
TRANSCRIPT

Discussion

- Ambassador Nathaniel C. Fick, US Ambassador at Large for Cyberspace and Digital Policy
- Patrick M. Cronin, Asia-Pacific Security Chair

Disclaimer: This transcript is based off of a recorded video conference and breaks in the stream may have resulted in mistranscriptions in the text.

A video of the event is available: https://www.youtube.com/watch?v=pRrzeoDNH9Y

About Hudson Institute: Founded in 1961 by strategist Herman Kahn, Hudson Institute challenges conventional thinking and helps manage strategic transitions to the future through interdisciplinary studies in defense, international relations, economics, health care, technology, culture, and law.

Hudson seeks to guide public policy makers and global leaders in government and business through a vigorous program of publications, conferences, policy briefings, and recommendations.
Patrick Cronin:

Hello. I'm Patrick Cronin, Asia Pacific Security Chair here at the Hudson Institute. And today it's a great honor to have with me Nate Fick, ambassador at large for cyberspace and digital policy at the State Department. That's the inaugural position here for trying to bring together many threads of technology and cyberspace over at the State Department. And Nate is an old friend and somebody I've got tremendous respect for. He's always been at the front lines of whatever he's done. I don't know whether it was maybe the classics major at Dartmouth did it for you. But at the front lines as a junior officer in our wars in Afghanistan and Iraq, front lines of a think tank at the Center for New American Security where I worked for Nate, leading that kind of startup, energetic think tank that's still going very strong. Front lines of in Silicon Valley, thinking about as a cyberspace security firm as the CEO there and now on the front lines of diplomatic security and technology, a very ambitious role thinking of all of those fusty diplomats with their pens and quills, and you're bringing them into the 21st century.

No, that's not fair. We know our diplomacy has been keeping up with the times, but my old images of growing up, of thinking of the Kennons of the world, looking for that pastoral future, and now we're in a world of tremendous technological change. It's a great honor to talk to you today about US leadership in technology diplomacy. And here maybe I just start by making a differentiation between there's technology and diplomacy. There we can think about the old and the new are constantly going to be intermixed. And I'm thinking, I just had an op-ed out today on Secretary Blinken's tireless diplomacy in Beijing where you're jet-lagged, you fly halfway around the world, the Chinese subject you to seven hours plus meetings with their foreign minister. You come back the next morning, you've got three plus hours with the top diplomat Wang Yi, and then finally you're subjected to the 35-minute interview with the Communist party, General Secretary Xi Jinping, who's heard every one of your talking points at this point. And you're supposed to be deflecting their points.

And yet the images, the words that instantly came out of Beijing and from others after that trip, were we being too submissive? Did the Chinese get the upper hand? Did we get the upper hand? There's the competition over narrative, where new technology's bringing that in. That's technology in diplomacy, that's going to continue to be part of the landscape. But here we're really to talk about technology diplomacy, meaning the governance of the rules of the road, the building of the institutions that we need at State Department in the government with allies and partners around the world, what we're trying to build in the world while we're trying to protect ourselves from the perils of high technology. When you think about AI and biotech combining to what that could be or whether it's building the positive set of rules that we could all abide by and live with and prosper from, the good things that could come out of technology if we can only make sure that their rules are abided by and enforceable.

Anyway, enormous challenges. You're the right man for the job, Nate, I'm delighted you're there. It's a very big task. I wonder if we could just start with a few words from you on maybe your vision of your role and the idea of US leadership and technology diplomacy.

Nate Fick:

Thanks Patrick for having me. Thanks everybody for being here. And it is gratifying to look back at CNAS where we had the pleasure of working together and see the place thrive. I'd like to think it's because of what we did there, not because we left, but the place does continue to do well. And before I talk about vision and what we're trying to do, I do want to acknowledge what you said about Secretary Blinken's trip to China because I think we underestimate the human
factors in all this. You went through that. You through fly around the world, you get off the plane, you go through this large dense set of meetings, you're jet-lagged, you're not eating well, you're dehydrated and you did it last week someplace else and the week before that someplace else. We don't really talk about the human factors in all this.

And when I was in the Marines, we talked about the last hundred yards. The idea that you had this massive defense budget, this institution of millions of people, all this money, all this doctrine, but it funneled into sometimes the point. And at that point, it's a person and a rifle on a bridge someplace. And in that last a hundred yards, it's just you and Secretary Blinken talks about that in diplomacy. He calls it the last three feet. And I think last year or this trip to China is a good illustration of it. We have no real domestic consensus here. Lots of different points of view, a huge noisy apparatus. We have a trillion dollar establishment that ends with him shaking hands with his counterpart in the last three feet. And I would just encourage us all to remember the human factors in all this.

It's structure and agency. We spend a lot of time on the structure. I think the agency's also really important and human agents deal with things like jet-lag and fatigue and just the physical exertion of it all. But that aside, I'll give you the answer on what we're trying to do that I gave Secretary Blinken when I first talked to him about the job on February 24th of last year, which was a momentous day in hindsight, obviously. The day of Russia's full scale invasion of Ukraine. I spoke with him by video around five o'clock in the afternoon. And so in hindsight, I do admire his ability to compartmentalize given what else was happening in the world at that moment. But he said, "Hey Nate, what would you do in the job?"

And I said, "Well, from my perspective, very much on the outside now, I think there are three things we need to do. And they are concentric rings. The innermost ring is we need to build capacity in the State Department to do this work because this is a new enduring feature. This is not a moment in time, it's not a fad, it's not a passing moment in international relations. This is the next phase and we need to build the institution and we should spend some time talking about that. The second ring is we have to assert our nation's lead foreign affairs agency role in the interagency process on this. We need to put diplomacy back at the forefront. As a CEO working with the government, occasionally I interacted with Homeland Security and Cybercom and other parts of DOD or justice.

I didn't interact with the State Department, so let's get state at the forefront and put the diplomatic tools really, really in the toolbox on all this. And then the third ring is we need to have a strong foreign policy in these areas out in the world. And our remit in this new organization includes cybersecurity policy. It includes information and communications, technology policy. It includes the full spectrum of emerging tech. And it includes, of course, the human rights element that undergirds all of those."

Patrick Cronin:

Important. I've heard you talk about a free, open, interoperable, reliable and secure internet.

Nate Fick:

That's a term of art.

Patrick Cronin:
That sounds somewhat almost incompatible to some of those terms, the interoperability, the concern about the balkanization of the internet with what other countries are doing. And this is where, to what extent can the US assert its leadership when you've got other actors, whether they're big countries or the private sector in some cases, pushing in a different direction?

Nate Fick:

I think we need to do two things at once. And it's probably true in every aspect of most aspects of international affairs. We have to remain anchored on the North Star, our vision of what the world could be or ought to be. And at the same time, we have to be ruthlessly pragmatic in dealing with the world as it is. And I think we have to do both of those things. And in this arena, I think that North Star is this idea of a free, open, interoperable, reliable, secure global internet that is not balkanized, that does not tolerate things like shutdowns and firewalls and content control by authoritarian governments. That remains true to its founding vision of democratizing access to information for people all over the world.

And that's the affirmative vision that is the North Star that ought to guide our thinking and our policy in terms of developing a positive, compelling, attractive vision of what this shared technology future can be. And I joke, I have two middle school daughters. I know walking into the room and pounding the table and saying, my way or the highway is not an effective parenting strategy. It's also often not an effective diplomatic strategy. We have a group of states that are with us and will always be with us. We have a group of states that are against us and maybe in competition with us for a long time. And then we have a vast middle, a huge number of people and countries, government's companies in the world that at different points are going to have to align themselves one way or another. And forcing them to choose is less effective than giving them a choice and providing a choice.

That's the North Star, that's the vision of, I think, the affirmative vision of what we want the world to be. And at the same time, I think we do have to be realists and pragmatic about the world as it is. And if you'll just indulge me, I'll give you a couple of paragraphs on that and then we can talk about it. I believe that technology competition, technology innovation as a source of national power or coalition power is increasingly foundational. It sits on the same level as more immutable factors like demography and geography and natural resources than it does on the level of GDP and military capacity or these more traditional measures of national power. Those things, GDP and military capacity and other measures are increasingly downstream of a nation or a coalition's ability to innovate technologically.

This is increasingly a wellspring of national power and influence of coalition power and influence in the world. And we ought to be very deliberate about stewarding our domestic innovation engine that has generated huge advantages for the United States in this regard. We should be encouraging our like-minded allies and partners to develop and steward and sustain similar innovative engines. And we ought to recognize that defending and extending those areas of technology advantage is going to increasingly be a source of our influence in the world.

Patrick Cronin:

I think we had Kurt Campbell on this stage just in the last month even talk about not seeding any ground on the technology front to China, so let me just ask you a little bit about this question. Even at the State Department, you hosted the Pacific Forum Authors recently. Great study earlier this year that came out looking at China's digital grand strategy. They really put the whole comprehensive part together. Xi Jinping is wedded to this. He learned it even as he was
governor of Fujian Province before he became the General Secretary of the party. How can we compete with a country that has such authoritarian power, an ability to, at a macro level, determine a grand strategy? And you're at the State Department trying to push up against a lot of forces across the interagency in your own ethos of the State Department nationally against private sector to try to pull together the threads of a strategy. How do you do that?

Nate Fick:

I think first and foremost, it can't be a fully symmetrical strategy. Look, I've been here and doing this long enough now and enough places around the world to see firsthand that China is executing a full court press all over the world on these issues. We see it glaringly on information and communications technology of all kinds. Think about this as the backbone of the internet. These are the pipes that get the internet into your phone or into your home. It's cable and fiber, it's data centers, it's satellites, it's wireless networks, it is the architecture. We can spend every dollar we have and every hour we have on cybersecurity securing all the applications and the data that sit on top of that architecture. And then we end up with very secure uncorrupted packets going back to Beijing in the architecture of the untrusted framework.

That's why getting the architecture right is important, and it's why the Chinese have made a 25-year concerted political and economic push to do that. Let's just illustrate it by example. I think it's illustrative. 30 years ago the United States and a handful of other countries, Finland, Sweden, South Korea, Japan, France, had what felt like an unassailable global advantage in telecom tech. We had Ericsson and Nokia and Samsung, which still exist, but also Motorola and Bell Labs and Alcatel and Lucent, and a long list of vibrant, innovative companies. Most of them are gone. The ones that remain are not as strong as they used to be. And why is that? Well, I think there was an element of corporate complacency. Incumbents get comfortable. There was an element of government and attention. I don't think we appreciated or acted on the reality that these technologies were going to be central to our geopolitical standing. But also the Chinese executed a deliberate couple decades strategy of IP theft and government subsidies. They stole the core intellectual property to begin building

Nate Fick:

... the core intellectual property to begin building next generation wireless networks. And then the PRC subsidized Huawei and ZTE around the world to do deals at less than competitive terms. So the net result now is, and this is the troubling part, Huawei is no longer relying on IP theft for its competitive advantage. That has catalyzed a domestic innovative capacity. So if you talk to European telecom operators, they'll tell you that the Huawei gear is quite competitive, in some cases better than the trusted alternative. So this is a playbook. It's a playbook with some distinct elements that got run in telecom. And if we allow the Chinese to run it again, they will run it in cloud computing. They will run it in AI. They will run it in every core strategic technology area that matters. And we need to be very clear-eyed now about not letting that happen.

So we can't do it symmetrically because we're not going to match them dollar for dollar in every geography around the world in the way that they are. So we need to identify the technologies that matter. We have to build the biggest possible coalition that we can. And I think there's an element of asymmetric competition. And in this regard, we do have a huge advantage. Because in the long term, I'll put my faith in free markets and democratic systems every time, both in terms of their political attractiveness to people, and also in terms of their ability to build and steward companies, innovative companies. And I think we're in the early days. It's too soon to call, but it feels like the wind is shifting a little bit, and that countries that have succumbed to the
sort of debt trap diplomacy that have built their infrastructure on untrusted networks are seeing now the national security consequences, the economic consequences, the human rights consequences, and they're looking for a way out.

Patrick Cronin:

We have found, you have found, the US government has found a lot of common ground with allies and partners in Europe and in Asia, but it's the so-called global south that maybe the bigger challenge where Chinese has more influence with co-opting them with Belt and Road Initiative money and other incentives. I know Indian Prime Minister Modi is in town as a symbol of the global south and a leader of that. What are the prospects of the United States winning over the other part of the world that it is not just the rich European countries or rich Asian countries.

Nate Fick:

So I think there are a few elements to that, and I agree with, I think, the premise of the question. And it does get back to that notion that, okay... And we had our chief admission conference last week with every American ambassador around the world back at the State Department for a few days. And in the secretary's opening comments, the first point he made is geopolitical competition is endemic now to everything we do. The grid power competition is back. Maybe it was always there, but it was below the surface. Now it's really overtly explicitly back. And technology is the primary realm of competition in this. It's the primary domain of competition. So we have to continue articulating that positive vision in order to get the states in the middle, the consequential hedging states. Yeah, I'm not going to name them, but we could all sort of think through who that is, want them to tip in support of the ideals that we're articulating.

I think if we try to match the Chinese financially across the developing world, across the global south in each of these deployments, we don't have the capacity or the political will to do it. Because when a trusted vendor comes in with a $400 million bid and Huawei comes in with a $0 bid and a soccer stadium, or a $25 million bid and a road project, we're playing market economics, they're playing geopolitics, we're playing different games. And so I think in the slightly longer term, we need to rely on kind of the compelling power of that attractive, positive vision, which people can laugh at that, but I see it in action everywhere on all the time. We also need to identify key strategic geographies that matter and focus our effort in places that matter most, rather than trying to spread it out everywhere. And I think you see that in the reconstitution of US alliances and partnerships in the quad. We see it in the revitalization of NATO and sort of the digitization of the alliance now, helped in a lot of ways by Vladimir Putin.

Patrick Cronin:

You've pointed to really the two sides of the job here, of both trying to create rules of the road and have that positive vision drive this vision, and on the other hand, some of the perils of this technology that could be disastrous. I want to ask you a question just about each one of those. The former, where, Nate, have you had the most success in bringing allies and partners together on some common rules dealing with some aspects of these new technologies? And then maybe we'll get to the peril question maybe, which about AI I want to talk about. Yeah,

Nate Fick:
Yeah. Great. Let's do both. And look, these are complex issues. There are plenty of simple answers, simple narratives. They're easy to understand, very compelling and totally wrong. So yeah, there's going to be nuance and complexity in a lot of what we're talking about here. So I feel like almost everything we discuss is going to have this duality to it if we're going to be intellectually honest. So successes, look, a success that long predates me is the 20 year ground game diplomacy effort at the United Nations to develop the framework for responsible state behavior in cyberspace.

And this was, again, kind of ground game diplomacy, classic one yard and a cloud of dust kind of stuff, but it resulted in this framework that has three major elements. The first is agreement that the body of human rights law that has developed over time in the kinetic world, in the real world, applies in the digital world, that people's rights offline extend online. The second element of it is a set of principles, of norms governing state behavior in cyberspace below the threshold of the use of force. And the third element is a set of confidence building measures designed to minimize the risk of inadvertent escalation. And what's important here is that this very complex, very robust three-part body of agreement has been unanimously endorsed several times by every UN member state. I challenge anybody, anybody here today come up with another topic. Name one thing in today's geopolitical environment where we could get unanimous UN member state endorsement.

We couldn't do it on a topic like child pornography online. We can't do it on anything. So the fact that that exists is actually a superpower in terms of infusing our work with legitimacy and moral authority. So that's a success in terms of building a big tent and getting people oriented on some principles where there is a sense of shared norms. Now, I'm the first to acknowledge our adversaries often don't give a crap about our norms and values. They disregard the responsible framework all the time. So that gets to the other half of this Janus-faced dichotomy. But last word on the positive side. So I saw this in action in Bucharest last fall when Doreen Bogdan-Martin was elected Secretary General of the International Telecommunication Union.

I thought I'd be sworn in a fancy little ceremony in Washington. I got sworn in by a notary public at a UPS store in Maine, with a line of pet people behind me waiting to mail their packages, who were completely unamused by what was happening at the front of the line, because I had to get a diplomatic passport quickly enough to get to Bucharest in order to whip votes in this election. Doreen's an American running to lead this international organization. She was running against a former Russian Deputy Minister of Telecommunications, who before that was a Huawei executive. The ITU has been at one of these international institutions that was really becoming a tool of the PRC vision. And Doreen won in a landslide. And I'll tell you, that that 11th hour vote whipping was a lot of bilateral conversations with delegations from across the developing world focused on their disillusionment with Chinese infrastructure as it had been deployed in their countries and their desire to align with the affirmative vision.

Patrick Cronin:

So on the negative side of the perils of technology, let's think about artificial intelligence, just for example. There are least, it seems to me, two major threats. One of them is a concern that was drawn by that great technology specialist, Henry Kissinger in his book with Eric Schmidt a couple of years ago about the danger of autonomous weapons and sort of algorithmic warfare, and the hint, even recently before Secretary blinker's trip, that maybe AI could be the beginning of a discussion with the Chinese on rules of the road in that, I didn't hear anything after the summit about that. I know you're getting briefed on this later and it'll be interesting to hear whether anything emerges out of that.
But that might be a common area, an interest of common interest with the Chinese that maybe they would talk about those rules, we hope. The other side of that is the disinformation side, and the deep fakes and the generative AI and what that's able to produce. With the threat to our democracies and to our institutions, and the fact that trust is already at low ebb with many of our institutions and with the electoral process, the fear of that... What's the role of US leadership in dealing with AI perils?

Nate Fick:

So let's level set a little bit here just to sketch out some context before going into the specifics, Patrick. ChatGPT, late last year, catapulted AI, and particularly generative AI into the popular consciousness, in a way that a lot of people, if they hadn't been paying attention to it, may think that this was a breakthrough, that this was a new plateau, but it wasn't. If you pull the lens back, this is just a long exponential curve. And this is just... We're just on that curve. And that curve stays steep for a long time. We're nowhere near the end of this curve. So things that seemed impossible 18 months ago are now commonplace, and things that seem impossible today are going to be commonplace in another year. So this was an awakening of the popular consciousness more than it was a technology breakthrough.

I've only been in government nine months. I was investing in this space previously. These technologies are unmatched in how quickly they've been adopted. This is the most rapid application adoption we have ever seen, quicker than anything else that came before. And again, that's not going to change. So we have a couple of things that we should talk about. We should talk about the large language models themselves, and the power of these generative models, and we should talk about their application kind of infusing everything else we do now with this capability. And then what the heck do we do about it as governments? So this sort of... Sketching the state of play from where I sit, you've got four companies right now that are all American businesses that have the most capable models. And these models require three things to develop. You need expertise. And the number of people in the world who really are in the top tier of global talent on this, it's in the hundreds right now. It's not that many people. It's not in the dozens, but it's not in the tens of thousands. It's in the hundreds. It's going to grow. But you need the people, and they're expensive, and they're sought after. You need a massive amount of computing power, huge amount of computing power. These businesses are pretty, for software businesses, they're capital intensive. In defense industrial terms, they're not. But you're talking about hundreds of millions or single digit billions of dollars of investment to kind of build a capable model, and you need a lot of data. Those are the three ingredients that go into it. And there are four companies right now that have the leadership positions in this tech, Google, Microsoft, OpenAI, and a smaller company called Anthropic. And they're all American companies. No surprise, frankly, given our technology ecosystem, the benefits of an immigration policy that makes the United States a place that entrepreneurs want to come and start and build their businesses, tax and regulatory policies that encourage business creation and growth, and then the ecosystems that develop in places like the Bay Area and Boston, and hopefully increasingly other places.

So those are the models that are the most capable. I think a very interesting question as we think about timelines, how much time do we have is how long is it going to take to develop a fifth model that has that cap capability, a fifth model that's either built by a company that's less trustworthy or a model that's open sourced? The best answer I can get is it's less than a year. We don't have a lot of time. If this is 1945, we don't have until 1957 to put together some sort of
a regulatory or governance infrastructure. So that's just by way of context. I think I agree... The near term risk practically that I am most animated by is disinformation and misinformation, and what the kind of rapid dissemination of fake content to flood the zone, particularly in a political context, does to our discourse. So that's a big one. And then...

Nate Fick:

... does to our discourse. So that's a big one. And then I would say that's the... When I was a Marine, we used to talk about the MLCOA and the MDCOA, the most likely course of action and the most dangerous course of action. The most likely course of action is that we embark on a political campaign season now where it is harder than it's ever been to separate truth from fiction. That could have huge corrosive effects, it could also have a galvanizing effect to help us get our arms around this. The MDCOA, the most dangerous course of action, is the application of these technologies in lethal terms. So autonomous weapons, biotechnology, to some extent cybersecurity, but the applications of AI to do really nefarious things using existing lethal stuff. So what are we doing about it? Am I going on too long?

Patrick Cronin:

Not at all, no. I mean, even on that issue, the idea of zero days that have not been exploited by Russia and Ukraine, but you're thinking about China prepping the battlefield or whatever, what's already in the system that we won't know about until that crisis occurs, and then suddenly, wow, all of these things were planted in during this peace time?

Nate Fick:

So yeah, this was a world I lived in for a long time. When you're on the part of the curve where you're connecting a billion things to the internet every quarter, and you're in this happy-go-lucky, laissez-faire software developer world, where everybody's spinning up virtual machines and writing code and open sourcing things, yeah, convenience goes way up and cost goes way down, but man, you introduce a lot of untrusted code and all the vulnerabilities that come with that.

One of the good applications of AI that I'm most excited about is using AI to write better software. That's pretty exciting, to see the bug rate go way down. I mean, you can imagine it is a road to really realize one of the pillars of the national cybersecurity strategy, which is really focused on building better software, and incentivizing that, and creating incentive structures and liability, punitive structures, to require the developers of software that we all rely upon to build good stuff. We have a software equivalent of... What was the Ralph Nader car? Was it the Pinto? A lot of equivalents of Pintos out there on the software road.

Patrick Cronin:

Or the Corvair, I'm not sure which. But either one, there were some bad lemons. Let's go back to the question of institution before we open up for some questions. And the workforce, the talent, what is the art of the possible here to build? I know both of our wives work at universities where they have a lot of young talent that they're seeing in the tech space. Are we able to track them into the State Department, into the Government, and build the kind of expertise? I know from Congress, to the executive branch, to the private sector, we need a lot more expertise to deal with this high-tech world we're in.
Nate Fick:

I actually think we can attract them. I think that, and this isn’t purely generational, but it's a truism, I don't have to go out and in my recruiting pitch, explain to young people why this is going to matter, they'll know. And there are still an enormous number of public minded people in the United States who want to spend some portion of their life and career giving back to the institutions that have made all of this possible for all of us. The question, I think, is, do we wreck them once we get them? That's where we're trying to reform the institution, and modernize the institution, so that it can compete in this arena, so that we're not recruiting the best and then burning them out and spitting them out in frustration in three years, or five years.

I'll be concrete, I'll give you a few examples of things that we've succeeded in doing in the last year. We've created a course at the Foreign Service Institute to train cyber and digital policy officers, with the goal of having a trained officer in every embassy around the world by the end of next year. If we build a little silo of excellence in Foggy Bottom, we will have totally failed, because State Department's work happens out at the edge, it happens in all those posts around the world. So we need to make sure that there's expertise on the front lines all around the world. That's one thing.

Second thing is we've created a secondary skill code in the foreign service. So below the level of cones, political, consular, economic, people who go to the course, work in a tech job, can get a T in their record. It's a T, a tech code. So we can tag people over time, we can tag jobs over time, it's tech people or tech jobs. We can begin to match people in jobs, we can begin to flow incentives to people. It's an important piece of institutionalizing this in an 80,000 person organization. We've created an award for excellent achievement in technology diplomacy, and we give people cash, 10,000 bucks a year in first place, five or two in second and third, handshake with the secretary, and acknowledgement that, “Hey, you did something awesome in tech diplomacy for America.”

And then last thing I'll leave you with on concrete change. I said in my confirmation hearing, I can imagine a future where every credible candidate to be a chief of mission anywhere in the world has a demonstrated commitment to these topics, recognizes they're important, has some basic fluency in them, is infusing these issues into every other policy issue at his or her post. And for the first time this year, in the selection criteria cable that went out for ambassadors, there's a robust set of requirements around technology issues.

So yeah, I think we are actually turning the crank to institutionalize it. One of Secretary Blinken's top priorities, going all the way back to my first conversation with him, was exactly this, it was modernize the institution. Because look, I mean no matter how long I and we are here, it's not long, the institution's going to endure, and these issues are going to be foundational for as far into the future as we can see.

Patrick Cronin:

State Department's come a long way in 20 years. When I worked for Colin Powell and he was just trying to bring new computers into the State Department.

Nate Fick:

Don't get me started on that, that's the IT side. That's a big problem, not my problem.
Patrick Cronin:

I know. I have more questions for you, Nate, but I want to turn to the audience and see if we have some questions. We have a microphone, Morgan's got the microphone. We'll start here and then there, those were the first two hands I saw, and then we'll come up front.

Nate Fick:

Great.

Patrick Cronin:

If you just quickly identify yourself and keep the question brief please.

Bertram Lee:

Bertram Lee, senior policy counsel for data, decision making and artificial intelligence, with Future Privacy Forum. Thank you so much for your comments. I was wondering, how does the State Department understand the need for more data, and more diverse data, in order for US companies to continue to be world leaders, with the idea that there is a significant pushback about AI bias, internally, particularly with companies pushing back on privacy regulations that require testing and auditing, and so on and so forth? How are you squaring those two things? Because as you know, we need our technology to serve the world the best in order to compete with our foreign adversaries.

Nate Fick:

Yeah, good question. I mentioned the three ingredients to these sophisticated AI systems. One of them, of course, is the data. It's garbage in, garbage out, right? Your results are never going to be better than the data you have. They may often be worse, because it depends on the algorithm too, but it's never going to be better than the data. So making sure that you have inclusive, representative data sets is key.

It's why the president is meeting with civil society leaders on this topic in San Francisco. We've gotten this, we, the imperial we, we government, we companies, we, our society generally, have gotten this wrong, glaringly horribly wrong in some previous generations of technology. We have an opportunity here to learn from our mistakes and try to get it right, and that means baking in some of the considerations that I think are behind your question with respect to bias. It is at the forefront of the considerations as this administration puts together a governance agenda with the companies on AI. My sense is it's at the forefront of their agendas as well. Now we need to make it real, but the conversations are happening.

Let me just say one more word on this, because I didn't quite get to it when we were talking about AI. The general approach that we're going to take is, starting with those big four companies, those companies are making voluntary commitments around what the guardrails are that they will voluntarily sign up to. Voluntary commitments by definition will not stifle innovation. They, I think, also are likely to be a starting point, but not an ending point. But they have the great benefit of speed. We've got to get something out in the world now and then we're going to iterate on it and build on it over time.

Patrick Cronin:
This gentleman in the back row there.

**Charles Faulkner:**

Charles Faulkner with ICF. I've a question about, I've spent a lot of time on resiliency and interoperability with some of the work that we do with DHS, how are you thinking, from the department's perspective, about capacity building with our partners abroad? From a foreign assistance perspective, making sure, and not just our more contemporary partners, but some of those emerging partners where their populations are growing, and obviously their capabilities, right?

**Nate Fick:**

Yeah. When I was a technology CEO, I often argued against my own narrow self-interest, and said that we should be thinking about people, process, and tech in that order. I think that's absolutely true in this role, in this domain. It is easy to think that there's a technology solution to so many of these problems. Generally, there isn't. Generally, it's people, it's process, and then only finally is it tech. We could spend tens of millions of dollars deploying cutting edge tech to improve the cybersecurity of country X, but they don't abide by Patch Tuesday next year, there're going to be holes you can drive a truck through in a very short period of time. I think all of which is to say that I agree with the premise of the question, which is we got to get the people element right.

The demand for capacity building around the world is just overwhelming, in a really positive way, I mean an extraordinarily positive way. The fact that nearly every society is focused on it. Generationally, hundreds of millions, billions of young people globally seek it, want it, and we have a lot to offer. So we've got a robust set of programs that are available. The demand far out exceeds our capacity to deliver, which is probably, it's better than the reverse problem. One of the things that we're working on now with the department is how to increase our capacity, our ability to meet some of this need. I think an important element of that is a dedicated cyber, digital and emerging technology assistance mechanism.

If you believe the framing that I gave at the front about why this stuff matters, then in my view we're in a bit of a paradigm shift, a phase shift, inflection point, not unlike, probably even greater than, after 9/11, when we did in fact revamp assistance mechanisms to do counterterrorism assistance better. We still have mechanisms that are not built for the technology era, in terms of authorities, speed, autonomy, and we are making a real push to change that.

I will tell you, I'm really gratified that it seems to have bipartisan support on the Hill. One editorial comment, I and we in the Bureau, we benefit immensely from the fact that this entire enterprise came out of the bipartisan Cyberspace Solarium Commission. The last administration got a start on getting it institutionalized, this administration picked up that ball. There's been a fair degree of continuity on this, and that has given the work, I think, even greater standing and power, particularly overseas, because it's viewed as something on which the United States might actually be able to maintain consistency.

**Patrick Cronin:**

The international capacity building is a critical demand out there from allies and partners. I know in the Asia Pacific and Southeast Asia, so many countries would come and say, “Can you
please teach us more than Cyber 101 though? Can we go beyond that? And how do we build that capacity?” It's a tough, tough issue.

I want to just briefly, before we go to another question, Nate, ask you about institutionalizing that education within the State Department. You've talked about the Foreign Service Institute, I've lectured there, it's a great institute, but it doesn't have the resources that they have at the Marines or the Defense Department to do massive training and education. What are you doing, what can you do to institutionalize this beyond this ambition of training one officer for every embassy?

Nate Fick:

I'll tip my hand a little bit. I don't want to say too much, because we've accomplished our 101 level objectives, now we've got to move on to the 201 level objectives. But I think you're absolutely right, Patrick. The FSI course is necessary but insufficient, it's the first step. I am struck that DOD is an organization, the Marine Corps, where I cut my teeth early in my career, these are doctrinal organizations that put a lot of value on professional education over the course of one's career. The State Department is different in that regard, and I think in this area, we would benefit from putting some more opportunities in place for members of the foreign service and the civil service to access this kind of training.

Now, we have a globally distributed team and a team that's globally mobile, so I think it meets the moment of remote, hybrid distributed learning. We should be able to deliver really high quality modules on things like-

Nate Fick:

To deliver really high quality modules on things like quantum computing, on advanced elements of cybersecurity, on artificial intelligence, on large language models, in partnership with universities or others that do this for a living. And we should be able to make that content accessible to our people kind of at will over the course of their careers. I think there's a huge demand signal for it, and we can do it in a way that's really cost-effective.

Patrick Cronin:

Great. Let's go back to questions. I think this gentleman had his hand up.

Sean Lyngaas:

Thanks. Sean Lyngaas with CNN. Ambassador Fick, good to see you. Thanks for being here.

Did Secretary Blinken raise cyber issues on his trip to China? Particularly the thornier issues, I'm thinking of things like the Microsoft disclosed campaign, Volt Typhoon, where US officials, including people at the NSA, felt that China was pre-positioning for potential future effects and conflict, and Rob Joyce told me that that was unacceptable. I'm wondering, to what extent did Secretary Blinken raise the issues on his trip? And if he didn't, why didn't he? And then if you could respond directly also to the Volt Typhoon campaign, do you think that is acceptable behavior from China in cyberspace?

Nate Fick:
Sorry, which campaign?

Sean Lyngaas:

Volt Typhoon, it was disclosed a few weeks ago.

Nate Fick:

First of all, the debrief of the Secretary on his trip will happen when he is back, so hasn't happened yet. So I can't offer much on the details of the conversation that took place. I think kind of broadly speaking, we really do need every responsible actor in cyberspace to abide by the framework that we've all signed up to and holding critical infrastructure, civilian critical infrastructure in particular, at risk is not behavior that we can endorse or tolerate.

Patrick Cronin:

Questions will be asked again later this week it sounds like. This gentleman had the two fingers right here, yes, there's a microphone. I'm sorry, and then we'll come over here, sir.

Patrick Wilson:

Good to see you again. Patrick Wilson. My question, I guess maybe prompted by the CNN inquiry too, is today's news about Huawei, the Cuba listening station, which has come up a lot. And I'm wondering what your view is, US companies are making billions of dollars still selling chips to Huawei with a license from the US government, which seems not consistent with US policy. Do you think that's just going to continue where large American technology companies selling to Huawei, every single Huawei phone around the world powered by a US provider? Seems not consistent with US policy, in light of this news today even less so.

Nate Fick:

I think that we are at a moment in time where we are all reliant upon 30 years of global supply chains that were optimized for one variable, and that was cost. And we've had little glimmers along the way of the challenges... That system that has resulted in immense benefits. Cheap goods everywhere and all the time. But we've seen cracks in the system. A ship gets stuck in the Suez Canal and it ripples through the global supply chain, early in the pandemic we saw it, and certainly now we're seeing it through a geopolitical lens. And I think we're in the early stages now of re-imagining first and then ultimately rewiring that global supply chain to account for factors in addition to cost. Factors like resilience and availability. And it's not a task for any one country, any one company. It is going to require large global multi-stakeholder coalitions. Lots of countries, lots of companies.

In my view, the kind of orienting principle is de-risking not decoupling. It's complex. It can't happen overnight. It's a big realignment that happens, frankly, over a period of decades. I mean, look how long it takes to build a premier chip FAB. This doesn't happen fast, but it's happening. It's happening everywhere. And I think we need to continue creating incentives for that rewiring in ways that are going to be maximally resilient for this next phase.

Patrick Cronin:
This gentleman over here on the aisle. That reminds me about the science and technology agreement with China is set to lapse in August. I mean, is that the kind of thing that de-risking means you keep going with that agreement in general, but then you try to have the small yards, high fences that Jake Sullivan's talked about? Or does that lapse and we just fence it all off, we can't protect ourselves from a kind of predatory nation?

**Nate Fick:**

Yeah. Look, they're highly credible points of view on both sides of that one right now. And I continue to believe, again, that there's a little bit of nuance and complexity to all of them. Is it possible to collaborate with China on AI for good, on applications of AI in the service of UN Sustainable Development Goals, things like climate research and weather forecasting and medical diagnostics? And there ought to be ample opportunity for wide global cooperation on some of these issues. And then certainly there are going to be areas of sensitive technology where we're less likely to find common ground.

**Patrick Cronin:**

Yes, sir.

**Mike Sugden:**

Thank you so much for coming out. I'm Mike Sugden with the Foundation for Defense of Democracies. And I just was wondering a follow-up to the capacity building question, are you in a position to assess how much your office will need budget wise to further your capacity building efforts or complete whatever goals you've set?

**Nate Fick:**

Yeah, so we're in the opening stages of that. In its first instantiation CDP had about $37 million in assistance funds. The number that we've been discussing in public and on the Hill has been $250 million as a meaningful increase. That will still fall far, far short of the demand.

**Patrick Cronin:**

We have time for a couple more questions. Yes, right there on the back and then right here on the aisle, those two. Thank you.

**Ryan Lovelace:**

Hi, I'm Ryan Lovelace from the Washington Times. Thanks to Hudson for having this event. Greatly appreciate it.

My question has to do with the vast middle, perhaps other countries, international cooperation. Germany's national security strategy last week mentioned that it fundamentally rejects the idea of hack backs. When you are responding to malicious cyber activity, like the kind that State Department warned about earlier this month regarding the DPRK's targeting of Americans, are hack backs on the menu of appropriate options? What should US government's response be?

**Nate Fick:**
So when we talk about hacking back, I draw a bright red line, a bright red line, between government activity and corporate activity. I think that a foundational principle in our society is that the government has a monopoly on the legitimate use of force. Otherwise, we descend in vigilantism. So I don't care if you're a Wall Street Bank or a big defense contractor that's spending a billion dollars a year on cybersecurity, you're not going to win a fight with the PLA. Not going to happen. You're not going to win a fight with the Russian intelligence service, with large state sponsored actors. So we really need companies not to pick fights that only the government can then finish. So that's where I draw the bright red line.

Then if you're focused on the government side of the line, I think that offensive cyber activity is a tool of national power, like every other military intelligence, economic, diplomatic, informational tool. There needs to be kind of robust democratic oversight within the context of the rule of law. But these are legitimate operations that can absolutely advance our national interests, and they're one of many tools at our policymakers' disposal.

Patrick Cronin:

Good. And on the aisle here.

Jasco:

Hi, my name is Jasco with Sumitomo Corporation. Thank you so much for taking the time to talk to us.

It is so obvious that digital economy will improve economically and societally have a major impact on underdeveloped countries. In the meantime, those countries tend to have less developed rule-based order. In order for companies to go into the market and, how do you say, provide service. I tend to see two major problems, which you already addressed. One is government's intervention, surveillance, digital authoritarianism. Also, Chinese playbook, IP theft, and subsidy. S.

O, if I were to live in La La Land, I wish for two things. There is a measure to prevent those authoritarian regime to intervene telecommunications. There is international norm or like a rule to be developed to prevent authoritarian regime to intervene in telecommunications operation, that's number one. Number two, to develop Huawei alternative in developing countries. Are there any efforts to do it? And I would appreciate your insight into.

Nate Fick:

Sure, thanks. Yeah. I think as you rightly point out, these things are somewhat related. Government surveillance and untrustworthy infrastructure are different angles on a similar topic. During the Summit for Democracy, a couple of months ago, the US announced an executive order prohibiting the use of commercial spyware by the United States government. I think it's a terrific positive step to establish that norm. To walk our talk, if you will, and begin to build the coalition around that norm now globally. I think it was launched with more than 10 countries in support, and that number has grown.

On trusted infrastructure, the arguments in favor of trusted infrastructure I think touch on a bunch of different areas. One is national security. The reality is it's very hard for the United States to share information or sensitive intelligence with partners whose communications infrastructure is insecure. So it is an inhibitor to closer partnership.
Second factor is economic. Most countries around the world are hopeful that they can catalyze and grow a domestic innovation economy. They want to attract big multinational technology companies, and they want to foster entrepreneurs domestically who are growing their own businesses. It's going to become less and less likely that large multinational tech companies will invest in geographies where there's untrusted infrastructure because it puts their IP at risk.

And then the third is human rights. And the fact that even though we have not codified a federal privacy standard in the United States, and I think we should, there are expectations in democratic societies around data privacy and individual rights that are not recognized by these more authoritarian regimes, that are not recognized by the untrusted vendors who are beholden to the regimes, by kind of law and custom.

So they're related points. I hear you. I agree that they are inhibitors to international investment. And one of the most compelling arguments we can make around the world is exactly that one. That if you really want to build a 21st century technology economy in your country, you will be greatly helped if you do it on a trusted architecture.

**Patrick Cronin:**

Nate, an hour flies by and our hour has flown. Thank you so much for joining Hudson today and joining me today to talk about US leadership and tech diplomacy. I, for one, am just delighted that you are the man in charge at those interagency meetings, inside the State Department, working internationally to try to advance our interests on a lot of these issues that the technology just intersects all of this diplomacy, all of our policy. And delighted they have convinced you to be in this position. So I hope-

**Nate Fick:**

Honored to do it. Thanks for having me. Thanks for being here.

**Patrick Cronin:**

Please, thank you-