Nathaniel C. Fick
Ambassador at Large
Bureau of Cyberspace & Digital Policy

Defense Writers Group
Project for Media and National Security
George Washington School of Media and Public Affairs

12 April 2023

Moderator: Just to remind everyone of the ground rules which you know, starting at this minute the conversation is on the record, but there is no rebroadcast of audio or video of today's discussion. I'll ask the first question and then Ryan Lovelace of the Washington Times is here. He'll ask, then we'll go around the table and we'll give Ambassador Fick a couple of minutes before 9:00 o'clock for any wrap-up comments. He does have an absolute hard stop a couple of minutes before 9 and since we're starting on time we'll be able to do that.

He's truly a man who needs no introduction, but I'll do it anyway. Nathaniel C. Fick is the State Department's very first Ambassador at Large for Cybersecurity. If you read his bio, he served with distinction as a Marine Corps officer in both Iraq and Afghanistan and his book One Bullet Away is truly one of the best memoirs of the forever wars. If you want to read a great book that will take you there, what it felt like, I highly recommend that.

He was a founding father at the think tank CNAS. In full disclosure, I was a writing fellow there, so I'm also biased in that regard. He founded a cybersecurity firm. As I mentioned earlier, he hands out donuts to parents at his alma mater's graduation.

Mr. Ambassador, thank you for being here. We are honored to have you.

Ambassador Fick: It's a pleasure, Thom.

Moderator: The opening question, if I could, we're meeting on the very first anniversary of the Bureau for Cyberspace and Digital Policy. Could you tell us what you think are some of the most significant accomplishments in this year and then what is number one through five on your to-do list.

Ambassador Fick: Sure. The Bureau was created, it was

initially suggested in the Cyberspace Solarium Commission years ago. And the last administration got started on setting this up, ran out of time, and so as Thom said, April last year it was finally established. It's an effort to integrate and elevate the department, the country's approach to technology diplomacy.

So cybersecurity is a piece of the remit. Digital policy is another. So that's the guts of the internet. It's all the cables and fiber, the data centers, the satellites, the wireless networks that actually get the ideally free, open, interoperable, reliable and secure internet to your router, and all of that obviously crosses international borders.

There's a third bucket that is in my portfolio which is emerging technology. So the diplomacy associated with AI, quantum science, biotechnology. We have an office of Digital Freedom, so I would think of that more as a horizontal rather than a vertical. It's to make sure that all of the policies that we develop and implement in the other three areas are rooted in a foundation of rights and values. Organizationally, it reports to the Deputy Secretary, to Wendy Sherman. So it's an attempt to incubate something inside a big bureaucracy that will endure.

The priorities -- I'll give you a few different cuts on that. Oh, you asked about accomplishments, didn't you?

Let me give you sort of some organizational accomplishments and then talk about some things in the world.

Organizationally, we created this thing. We have 115 people in it right now with another 30 or so to go. I'm acutely conscious of the fact that no matter how long I'm here, I'm a short-timer as any political appointee is. It's just the nature of the world. And the only way this thing succeeds is if we can create the culture and the incentives inside the career foreign service and civil service that makes sure that the work is viewed as important and rewarding over the long haul.

Just yesterday we succeeded in creating a skill code for the Foreign Service in cyber, digital and emerging tech. This sounds weedy, and it probably is weedy, but what it means is if a Foreign Service Officer spends a couple of years in a designated technology tour, he or she gets credit for that in their record. That's the first step towards incentivizing people to seek out these jobs.

I'll give you an analog from the defense world. This kind of captures broadly what I think we need to do.

You all know that over the course of the '70s and '80s, the US had a bunch of special operations failures. Forensically one of the reasons missions like Desert One or the invasion of Grenada were such clusters is because the military didn't work well jointly. So Goldwater/Nichols in 1986, one of its fundamental tenets was requiring people to do a joint tour in order to get promoted to flag rank. So overnight, instead of having the bottom ten percent of your O6s hiding in joint tours, waiting to retire, you had the top ten percent seeking them out in order to get promoted.

I said at my confirmation hearing, I can imagine a future where every credible candidate to be a Chief of Mission, every future US Ambassador anywhere in the world, has to have some demonstrated understanding of technology issues, and a willingness to engage on that, because please, somebody, give me one area of US diplomacy today where tech isn't totally infused into it. You can't track this East Asian diplomacy without tech diplomacy. You can't do human rights work without tech. You can't do climate diplomacy around the world without tech. There isn't one. So we have to infuse it into the culture of the place and reward people for working on it. That's the internal kind of focus and accomplishments.

Out in the world -- I'll give you my last thing internally. We set up a course at the Foreign Service Institute, the school in Arlington where the Foreign Service is trained. We have a course now in cyber and digital policy and a goal of putting a trained cyber and digital officer in every embassy around the world by the end of next year. So we'll have somebody in every embassy globally who has some basic training and understanding of these issues.

That translates to out in the world. I'll give you ua couple of kind of episodic things.

My very first diplomatic trip was to Romania last fall, to Bucharest to [whip] votes in the final days before the election for the Secretary Generalship of the ITU, the International Telecommunication Union, which is one of those organizations that we all should care a lot more about than we do.

The idea was started in 1865 to ensure that telegraph standards on different continents were interoperable, so that US telegraphs could talk to Asian telegraphs, could talk to European telegraphs. And that mission of global connectivity continues right down into the digital era today.

So the last Secretary General of the ITU was a Chinese official. In the election that happened last fall we had an American running -- Doreen Bogdan Martin -- against a former Russian Deputy Minister of Telecommunications, who before that was a Huawei executive. So this was like a comic book script of an election scenario. It was a huge effort on the part of the US government for a long time, culminating in this dedicated vote-gathering exercise in Romania. And Doreen won. So now we have this window of opportunity, maybe four years, hopefully eight, with her at the helm where we can really use this US body to help ensure that the standards and the norms around telecommunications are more aligned with openness and security than they are with a more authoritarian approach. I'd say her election was our first win as an organization.

I'm talking too long. I'm going to pause there. I'm happy to talk more about priorities or whatever you want me to do next.

Moderator: That's great. The first three questions will be Ryan, Jeff and Dmitry.

DWG: My question has to do with international cooperation and kind of the new [inaudible] partnerships that [inaudible].

The last [inaudible] exercise had three countries in the Asia Pacific, and the upcoming one's got more than 30, and General Nakasone, the Cyber Commander, just got back from [inaudible]. So my question is, are you, is the US with international partners preparing for some kind of cyber conflict with China?

Ambassador Fick: I'm the diplomat, so my fervent hope is to avoid cyber conflict with China, but at the same time of course bolstering, a key piece of our remit is bolstering cyber capacity among our allies and partners all around the world. I've been all over the Indo-Pacific in my brief tenure already. I'm going back next week. The same across the NATO alliance and everywhere else in the world. The thing about the digital space, of course, is that it's global in scope and risk

federates across connected systems.

So cyber in security in a place that may geographically seem pretty remote, if that place is connected to other places that are more strategically central, the risk swims upstream. So you kind of can't ignore anyplace. But yes, cyber capacity building of our allies and partners is one of our top-most missions.

DWG: -- trip to Romania, you're headed back to Asia. How have people received you? Do they want America's help more than perhaps they have in the past?

Ambassador Fick: It's actually been incredible. I have been, me personally, amazed to see the demand signal around the world for American assistance on these things, but also for American leadership in the bodies, the multilateral bodies where these things get adjudicated.

So Albania. There's another early thing that I got involved in. Last summer Albania was the victim of an Iranian cyber attack because Albania had given refuge to the MEK when the US pulled out of Iraq. Albania's a NATO member. The US has been advocating I think around the world for a long time for countries to digitize their government services in order to provide better services to citizens and to help cut corruption out of the system. So e-Albania was a pretty elegant response to that request so that Albanians could register to vote online and get their driver's licenses and pay their taxes and other stuff. The Iranians just thumped them.

I went to Albania with Ambassador Linda Thomas-Greenfield at the UN and we stood in the main square in Tirana with our Ambassador there, Yuri Kim and kind of had a two-fold mission. The first was to remind the Iranian attackers that Albania is a member of NATO and this is a problematic path that we don't want to go too far down. And second, to coordinate really intense cyber assistance to Albania in order to, again, in an information sharing body like NATO, risk federates. So there can't be soft underbellies.

So Albania appointed a cyber coordinator, a guy named Igli Tafa, who's very capable. The US has quickly rolled out $25 million cyber assistance to Albania. We marshaled a bunch of private sector partners to come in and work with the Albanian government. Got e-Albania back online. Put basic security

measures in place, and then started the process of long-term capacity building.

So that model in Albania, we see demand for that everywhere. We're doing something pretty similar in Costa Rica right now, for example. It's global in scope.

DWG: Ambassador, thank you very much for doing this.

Just a few weeks ago we heard from a senior Defense official about how countries who are willing to do something kinetically, they're sure as heck willing to do it in cyber. There's been a long discussion about what the redlines are perhaps when it comes to cyber warfare.

What are you seeing in terms of where those redlines are, if they exist at all, whether it's a nation state or a lone actor, and to what degree are you involved in trying to establish redlines or at least norms when it comes to what is a legitimate cyber target and what's not?

Ambassador Fick: Good question. Let's start with the norms.

Over the course of more than 20 years there as this incredible ground game, diplomatic effort at the UN. Really like one yard and a cloud of dust work. Totally thankless, slow, hard, frustrating, that resulted in, in the course of a body called the Open Ended Working Group and its predecessor organizations. Resulting in something called the Framework for Responsible State Behavior in Cyberspace, which is a pretty comprehensive set of norms, voluntary norms, and confidence-building measures. That's all unremarkable. Here's the remarkable part. It has been endorsed repeated now, unanimously, by every UN member state. That's kind of a stunning achievement. I would challenge anybody around this table to identify a single issue on which we could get unanimous UN member state endorsement in today's geopolitical environment. You couldn't get it on an anti-child pornography measure online. You couldn't get it on anything. So the fact that exists is kind of a super power from a normative standpoint. It gives incredible legitimacy and moral authority to this framework of responsible state behavior.

That's all great. The challenge, of course, is our adversaries tend not to care very much about our norms, even if they endorse them. Right?

That gets then to the next piece I think in your question which is okay, when the norms are insufficient, how do you kind of put guardrails on good behavior? I'm generally a believer that most of the mechanisms that we're familiar with should extend into the digital world as a starting point. So we don't need a new set -- the Russians and the Chinese, for instance, would love for us to start fresh in the digital world and build a new architecture of human rights law and norms. And the United States says no. We have a century-old body that is going to extend into the digital world and we'll talk about adjusting for new and different circumstances if that's required, but we're going to start with what we have. I think the same is true in this regard. That generally, like a sense of declaratory policy and escalatory policy, that deterrent framework is something we need.

Of course a little bit of ambiguity is always going to be the case in something that's as fluid and dynamic as the cyber world, but generally speaking, I think we're in a 25 year old deterrent hole where our adversaries have done things to us using cyber means that they never would have done in the kinetic world because they knew they could get away with it and they did get away with it. From stripping critical IP out of American companies to interfering in elections to compromising the personal data of citizens to harassment and worse of journalists. They've gotten away with it. So we have a deterrent hole that we have to dig ourselves out of.

DWG: You mentioned Russia, China involved in the [inaudible] big four when it comes to cyber adversaries. What have you learned about what your role needs to be based on what we've seen with cyber in the Russian invasion of Ukraine, and also looking ahead to what this means for a potential Chinese invasion of Taiwan?

Ambassador Fick: I've spent a lot of time and energy in NATO, in Eastern Europe, on Ukraine. We're meeting again soon with Ukrainian counterparts. I think a couple of things. The war in Ukraine, at least in my little slice of the world on the digital side, the war in Ukraine has fundamentally transformed how we think about public/private partnerships.

I was a CEO before I built the cybersecurity software business and I met a lot with government counterparts and they would talk

about public/private partnership and my eyes would glaze over because it generally didn't mean anything. It really does actually mean something in this context. I'll give you a few examples.

Before the invasion on February 24, last year, with the help of the private sector, the Ukrainian government migrated its entire government enterprise to the cloud, and that gave them the ability to continue to communicate and provide services to citizens even when all of the towers were smoking piles of twisted metal. That actually was an extraordinary accomplishment.

Second, proliferated resilient satellite communications. Game-changer in every sense.

Third, there's been a lot of public speculation about why Russian cyber attacks in Ukraine, why there were no Russian cyber attacks in Ukraine. There were a lot of Russian cyber attacks in Ukraine. They just didn't succeed, and they didn't succeed because the feedback loop between the software vendors with stacks deployed in Ukraine and the Ukrainian government's and other governments', that feedback cycle to adjust and patch and blunt the attacks was fast and it was effective.

There are a lot of lessons there that are portable to other scenarios, to get to your question.

Moderator: Dmitry?

DWG: Good morning, Mr. Ambassador. Dmitry Kirsanov with TASS.

This is actually sort of a follow-up to the question about redlines. I wanted to ask you about the arms control in cyberspace. The United States has frozen obviously, the cyber dialogue with Russia. I don't know if you have one with China right now or not. And is this even on the agenda for you? The idea of having some kind of a cyber treaty, be it bilateral, trilateral, multilateral? Or this is just on the backburner right now and you're not really thinking about this because of the whole geopolitical situation?

Ambassador Fick: Again, as a general rule we're extending existing bodies of international law into the digital domain rather than advocating for the creation of new digital-specific

treaties. And the US is trying to lead by example in important areas of arms control, if you will, in the cyber domain, I think exemplified by the executive order a couple of weeks ago prohibiting the use of commercial spyware by the US government. And that I think is an effort to acknowledge that the human rights elements of this, the economic elements and the national security elements are inextricably interrelated. And one other word on that EO that I do think is maybe worth noting, it's not a static tool like an entity list. It's not a list of companies, it's not a list of technologies. Given the dynamism in the space, static lists like that are too easy to evade. You can redomicile, you can reincorporate. There's a fluidity to all of this. It's a factor-based prohibition which is, we think, much more flexible, much more dynamic, and better suited to sustained effectiveness at the pace of technology change and frankly commercial kind of flexibility.

DWG: Are you engaging with the Russians and the Chinese on trying to at least have some rules of the game at this point? To have those guardrails that you mentioned so this [inaudible] would not just spiral down uncontrollably?

Ambassador Fick: I think one of the tenets of diplomacy in my world, in my view, is that it's most important when it's most difficult. It's important, essential, to maintain the channels of communication when things are hard. So yes, I'm across the table from Russian counterparts with some frequency. And with the Chinese as well. I can't get into a ton of detail about it but we do maintain a channel.

DWG: Thank you, sir.

DWG: Part of your remit as described this morning is promoting cooperation, US norms, things like that. And I'm wondering if this new leak of Ukraine intelligence that burst forward about a week ago now has made your job as a diplomat harder? Have any allies or countries reached out to you saying I don't know if I want to work with you now because of what I'm reading in the paper, what I'm seeing online? And if they haven't, what would you tell them if someone called you up and said I have a problem because of this leak?

Ambassador Fick: This is one topic where I just am not able to spend a lot of time talking this morning. For a host of reasons. I'm just not able to talk about it.

DWG: Switching gears then, you sort of touched on this in your first answer, talking about Albania and Costa Rica. You talked about a dedicated cyber assistance fund, kind of foreign aid. I'm wondering if in your mind you have a dollar figure in your head, how much would be required for that sort of thing? CISA had similar [inaudible] for states and local governments. Do you have a dollar figure in mind? How have talks gone? In your mind, would that come up in next year's budget or be stood up immediately?

Ambassador Fick: I think the basic need here is a dedicated mechanism that can move quickly enough to be useful given the pace of cyber threat actors, and our current assistance mechanism is set up to do other things. It's not architected to move at this pace. And it doesn't have the kind of flexibility that you need to address cyber issues.

For example, a lot of assistance dollars are actually not able to support military or law enforcement organizations. That's a challenge in the cybersecurity space when those are exactly the organizations that own those capabilities in partner countries where we may want to go help out. So there's an architecture problem, there's a speed problem.

So yeah, I am advocating for the creation of a dedicated, and I would broaden it a little bit, it's cyber digital and emerging tech. So a technology assistance fund and account. My sense is there's pretty broad bipartisan support for it on the hill, and there's a relatively recent historical analogy for it. We did it after 9/11 with counterterrorism, the NADR account, and that kind of body that sought to provide the sort of speed of flexibility that was needed at that moment. I think there's a pretty broad awareness that we need to do it now.

DWG: Any dollar figure in mind? Your like back of the envelope think, you know, number of countries, number of --

Ambassador Fick: I am under no illusions. We cannot and should not look to deliver sort of Albania-like levels of assistance everywhere that need it. There has to be some clear sense of prioritization and our cyber assistance needs to serve, our digital assistance needs to serve our foreign policy priorities. So it's not, the number's not $25 million times 192. That's not the number. But we're in the process of figuring out what can

both meet the need and be achievable.

DWG: Would you submit legislation to the Hill or hope the Hill comes to you with legislation?

Ambassador Fick: We're in a two-way conversation on it right now.

DWG: Thanks for taking my question.

AS you know, the Pentagon has been doing what is called defense forward, sending cyber teams into Europe, Eastern Europe, to defend American interests both in the context of what happened after the 2016 election and for other efforts.

Now in your dialogue and conversation with other countries, is this something that other countries -- are you seeing that they want to emulate similar kind of defend forward type of cyber operations? Are you okay with the idea of that becoming a norm as you go forward?

Ambassador Fick: I talked earlier about the kind of state of global demand for US engagement and support. I would put the hunt forward capability in that budget. I'm not sure I've been anyplace in the world where there wasn't demand for hunt forward presence.

DWG: When you say hunt forward, you're talking about American presence in those countries?

Ambassador Fick: American presence.

DWG: What about their own? Let's say, for example --

Ambassador Fick: Yeah.

DWG: -- wanting to supply cyber people in other countries.

Ambassador Fick: I think we have an interest in our like-minded allies and partners being capable and sharing the burden. So obviously the work needs to be technically adept and it has to be aligned with our sense of the norms and principles and values that are intrinsic to doing this stuff well. But I think there's more demand for the capability globally than we can right now meet.

DWG: Are you trying to draw some norms as opposed to letting this be kind of a free-for-all? In the context of the United States deploying, maybe there are already some rules in terms of do's and don'ts, but --

Ambassador Fick: It's so far from being a free-for-all. This is incredibly tightly regulated and controlled. It's nowhere near a free-for-all. It's in accordance with kind of host nation desires and their objectives, and it's fundamentally aimed at cleaning and securing their networks.

There's a misconception I think about hunting. Hunting is defensive, not offensive. Hunting is fundamentally cyber defense. It is the securing of allied and partner networks. And I think a conceptual shift in hunt forward in the last couple of years ha been kind of the old adage of moving from giving somebody a fish to teaching them to fish. It's become an important piece of our capacity building work.

DWG: [Inaudible] Policy Institute.

I'm interested in your comments earlier about the importance of this being a public/private partnership and how that's growing [inaudible]. In Ukraine, obviously that's [inaudible] in terms of how to deal with the conflict. Is that always [inaudible] public/private partnership? And then translated in terms of the defensive work that they're doing across [inaudible], is it [inaudible]? [Inaudible] to allies and partners? Or is it something that's [inaudible]?

Ambassador Fick: I would say the public/private aspect of all this work is as intrinsic and cross-cutting as the human rights aspect of this work, the digital freedom aspect of this work. You can't do effective government policy-making or diplomacy in any area of technology without it being multi-stakeholder. We need the companies engaged, you need civil society organizations engaged, because the government doesn't develop the tech. The government generally isn't developing the technical talent. The government generally doesn't own and control the attack surface that you care most about. So it sits in the private sector. It is of the private sector.

If I were to frame all of this work a little bit more broadly then I think it becomes clear.

So the way I'm thinking about this is technology innovation as a source of national power looks more like geography or demography than it does like GDP or military capacity. What I mean by that is, it's increasingly foundational. It's traditional measures of national strength like GDP, like military capacity, are downstream. Increasingly downstream of a country or a coalition's ability to innovate on technology.

So it means that almost everything in our future is going to depend upon our ability to innovate technologically, maintain an edge in the technology areas that matter, and this isn't a hypothetical. I'll give you an example.

Thirty years ago if we were sitting here having breakfast in 1993, the US and Korea and Western Europe together would have had what felt like an unassailable advantage in wireless networking technology. Ericsson, Nokia, Samsung, Alcatel, Lucent, Bell Labs, Motorola, this incredibly rich ecosystem of innovative companies that was in the process of connecting the world. All these things sitting in front of me are because of that. And we lost it. We lost that advantage. We took our eye off the ball, we didn't cooperate and collaborate, and the Chinese basically ran the table. IP theft coupled with PRC subsidies of Huawei ran the table globally, and they're ready to run that playbook and indeed are running that playbook in other technology areas today.

So we should be deliberate about identifying the areas of technology strength that we currently have, and we should be sustaining and defending them. And that requires close collaboration with the private sector.

DWG: Is that cooperation across nations as well?

Ambassador Fick: Absolutely.

DWG: [Inaudible] partnering with [inaudible]?

Ambassador Fick: Yes.

DWG: [Inaudible] from Australia saying [inaudible] helping to bring these private sector companies together?

Ambassador Fick: This is a major line of effort in the context

of the Quad. Exactly what you're talking about. So yes.

No country, no small group of countries can do this alone. The supply chains are global. The critical minerals are global. The expertise is global. We need the biggest group of talent, the largest grouping of GDP, the greatest number of innovative companies, the largest possible set of markets. This is not narrow.

Moderator: As you can tell, she's from Australia. Thanks, Bronte.

Questions from this end of the table?

DWG: Hi, Kimberly Underwood with AFCEA International, Signal Magazine.

How do you form your diplomacy related to emerging technology and cyber? What's the process for doing that? What are the considerations? I know you mentioned how innovation is increasingly foundational. How are you aligning that with our foreign policy priorities?

Ambassador Fick: When you say foreign diplomacy do you mean like established priorities? Or objectives? Or --

DWG: How are you going about performing diplomacy related to AI or quantum or --

Ambassador Fick: I'll give you an example.

There has been in academia and think tank land and other places, there's been some discussion about whether we should create a T12 of a T15 kind of body of techno-democracies. A new alliance, if you will, focused on this stuff. That's an appealing idea in a lot of ways. It's simple, it's clean. But I have a different point of view. I think it's very hard to do something like that and stay anchored on an affirmative inclusive vision. It becomes inevitably who's in, who's out. And that's not how we should be framing this.

We spend a lot of time talking about China and Russia, but I think the font of all of our work here should flow from a positive, inclusive, affirmative vision of what a shared technology future can look like. And that's not just feel-good

talking points.

I have two daughter in middle school. I know pounding the table and saying my way or the highway is not effective. Right? It's just not. There are smarter ways to get to the objective that you want.

The positive, inclusive, affirmative vision can have an attractive power all its own. It can provide political space for countries that maybe are historically unaligned to side with us in area that they want to side with us without appearing to be forced to make a choice. Small states maybe that have to live in the shadow of the PRC, across the Indo-Pacific, it gives them the maneuvering room to side with an open, interoperable, reliable, secure technology future.

I'm getting to answering your question which is rather than setting up an exclusive body, something that we're trying to do is infuse the technology work into the existing organizations that have broader membership and the OECD is a good example.

I was at the OECD Digital Ministerial a few months ago in Spain and we launched something with the UK called the Global Forum on Technology which is going to exist within the Secretariat of the OECD.

That's another problem with creating a new thing. Governments are really good at creating new things but nobody ever shuts down old things. So you end up with this like massive accretion of things. Every one of those things costs money and costs time and energy, and time and energy are zero sum.

Let's focus our time and our energy in the existing bodies that work and let's modernize them and introduce the technology issues across the full set of their kind of scope and responsibility.

So the GFT is this new body within the Secretariat of the OECD. It's not new overhead. It's intended to be a forum to get this broad group of dozens of countries talking about and aligned on issues related to the earliest emerging tech.

One of the first issues that we hope is going to be addressed in the GFT is synthetic biology, programmable genes. This is something where running the Huawei playbook globally on

synthetic biology gives me chills.

So that's a good example of something we're trying to get going.

DWG: Thanks so much for being here this morning.

Last week at the Atlantic Council you spoke about the creation of the international cyber strategy which I know your office is working on. Can you elaborate a little bit more on what you're hoping strategy will include? A timeline for rollout and also how you're hoping it will fit into US efforts to create new norms in cyberspace?

Ambassador Fick: Absolutely.

The NDAA tasked my office with leading the development of the International Cybersecurity and Digital Policy Strategy. Throughout the creation the drafting of the National Cybersecurity Strategy we had always thought about that fifth pillar, the international pillar, as kind of like a API that we would plug a more robust international strategy into. So that's now what we're doing.

These things need to be somewhat derivative of each other, right? The National Security Strategy, the National Cyber Strategy, the International Strategy. They have to nest and be coherent. So they have to be sequenced. I hear every night, when I go to sleep I hear the loud, ticking clock of 20 months or so to go here. And so time is of the essence.

I think a lot of the intellectual spade work has already been done. We've been doing the work. But there's a process of interagency collaboration and input and collaboration from partners and allies. That's going to take more time than the actual drafting.

I don't have a date yet. We kind of just had, we're in the process right now of rolling out the actual work.

DWG: Matt Beinart, Defense Daily.

Focusing on the [inaudible] specifically, in your discussions with other countries and bringing the US' own experience so far kind of in this nascent technology area, where are the discussions around AI in terms of the sophistication of cyber

attacks, how it's shaping that threat landscape in correlation with how AI is bolstering the defensive aspect of this? Is one far out-pacing the other? Is it you're all just kind of figuring out your way as this technology kind of rolls out and gets applied in different areas? How is that kind of shaping up in your discussions?

Ambassador Fick: The point of view that I'm advocating for is that AI's fundamentally different from any other area of emerging tech for one key reason, and that's its generative quality. In advance of another technology area, you know, a great new firewall in cybersecurity does not enable you to build an even greater firewall, but a capable AI system actually does enable an even more capable AI system. So early advantage compounds and becomes more unassailable and early its disadvantage compounds and it can become impossible to close a gap. So I do think its generative quality makes AI fundamentally different. It makes it essential that we establish norms and standards that we're going to be willing to live by when the technology is more proliferated in the world.

Another analogy I use all the time is one that Thom, you and I used to talk about this when you were writing your book. Was that like 2010? When the US had a monopoly on drone technology, I was trying to make the case that it was really important that we establish norms that we would be willing to live by when the tech was more distributed. You can argue whether we did that or not.

But I think it's imperative here that these technology genies can't be put back in the bottle. You can't constrain -- there's a very limited ability to constrain the proliferation of these capabilities globally. And so in the early days of normative development of a technology that's going to change everything in the way that AI will, we and the broadest possible coalition of allies and partners need to have normative alignment and we have to live by what we say.

DWG: You mentioned previously how we already have established kind of human right norms that can be applied to the cyber realm. You mentioned AI is fundamentally different, essentially different from other emerging tech areas. Will it take a concerted effort to maybe not from the ground up, but really focused specifically on norms, whether it is just human rights or just more broadly on AI, or can you apply some things for now

just to bet something in placed?

Ambassador Fick: We're not starting from zero, which is good. There's the White House blueprint on responsible use of AI. There's been a lot of work in defense on what responsible engineering of autonomous systems looks like. Our allies have been doing a lot of work. Back to the OECD which includes the global partnership on AI, [G Pay]. AI's a line of effort in a bunch of the bilateral, multilateral discussions that are taking place, so we're not starting from zero. There's a lot there.

I would say the challenge is more one of harmonization. Okay, there are a lot of disparate efforts. How do you pull them together in a way that is going to be both broad and inclusive and also effective?

One of the fundamental tensions of this work I think is that with breadth comes legitimacy, and with breadth comes generally a decrease in speed and sometimes a decrease in efficacy. So how do you do something that is both really broad, really fast, and effective? So I think it's a harmonization problem more than anything else.

Moderator: Just a personal note, if I could. You mentioned counter-strike in the work on drones. Again, Nate was a great conversationalist there. My new book comes out May 9th and we update that with a cyber chapter and make the case that drones, that we've lost our monopoly, that there's really even today nobody in charge of defending against drones, and it's a huge vulnerability.

Over the White House, over the Pentagon, Super Bowl, yes. But if the University of Oklahoma is playing the University of Texas and somebody flies a drone over with powder, who's watching? Who stops it? And that's a cyber problem, too.

Ambassador Fick: I'm so glad you're making that case. I don't see other people drawing that analogy. I think we have a compelling, visceral example of what not to do within all of our recent living memory and we should learn from it. I'm glad you're making the case.

Moderator: I'll drop a copy off to you.

John Ismay?

DWG: Mr. Ambassador, I was wondering when the United States is looking at a cyber attack, how do you look at crafting a response that doesn't say target civilian infrastructure -- power, water. I've heard of cyber attacks, infrastructure attacks seem to be one of those commonly mentioned. Maybe it's because they're perhaps the most easily understood. But how do you go about crafting a response to an agency the fact that it doesn't then harm the civilians in that [nation]?

Ambassador Fick: It's very rare in my current line of work that having been a classics major in college is an advantage. Usually it's not an advantage. But it's an advantage here. So I think it's simple, actually, at the level of principle. There have been two twin principles of just war theory in Western thought for the last almost 1500 years, and in American thought since our founding. Those principles are proportionality and non-combatant immunity. They need to be sacred. We're not always going to get it right, but those should be the twin north stars that we steer by. I think that absolutely applies in the cyber domain. It becomes harder to do because of the interconnectedness of networks. But there is a clear distinction, a clear distinction between how the United States thinks about targeting and how our adversaries think about targeting.

We should not be holding civilian infrastructure at risk. We shouldn't be doing it and we don't do it. Some of our adversaries do. And so I think that the principles are kind of infused in all of the decisions and all the policy-making in this realm.

Again, get back to the foundational point of we have more than a millennium of established tradition, norm, law, rule, principle in this space and they should extend into the digital domain.

DWG: What sort of things do you look for if you're not going to attack infrastructure? What do cyber attacks entail that aren't --

Ambassador Fick: Look, I'm outside my remit here because, again, I'm a diplomat. I'm not an offensive cyber targeter. But military systems obviously. Supply lines that are providing military capacity, command and control, military communications. There are plenty of things that are out there that are not

directly tied to civilian infrastructure.

DWG: Lauren Williams with Defense One.

I want to go back to capacity building a little bit. I understand that you're still figuring some things out, but you mentioned that the interest globally has increased. So I'm just curious about why they're having this permanent line item that I would assume goes up with time, if that's sustainable especially when you're talking about something like cybersecurity technology, software, [inaudible] that really don't stop changing and evolving. I would assume that countries are going to continue to communicate this.

Ambassador Fick: I believe that the essence of strategy is the allocation of finite resources against infinite priorities. That's it. I said it earlier, you can't just keep adding stuff. It's like barnacles on the bottom of a boat. Every now and then you've got to scrape them off. Things that creep, it's easy to say yes, it's easy to launch new programs. It's really hard to say okay, this one's not working, or this one's time is past, or this one is redundant. So I think that ideally, increases in technology assistance come mostly from a reapportionment of other resources because it can't just all be net new.

DWG: Do you have any other countries -- I know Costa Rica is the most recent, but other countries that are being considered for assistance in the pipeline?

Ambassador Fick: There's a full pipeline of conversations that are underway. There are assistance activities that are underway in a lot of places around the world simultaneously. And again, it's I think a representation of the fact that it's a global problem and there's huge demand.

I should also say one other thing. The demand, it's not just for assistance dollars. We need to think a little bit more holistically about what assistance means. So it's dollars. It's software. It's capacity building for people. Training people. But it's also, and this stuff is really important and has the benefit of being free. It's conceptual assistance. It's organizational assistance. It's cultural assistance. A lot of time and effort and energy and expertise goes into building out a strategy or building out a set of best practices for a bank, thinking how to secure railway infrastructure.

These things exist within the US government. We should be and we are now providing those kinds of templates to our partners so they don't have to reinvent the wheel. Yeah, they have to tailor it for their unique circumstances, of course, but I suspect that you appreciate better than most that editing something tends to be easier than writing the first draft. So let's save them the challenge of writing the first draft and provide hours that they can then edit.

Moderator: We're within the seven minute mark. We have two last questions. I'll bundle them so we can meet your 9 o'clock.

DWG: First, you talked about standard setting. I wonder if you could get into the details a little bit on what are the standard setting [inaudible] that you're in right now. What are the specific standards where there is sort of disagreement. I'm also curious if you can speak a bit about where the State Department sits right now in the approval of offensive operations. The last three administrations, the Obama administration had very tight control. Team Trump kind of took the reins off. It seems as if the Biden administration has continued that approach. One of the game points seems to be where the State Department sits in the [inaudible]. I wonder if you can talk a bit about the department's role in approving operations.

DWG: To change gears a little bit, going back to your opening remarks about the skill [inaudible] for the Foreign Service. Getting people in the door who have the kind of skills that we're talking about today.

How is that demand signal? How is that incentive working in terms of getting the right people in the right door at the right time? And as far as that goal, you mentioned as far as getting people with this aptitude, you know, at all posts overseas. Is that an aspirational goal? Is that something we're seeing progress on? Just where things stand on that.

Ambassador Fick: Let me start there. First of all, the demand among Foreign Service officers for the training in order to own the portfolio overseas exceeds our ability to meet it, which is awesome. It's great to see. I don't think it comes as a great surprise to a smart Foreign Service officer that this stuff is going to be more important and it's going to be increasingly important. So if you want to work on the core issues, on the

most important things, then this is a pretty good bet.

So we had multiple applicants for every seat in our last training at FSI. It was over-subscribed. We're doing another one in London next month. We'll do another one at FSI here in Arlington in August. And at that pace we will I won't say easily, we will meet our goal maybe easily of having a basically trained officer everywhere we need to have one by the end of next year. So that's been great.

Recruiting people to join the team kind of internally here at headquarters, the NDAA gave us 25 accepted civil service hires which is essentially the ability to do an end run around a lot of the bureaucracy of the hiring process in order to bring people from the private sector in. And we're making full use of that.

I think that we need people with technology experience and expertise, but also people with commercial sensibility. Back to the point about private engagement, you need to go sit with companies and develop joint plans and not be viewed as the Fed. Right? You've got to b able to sit down and actually have that discussion and understand what works and what doesn't work in a commercial context. So that accepted hiring authority is a huge advantage in that regard.

On standards, I was with the Director of NIST last week. We increasingly need to make sure that we and NIST are shoulder to shoulder in the development and the promulgation of standards across all of these technology areas.

I would put this too in the category of American leadership matters. People around the world are looking for the US to do the spade work to develop the standards that have the philosophical grounding in the buzzwords of open, interoperable, reliable, secure, and frankly, it's across every technology area. so that is happening.

There are standard-setting bodies that are primarily populated by private sector representatives where we are planning to ramp up our engagement because a lot of the, not norms, but a lot of the technical standards are set in bodies where we haven't been as deeply engaged as we need to be. And there's a broader point that I would make briefly there. That is nature really does abhor a vacuum. When the United States leans out of

international organizations in frustration, our adversaries lean in and fill that void. Every single time.

So can I get frustrated at the UN? Absolutely. Can I smile and have sympathy for the view that you could cut the top half off the building and see no decline in efficacy? Yeah. But guess what? The minute we take a step back, others take advantage of our absence. So we need to be there and we need to be there every day. It gets back to that one yard and a cloud of dust. Ground game diplomacy over a 20 year period that resulted in the Framework for Responsible State Behavior in Cyberspace.

On offense. I would say there that maybe partly by virtue of having had some early background in the defense world, I have a good collaborative relationship with my defense counterparts and we get together on a regular basis to talk about things that are happening in the world and to make sure that broader foreign policy considerations are injected into all of the planning from the beginning rather than becoming a thought kind of right at the end.

Moderator: And with ten seconds to spare, Mr. Ambassador, thank you for a thoughtful and thought-provoking discussion. We learned a lot. Really appreciate you being here.

Ambassador Fick: Thanks for the invitation.

# # # #