a Select Committee -- and I'd say if you asked Angus King what's the base failure that he didn't get, it was that -- but I just don't think that's realistic.

We felt we were spread across 65, 67 subcommittees and committees, that it was just you weren't going to get that many people -- unless you had a really blazing incident where the problem was congressional oversight, you weren't going to get that kind of thing.

So in the absence of it, having someone who could consistently talk to many of those committees -- not all 67 -- in the National Cyber Director, I think that's true for artificial intelligence.

SCHMIDT: And the other thing that's important is the person needs to actually know what they're talking about. So this is where the competency starts.

GALLAGHER: Can I ask, Eric you've served on the Defense Innovation Board and all these outside boards, but I feel like we still just make it too hard for someone with your background and your expertise to come in and do a stint for two years, let alone longer, in DOD. I mean, push back if you think that's...

SCHMIDT: Well, there are people who are foolish enough to do that.

(LAUGHTER)

Doug Beck, for example, just became the head of DIU and he's a public servant working at Apple, right, and he gave up his Apple job for a while.

So one of the things that I learned in my military work, which I think you knew very well, is people actually love the country and they're willing to actually, you know, give up stuff for the right role. So I think that part of our job is to create an opportunity where the really clever, educated person says "this is how I can serve and this is how I can evolve in my career."

And Washington is full of young people where their careers are made by their service here, right? And there's this enormous group of people who are highly educated men and women who believe in their country and they want to help.

There's this cynicism that I encounter every day, which I think is just fundamentally wrong. There is a group of people who are just waiting to be here to help us solve these problems. The problem that we have is we have not created the position for them that they can find, interview for, and get. Then we won't give them a clearance for a year. Then we won't give them a raise. We can't give them hiring authority.

You know, there's all sorts of administrative things but there's not a lack of will. It's an administrative problem, it's not -- at that level, it's not a desire problem.

GALLAGHER: Yeah.

BAJRAKTARI: Mark, I'll take it over from there because I think both Representative Gallagher and Eric touched on a lot of topics that we were planning to actually discuss. But for you, Representative Gallagher, as the Chairman of the China Select Committee, the one issues that we have encountered on the A.I. Commission side is, you know, the public-private partnership that you mentioned and the relationship between public and private has changed over time.

I remember the post-Snowden days, then the Google -- every interview Eric had was the Google Maven scenario. I think Ukraine has opened up a new chapter in that dynamics. We have seen public and private working hand-in-hand to really support the Ukrainian efforts.

But you also lead a China Committee, and I think when, on our side, we have this divisions and this statements of public-private, you′re facing a competitor that doesn′t have those challenges.

GALLAGHER: Yeah.

BAJRAKTARI: So how do we bring these two communities closer together? Eric talked about the talent and the enthusiasm that exists. But how do we move across these barriers that we have sometimes?

I know how difficult it was on the A.I. Commission to have CEOs from top tech companies that serve on behalf of Congress related to a tech issue.

GALLAGHER: Yeah. Well, first of all, on the Maven scenario, I remember -- I might have even just been a member-elect. I wasn′t even sworn in -- and McCain -- no, it would have been the year after. I was a freshman member.

And then-Chairman of the Joint Chiefs Dunford was on a panel at the Halifax International Security Forum and he was asked about the Maven scenario, which was still kind of hot on everyone′s mind, and he said something that always stuck with me.

He said ″listen, all you companies out there in the audience, you′ve got to realize, like, we′re the good guys, OK? We′re the good guys, and if we don′t have that basic recognition that, you know, America is leader of the free world and that means something and that we should seek to win this competition, I think all our other efforts are going struggle.″

I think we′ve come a long way since then. In fact, I almost think the problem now is not that employees of certain tech companies are loathe to work with the Defense Department, it′s that the Defense Department is just so hard to work with. I mean, it′s like an impossible customer, for the reasons that Eric suggested earlier.

So a lot of success in this area just comes down to fixing DOD′s ability to buy stuff in a way that isn′t totally insane, right? Like, not doing the SBR's "participation trophy" process, which just contributes to our valley of death issue, and figuring out a way where DOD leaders are willing to accept risk and make big bets on winners and -- which implies that certain people are going to lose competitions. We just haven′t had that. We still struggle. Despite all this authority that Congress has actually giving DOD, they′re unwilling to exercise that authority because they′re very risk-adverse.

The second thing I would say is, when it comes to authorities and talent, we′ve also given them a lot of authority to hire people. So one of the things we′re doing on the CITI Subcommittee on Armed Services is basic oversight of DOD to ensure that they′re using Cyber Excepted Service, for example, in order to recruit non-traditional, highly talented people to work in DOD, which -- and I′ll just hammer or foot stomp a point that Eric made earlier -- you just have to realize, when you′re doing that, at least in my opinion, like, it′s never going to be about the pay. Yes, we should have flexible ability to pay highly talented people more. but you′re never going to be able to pay them as much as Google is.

So it can be about the mission. You can compete for top level talent on mission. The NSA does it every single day. What we want is for CISA to be able to do that, that the mission of CISA becomes so sexy that someone who′s really talented, who could go work for a top level tech company, says ″you know what? I actually want to spend five years defending the dot-gov network from bad guys that want to hurt us and our allies, i.e. the good guys.″

SCHMIDT: One of the -- I completely agree with everything you said, Congressman -- one of the things that′s changed is the Ukraine War has finally taught all the people that I work with that there is evil in the world and -- shocking, I might add, shocking that they didn′t know -- and I think that these issues are now clear. I think everything you said is exactly correct.

I look forward to serving on your Military Procurement Restructuring Commission that you′re going to be leading and helping you in any way.

GALLAGHER: You volunteer me for too many outside extracurriculars.

(LAUGHTER)

SCHMIDT: But what I would say is I worked on this a little bit, and so because I was on both sides, I talked to the military and then I talked to the Congress. And the congressional people would say ″well, we gave them all these authorities,″ and then the military would say ″well, they told us what to do and we didn′t like it.″

And so that′s literally what they say privately -- and so my suggestion was the following: Inside the government, pick some -- sorry. Inside the military, pick some projects where you can use the authorities Congress has given you maximally as an experiment, as opposed to minimally. And the way you would do this is you would actually have a conversation with Mike Gallagher, and you′d say, ″We want to take a risk here. Do you agree,″ right? And you will absolutely say yes. And then you have agreement between civilian oversight and the military to take some risks that they don′t think that they are emotionally allowed to.

You can think of many areas. The one I am always interested in is the one around missile defense, because missile defense is really, really hard, and our opponents are creating these enormously-frightening things. I want to know how we′re safe. So that′s an example where, let′s take some risks. Let′s work with Silicon Valley. Let′s work with some of the technologists around autonomy. We′ve got some clever ideas, but they′re risky, right?

And by the way, in the budget that we have, we can take a small amount of risk and nobody′s going to notice even if we fail as long as Congress says it′s OK to take the risk. That′s the bargain you′ve got to create.

MONTGOMERY: I′ll pick up on that, because Representative Gallagher and I have been working on one of these exact issues and -- I′ll just say without going into too much detail -- hypersonic missile defense is something we have to get good at.

GALLAGHER: As soon as you said that, I knew, Mark was going to start. He's obsessed with it.

MONTGOMERY: Yeah, yeah, yeah. You know, it′s bad if the Chinese and Russians are good at offense. It′d be nice if we could catch up on that, but we have to catch up on defense. And what I think is happening in the Department of Defense is the current couple ideas they have might not work. So instead of like just betting on both of them and seeing what happens, they′re going to cancel both and say, ″We′ll roll this to the 2030s.″ In other words, risk assumed by somebody else in some distant future is not risk that they′re held accountable today. And we still haven′t broken that paradigm, even, I think, in a current Office of the Secretary of Defense that′s fairly dynamic on a lot of issues. This issue of failure is not allowed.

If a venture capital firm was 30 or 40 percent successful they′d be highly-successful. If you′re a PEO, a program executive office in a service and you′re not 90 percent successful, you′re a failure. Those two dynamics cannot continue to work in concert. The department′s going to have to change.

SCHMIDT: Can I add that when we did the initial programming in Google, Larry and Sergey, who are obviously brilliant, said, ″Here′s the rule: We′re going to spend basically 70 percent of our resources″ -- the company was small at the time -- ″on search and ads, which is our business. We′re going to spend 20 percent of our time on adjacent businesses, and we′re going to spend 10 percent on unrelated things.″ And I said, ″I′ve never heard such an idea. What a terrible waste of 10 percent of the resources of a firm.″ So Sergey, who′s a mathematician, gets up and on a whiteboard proves mathematically using math I didn′t understand that statistically, you want to have this amount of risk in this bucket.

That′s not how we run the military. So let′s use my 10 percent. Ten percent of $800 billion is $80 billion. Why don′t we take one percent? Let′s take one percent of $800 billion, $8 billion, and apply it to really risky stuff which is probably going to fail, and one of those 50 things will solve your hypersonic problem. Is that a good use of our country′s money? Absolutely, right? Absolutely.

GALLAGHER: Can I add to that? That there is actually an authorized bucket, let′s just call it -- it′s called the multiserve -- I forget what exactly what it′s called. We created it. I wasn′t a member, but it was 2015, 2016. McCain revised an old concept, that up to a billion dollars, you can put into this bucket for, like, a SecDef priority, for a big risk. The money has never gone into that bucket because no comptroller wants to anger the appropriators.

SCHMIDT: Right.

GALLAGHER: They′re afraid of the backlash. It′s your point about risk.

SCHMIDT: And since you are a representative of the Congress here, the fact that you have Armed Services and appropriators in separate committees is a problem because their incentives are not in alignment. And I will tell you that, in software, I met with a very, very senior -- you know, what I thought of as a five-star general -- I guess we don′t really have them -- in charge of everything. And he′s got all the Marines -- you were a Marine -- and all that around him, going, like, ″You′re a big cheese.″

He said, ″Yes.″

And I said, ″If you′re such a big cheese, why can′t you get 50 people to work on the software problems that we identified?″ They′re cheap relative to the billions and billions of dollars that he controlled.

And he said, ″I tried.″

And I said, ″Well, what happened?″

And he said, ″They were appropriated away from me.″

And I said, "What? OK, you're, like, the biggest cheese I have met, right?"

(LAUGHTER)

"You have, like, medals and medals and medals. And they did this to you?"

He said, "Yes."

That was -- I mean, it was a one-word answer.

So it doesn't make any sense to take these people, enormously important, enormously well-trained, enormously powerful leaders in our country, and give them such nickel -- I don't know how to say it -- nickel-and-diming. It's just a bad way of running things.

And, by the way, he wasn't asking for $1 billion. He would have taken, you know, $100,000, $1 million.

MONTGOMERY: I do want to get to one other issue, just because it's right in the news now. As we mentioned earlier, the unprovoked Russian aggression against Ukraine. It really has shown the critical role the private sector can play in supporting allies partners, and we're seeing that, especially with the -- under cyber duress.

Eric, what do you think of the private sector's role to date?

And where do you think the private sector's best positioned to assist Ukraine?

SCHMIDT: So I was curious, because I've lived through Maven and I lived through all the crap that went on between the tech industry and the government and not being in alignment. And I wondered what would happen in a real war, a shooting war, with the tech people?

In other words, would they fall in or would they fall out, right?

And I can answer definitively that they fell in. And they fell in, in a really, really powerful way. So in Ukraine, what happened was the -- when the war started on February 24th, they had an app called DIIA, D-I-I-A, which was one of these passport identity apps.

And they added a feature where you could take a picture of a tank that was geo-located, and then it would be -- it would be -- a separate group would make a targeting -- A.I. would classify it and it would be an A.I. targeting decision. And then a different group would go and shoot the tank and kill it.

And that is the proximate reason why the invasion on the 24th --remember the column of tanks that was -- that was, you know, there? That's why that invasion was largely stopped. It was the courage of the people and the underlying broadband that -- that was in place.

So I learned something, which is a small set of software people, using networks and analytics in combination, can dramatically change the asymmetry, or asymmetry of war.

Today -- and I wrote an article about this, which you referenced earlier in your comments, about innovation power. I believe that the future dominance will be about innovation, not hard power or soft power but innovation, innovating in the future. Because everyone's going to be competing, and I want us to be the winner in that.

If you look at Ukraine today, it's largely a drone war. They call it an army of drones. And they've used about 50,000 drones, most of which are suicide drones, and that's how they've solved their lack of air cover and so forth and so on.

In fact, the Russians have been forced, because of HIMARS, which is very successful, and then the drone stuff, the biggest interesting outside supplier to Ukraine has been a Turkish company which makes these extremely powerful drones that have been well tested in the battle, starting in 2014. They have a lot of experience with it.

A doctrinal point is that future conflict between nations, and maybe with asymmetry -- with asymmetric actors, will largely be autonomy- and drone-related. Right, that that's in fact -- we're -- we don't want to send humans into this; we want to send -- and you're actually a courageous person, and I'm actually not. If I were unfortunately in a war, I'd want to have 50 drones ahead of me watching

(LAUGHTER)

SCHMIDT: ... and 50 drones behind me, making sure there's nobody from behind me.

And those are my negotiating conditions, General, for entering in your war, right?

(LAUGHTER)

That's how scared I am, right? Why can't we do that for our soldiers, men and women? Right? We owe that to them, in my opinion.

MONTGOMERY: Mike, anything you want to add on the government's role in Ukraine?

GALLAGHER: A small cyber point. I think we have to recognize that we actually had an intensive partnership with Ukraine prior to the collapse of deterrence in February. We -- we -- in 2018 we sent $50 million for cyber partnership to help them with defending their critical infrastructure. We had a training program that went back far before that. We had hunt forward operations under way.

And I think, to the extent -- that -- I think that's paying dividends right now.

SCHMIDT: I think you're underselling it. Part of what happened was, in the first week, the Russian doctrine was to shut down their critical infrastructure, and their attempts failed, thanks to what you did. So thank you.

GALLAGHER: Well, it was Nakasone and some other people.

I will take credit for it. I'm very good at that...

(LAUGHTER)

... as a member of Congress. My only point there, I guess, is, sort of, you know, a simple one about the importance of maintaining forward presence and partnerships with allies and partners. And I think there's an obvious lesson there for Taiwan and other beleaguered democracies that live in the shadow of totalitarian aggression, all the more reason why we shouldn't, sort of, retreat internally and why we have to stay forward-engaged, because, as Dr. Smith said earlier, Ukraine was a big reminder that there are -- there are bad guys that are going to do bad, evil things in the world.

SCHMIDT: You know, I think that the other comment -- and we -- I think we think we forgot this in our narrative, is that we -- our current sort of positioning is related to the effects of the Second World War. And the Second World War could be understood as a fight for freedom versus the other models.

And I think we forget that fighting for freedom is what the American mission is. And freedom means freedom of movement, freedom of thought, freedom of speech, the things that democracies represent. And so I guess my political advice would be start with freedom. I think we are taking it for granted. And the reason, you know, I and others are trying to help is that I actually care.

GALLAGHER: I appreciate that.

MONTGOMERY: You know, as we head into questions here, one thing I'd add -- I agree with all that. In the cyber world particularly -- we just started a study at the CSC, and one of the things we found is we actually do about $2 billion a year in cyber capacity-building around the country -- around the world, I mean. And only a small percentage, maybe 5 percent, is the hunt forward operations that get all the attention.

My fear is, is that it's not, kind of, organized, prioritized and assessed, you know, to get out there and, you know, resourced to get out there. And so we're really hoping Nate Fick -- you know, when we created his position -- when Congress created his position, they also said "you owe us an International Cyber Security Strategy at the end of 2023."

And I hope that's more than just what State Department can do, but it's what everybody can do so that Congress can then oversight an actual plan, because that's a lot of money to spend but we saw the return on investment on Ukraine.

GALLAGHER: Yeah. We saw certain allies step up and exhibit capabilities that we didn't truly appreciate prior to it, so -- in the cyber domain.

MONTGOMERY: Certainly the Estonians ...

GALLAGHER: Yes, exactly.

MONTGOMERY: ... come to mind on that.

Hey, so we better turn to questions from the audience here. I'll leave the last 10 minutes for that. So please raise your hand, we have some mics, but identify who you are and then zip out a question.

Oh, there we go -- Jonathan?

QUESTION: Sorry, cheated. I'm John Sakellariadis. I work as a cybersecurity reporter for Politico. First of all, thank you for the great panel. A question, kind of, for everyone here. I've talked to some folks in the adversarial AI community, and they've expressed a lot of concern that companies are moving too quickly to integrate AI, (inaudible) in particular, into new products and services. How concerned should we be about that problem, the security vulnerabilities we are creating via AI deployment. And without prejudging any answers from the panelists, what do you make of Microsoft's proposal of regulating the deployment of AI in critical infrastructure?

SCHMIDT: I don′t want to comment on Microsoft′s specific proposal. There is going to be -- there′s going to be regulation around extreme risks and so forth. The problem with regulating critical infrastructure is if you write it the way you would naturally write it, you′ll prohibit its use because it can′t explain itself. That′s sort of the core problem everyone is facing.

Adversarial A.I. is a situation where the model is -- weights are modified in such a way that instead of producing the right answer, it produces a slightly different answer. At the moment, it′s largely a theoretical concern because we don′t understand why the weights do what they′re doing in the first place. So we have some time to work on this.

So adversarial A.I. is not my highest concern. I think my highest concern is actually much simpler. When you have these models that are proprietary, they need to be secret. If you look at LLaMA, Facebook released it for research use, and within 48 hours, it was stolen on the deep web and now everyone′s using the LLaMA weights, including the 65 billion one, and -- which is presumably not what Facebook wanted. That′s not an existential threat to America but it′s an example of what could happen in the future.

So I think keeping the model secure is priority, and that needs to happen very fast. The work of this commission is very important, right, for that security. That′s why their recommendations are so important.

QUESTION: Yeah, thank you. Shaun Waterman from Newsweek. Dr. Schmidt, can I ask about this focus that you talked about on extreme risks and existential risks? I wanted to, you know, for thirty years we were warned about the danger of a cyber Pearl Harbor, and it turned out that what was probably more dangerous was a cyber South Bronx. You know the rank and criminal activity that appears unstoppable. Are we missing something by looking at these really big risks and perhaps paying less attention to the smaller risks? I mean isn't the real risk from generative AI that can turn anything to crap? You know you can't trust anything you read on the internet, or see on the internet?

SCHMIDT: So now you′re talking about the things that I mentioned about social media, because in fact people will experience A.I. in the form you′re describing through social media, so I agree with that.

If you imagine creating an Internet regulatory body, which I′m not advocating, just imagine all of the things that would be on the agenda for that body, all of the complaints that we have about what happens on the Internet cause we live on it. So I think it′s better to not view it as a Internet regulation or an A.I. regulation but solving a problem.

I think that there is a very, very significant misinformation problem coming. We need to get ahead of that. I′m calling the alarm, I′m saying right now it′s going to happen. Get our act together. And the reason, by the way, is that stable diffusion and other tools are broadly available to good people but also bad people.

QUESTION: Hi, Elias Groll with CyberScoop. Folks at OpenAI have started pushing ideas around AI governance that have been inspired by arms control, almost, in particular I'm talking about IAEA but for AI. I'm wondering if you folks on the panel would like to react to those proposals. Do you think that these arms control frameworks are useful in thinking about AI governance, or does this kind of take us down the wrong route?

GALLAGHER: Well, I was enjoying this model where you would get asked questions and I just sat back.

(LAUGHTER)

I confess I'm a bit skeptical -- or let me put it differently -- I think there is work that needs to be done prior to that discussion, and put aside sort of whether or not the IAEA itself is appropriately resourced and structured to, for example, inspect Iran's nuclear program, whatever.

Right now, this debate has just started on Capitol Hill. Obviously, Sam Altman recently testified before the Senate. We're hoping to continue the discussion in the context of China. So there's a few smaller things we need to do before we get to the question of some sort of international body for regulating A.I.

One would be to take a hard look at the A.I. guardrails that DOD has, which Eric and Ylli have talked about, and I think by and large, we think they're directionally right. And whether those can be shored up and then extended across the federal government and whether that sort of becomes the framework for how you don't slow down or pause A.I. development but have enough guardrails where someone in northeast Wisconsin can be confident that A.I. is not going to destroy humanity. So that strikes me as tasks number one, two and three for Congress, in partnership with the private sector.

And then there's smaller issues, like, you know, everyone, in a bipartisan way, has supported the recent export controls on chips to China. There is a suggestion we've heard from many people, however, that there's a loophole in those export controls that might need to be shored up so that China doesn't get access to, you know, a GPU that effectively provides 97 percent of the functionality of the things we're trying to prevent them from getting access to so we can maintain our edge in this race.

So I don't know, that's -- I need to do more homework on the international regulatory thing but there's a lot of other things we need to do first.

MONTGOMERY: One thing I'd mention on that is that, in 1999, I was working with the National Security Council. The Russians came to us about a cybersecurity arms control regime, and I just remember that their lead negotiator was Lavrov, which, you know, in hindsight...

(LAUGHTER)

... you know, our response to him then was -- there was a trust but -- as you walked away from this, there was a trust but verify that you just couldn't get to verify. And I think, so when it comes to an international agreement on this, it's going -- I think it's going to be very hard.

SCHMIDT: Well -- and just to add, Mark, the IAEA is very, very invasive. So remember that they can go to your nuclear site and send people in and inspect.

GALLAGHER: Yes.

SCHMIDT: So it's a pretty big jump from where we are now to having government inspectors going in and reading the code of random people, right, which may be necessary but we have to really think through how that would work.

MONTGOMERY: International inspectors.

SCHMIDT: Yeah.

GALLAGHER: Maybe, like, the core point is a sound one, which is simply we should be on the same page with our allies and partners when it comes to the overall framework that preserves our innovative edge while also guarding against the extreme risks.

SCHMIDT: Well, what's interesting is -- and you may -- in your China role, you may or may not agree with this -- I think that -- and you speak to this, I guess -- China's list of concerns over extreme and existential risks may be the same as ours, right?

So you don't know until you have the conversation. So how do we have that conversation? Who has it, right? I'm not authorized to have that conversation. Perhaps you should. I'll give you another assignment, I'm sorry.

GALLAGER: Well, I would say one -- maybe one caveat to that would be -- those of us who love freedom would view giving the government or a party the ability to use A.I. to completely control and influence every decision a citizen makes as an extreme risk and a bad thing, whereas Xi Jinping and other members of the Chinese Communist Party would view that as, like, goals AF, as the kids say ...

(LAUGHTER)

... so there are -- a bit of a -- a bit of a difference there.

MONTGOMERY: All right, one more question ...

QUESTION: Thank you, I'm Suzanne from The Record. I wanted to ask about the privacy concerns imbedded in AI and our privacy. And, you know, ChatGPT uses the prompts users put in to train the algorithm model. So, you know, people have talked about that leaking. Is that a concern? Are there other concerns that relate to privacy with AI that you were having?

SCHMIDT: Well, today, the training is largely static. You start training, you wait six months, you get your model, then they do something they called RLHF, where they basically fine-tune it using human feedback.

So the odds of your query in ChatGPT showing up in some other context, at the moment, are pretty low. So I'm not particularly concerned about that. So I think that the general concern is valid. At the moment, the technology is so static, it's not learning very well, it doesn't -- you can't really -- it's not up to date and so forth.

When these systems, which is not today, don't hallucinate, can learn continuously and have really good memory, which they don't have today, then I think your concerns will be quite legitimate. But we're not there yet.

MONTGOMERY: And I know we have to wrap, and before Ylli says it, I just want to first publicly say -- and Mike alluded to it -- but the support -- the A.I. Commission started about two to three months before us four years ago. Without the A.I. Commission, we would not have been successful in meeting our mark, and if we hadn't met our mark -- we released our report the day before COVID really locked down D.C. -- we wouldn't -- it would have really set us back. So I want to ...

GALLAGHER: We had the first super spreader event.

MONTGOMERY: That's right.

(CROSSTALK)

(LAUGHTER)

(CROSSTALK)

MONTGOMERY: I think we like to say we had the last non-super spreader event.

(LAUGHTER)

SCHMIDT: And because we were slower than you, we started from your reports.

(CROSSTALK)

MONTGOMERY: And I think we both need to thank Ken Rapuano, who's in here, from Office of the Secretary of Defense, and he worked on our commission, but more than that, made sure we got -- OSD is not a bureaucracy that Ylli and I were unfamiliar with but we also couldn't defeat it on our own, and I want to thank Ken, he was fantastic.

But Ylli, back to you.

BAJRAKTARI: No, thanks, Mark. And the fact that, two years after, we were still talking about this issues, you know, indicates that we have not finished our work, and I think what you're doing with CSC 2.0 and what we're doing with SCSP is really a continuation. Because I think we are still living in the middle of this technology evolution. Whether we're dealing with cyber or A.I, I think these are things evolving by the day.

And the work Congress does, the work that Eric can help bring from the private sector really is something that I think we need as a country, and I think we need to bring these communities together so we can find solution to the problems we have.

And so I want to thank Representative Gallagher for serving our country, Mark for being a tremendous partner, Eric for all his -- your willingness to jump in and help, and then -- and thanks for everybody for showing up today. And we will continue our work. And have a good day, everybody. Thank you.

(APPLAUSE)

END