Safety in Numbers: Improving Cyber Capacity Building

Featuring Amb. Nathaniel Fick, Annie Fixler, and RADM (Ret.) Mark Montgomery
Moderated by John Sakellariadis

MAY: Good morning and thank you all for coming out for today's event hosted by the Foundation for Defense of Democracies.

I'm Cliff May, FDD's founder and President. We're happy to welcome you both in person and those of you on the live stream for this very timely discussion on how the U.S. government can better organize to help partners improve their cyber resilience and why partner capacity building is so important for America's national security.

This conversation, coordinated with the release of an important new publication on the topic, has been organized by FDD's Center on Cyber and Technology Innovation, CCTI. Both CCTI's Senior Director Admiral Mark Montgomery and its Director Annie Fixler are here joining us on the panel today.

But our featured guest is U.S. Ambassador-At-Large for Cyberspace and Digital Policy Nathaniel C. Fick. Prior to joining the State Department, Ambassador Fick was a technology executive and entrepreneur, serving as CEO of the cybersecurity software company Endgame, as well as an operating partner at Bessemer Venture Partners.

From 2009 to 2012, he was CEO of the Center for New American Security, and before that, Ambassador Fick served as a Marine Corps infantry and reconnaissance officer, including combat tours in Afghanistan and Iraq. We thank him for his service and we're honored to have him here in this panel today.

Today's discussion will be moderated by Politico cybersecurity journalist John Sakellariadis – not so bad.

SAKELLARIADIS: Well done.

MAY: Alright – who covers election security, critical infrastructure protection, and digital surveillance. Before I hand the stage over to John, just a few words about FDD for those who may be new to us.

For more than 20 years, FDD has operated as an independent, non-partisan research institute exclusively focused on national security and foreign policy. As a matter of pride and principle, we do not accept foreign government funding. We never have and we never will. And for more on our work, please visit our website, FDD.org, and follow us on Twitter, or X, or whatever it is now @FDD.

And that's enough from me, John. Over to you. Thank you.

SAKELLARIADIS: Thanks, Cliff, and thanks to the Foundation for Defense of Democracies for giving me this opportunity to moderate today. The report that Mark and Annie put out has eight broad recommendations, and one of them, I suspect, is going to resonate very strongly with you, Ambassador Fick, and that's for Congress to appropriate more funds to support international cyber assistance initiatives from the U.S. government.

You have come out in support of something similar already. Can you talk to us about your vision for such a fund and why Congress should appropriate more precious taxpayer dollars for it?

FICK: Sure. Thanks, John. Cliff, thank you for the welcome. Good to look around and see so many old colleagues and friends in the room. And Mark and Annie, I commend you on the paper, which really is a terrific synopsis of –this important issue, and I don't say that only because it highlights –– the role – for CDP but I thank you for that.

In – in answering that question, John,–maybe I can take half a step back –and make five broad points about assistance in this area from my perspective. And –first of all, though, just to – frame it, I wouldn't make the argument–– that we are re-emerging – or we're re-entering an era of strategic competition. Maybe it was always there but it was below the water line. It's back above the water line now. And technology broadly is the primary arena of competition – primary arena of competition.

So first point, the National Cybersecurity Strategy calls out allies and partners as, quote, "America's foundational advantage in the cyber domain." This is as transnational an issue as any. There is very little that any one country or small group of countries or one company or set of companies can do on its own.

Secretary Blinken, when we had our chief submission back a few weeks ago, did make the point that strategic competition is endemic now to everything we do and that tech is this – is the – the primary field of that competition.

So second, the demand for capacity building – in this domain is enormous and it far outstrips our supply. Think about not only the Iranian attack in Albania or – the attack in Costa Rica. And very pleased to see Ambassador Crespo Sancho – sitting here – thank you.

Our ongoing enduring support in Ukraine and then a –whole host of other ––other things as well, –the demand far outstrips our supply.

Third point, it's easy to think about these as technology problems that therefore have technology solutions. I would make the argument that actually the solutions are generally people, process and technology in that order. That it's –not a simple matter of deploying tech, which is a good thing for us.

That leads to the fourth point, which is there's very little need actually to invent the wheel in this domain. There's a lot that the United States has done whether it's CISA's [Cybersecurity and Infrastructure Security Agency] industry and sector specific work that can be templated and exported or the ONCD's [Office of the National Cyber Director's] work on strategy and workforce development that can also be templated and exported, of course customized for unique circumstances, but let's not reinvent the wheel.

And then – really fifth, I mean and this gets – that's the framing and this gets to ––the fund, we need mechanisms and resources that are fit for purpose in this new world. And –frankly, it's not that new.

We're –behind where we ought to be in putting the structures in place. Very quickly after 9/11, we revamped what counterterrorism foreign assistance look like, and we made sure that the resources and the authorities that the mechanisms were aligned with the nation's need.

We are not currently aligned in that regard, and again, going back to those opening points, I – think we're in the midst of a phase shift here that's going to endure for quite a while.

So, what we need in –my view and our view is –the cross cutting ability to deliver assistance in not only cybersecurity narrowly, but also digital policy and the data rich emerging technologies like AI and quantum computing as they increasingly converge.

We need to be able to do it quickly. There's a speed problem right now. We can't have six, seven, eight, nine months from incident to first dollar on the ground, as we've seen recently in a couple of these high profile incidents.

We're not moving at the speed of the adversary. We're not moving at the speed of the tech.

And – then third, just to get – a little bit more granular on it,– we do have a challenge with current income thresholds, and this is a little bit different from the kind of – from more traditional capacity building, where maybe the greatest need is actually in lower income countries.

That's not the case here, where we can't afford to have just a – one somewhat hypothetical example, a soft underbelly, anywhere in the NATO alliance, because risk federates across relationships. So, even if it's a high income country, we need the ability to respond quickly.

So, we've been making that case successfully, internally at the [State] Department. We've been making it, I think successfully at the White House. We've been making it successfully on the Hill. I do want to thank Chairman Menendez and Ranking Member Risch in the Senate Foreign Relations Committee –for their bipartisan support for this, the Appropriations folks and also HFAC Chair McCaul and Ranking Member Meeks.

This is one of those kind of unfortunately relatively few areas– where we have a strong I think, bipartisan and bicameral consensus that this matters and we need to do something soon.

SAKELLARIADIS: Mark, Annie, for anybody who reads this report, one thing that becomes eminently clear very quickly is just how much activity there already is going on across the interagency from even IRS to DHS. Can you kind of grade for me the efforts that the U.S. government is undertaking today and how can they do better?

MONTGOMERY: So, first, I – I'll go with the how can they – how can they do better then get into the grades. I –think one of the keys here is that is this international cybersecurity strategy that Nate's team is – working on right now – was dictated by the Cyber Diplomacy Act, which was included in last year's State Reauthorization Act, which was included in the NDAA [National Defense Authorization Act], so you know, a lot of us had been recommending this.

And the idea is put State in charge, not of just State Department's international cyber capacity building efforts, but all federal agencies. And – what I mean by that is that doesn't mean they do the day to day operations of them, but they have an understanding. They can – you know, – they can assess, organize and then develop plans to prioritize and resource across these federal agencies.

And the reason they have to that is what you are alluding to, which is that we have – I think we have some duplicative programs and agencies. We definitely have gaps in what we want to see done, and we don't necessarily have the focus that Nate was getting at. And Ambassador Fick is exactly right, you know, U.S. security assistance needs to have purpose.

We push very hard that the purpose needs to be building the resilience of the – cyber resilience of the countries that we are operating with – first and foremost, that we're operating with militarily, so making sure that we have military mobility in those countries, but then secondly that it's the ones with which we have strong economic productivity ties so we continue to maintain our economic strength in – during a period of cyber pressure.

And –so, sometimes that poor countries, sometimes it's– medium economy or middle sized economies. Every once in a while it's a – it's a rich one, but our – security assistance should be applied across, particularly those first two groups, based on the priority of the organization.

So now, you come back to the grading – of the agencies. You know, I – think State Department had a very regionally focused program before we created CDP [Bureau of Cyberspace and Digital Policy], it was very much in there and I think it would then as State Department assistance does and regional programs go to the poorest countries first, regardless of where it is and regardless of their actual interconnectivity and need.

You know, but how much need you need for cyber resilience is sometimes defined by how strong the networks are in your country, not necessarily how rich or poor the country is.

And then, I do think that there are some duplication of programs, particularly across things like forensics, you know, where we have programs in – FBI and in DOD and in Secret Service. You know, we just need to make sure that we – that with a limit what which – which are in the – what are in the end limited resources we're applying them properly.

And then – and if I had a final thing is we don't get scalability, because we have so many agencies involved, not prioritized. State Department can give that scalability. They can say look, we – if you bring all of us – and I'm just making this number up, $1.5 billion for the security force assistance across all federal agencies, that has – when prioritized properly, has impact.

If it's broken up into – silos and not allowed to be led by State Department or organized by State Department, you have a problem.

And one last thought, State Department can organize this. They can propose it. They could – they can get it ready, but they're going to need – they cannot compel the interagency into compliance. And this is true in any area. And so – what that's going to require is the – White House, the National Cyber Director and the National Security Council and the Office of Management and Budget to be onboard with this plan.

So, that's asking a lot from this plan coming out in December – coming out I hope, in December, but you know, sometime in the next six or six months – that it can meet all those goals, but you know, that was our – key recommendation here. It was based on our assessment of the various agencies.

FIXLER: Yeah, I just wanted to take sort of a step back and think about like what – because we're talking about prioritizing and making cyber capacity efficient, so what – sort of what all falls into cyber – capacity building is the traditional stuff that you think about, which is sort of technical assistance, training, assistance and – and training as regards to developing strategies and legal regimes – a lot of those programs are out of State but also out of the Department of Justice or Homeland Security, even Department of Energy has technical training programs – so it's all of those pieces, – and we also mentioned – you mentioned the IRS, which – is sort of an interesting thing, that we're seeing initiatives out of IRS and Treasury and Secret Service that are about helping partners and allies learn how to sort of follow the money in cyberspace as another important piece of what capacity building is looking like sort of in today's world.

And all of these programs, while we talk about wanting to make them efficient and not duplicative and – closing gaps, – they are important because what we've learned in Ukraine is that cyber defense works, right? It is possible to

keep attackers out and to respond quickly to mitigate attacks, to recover quickly when that happens. And so we want – you know, we want our allies and partners to be strong in that way.

But some allies and partners are not as resilient as they need to be. And so sometimes, attackers get in and they succeed in really big ways. And so when that happens, we need the response – the sort of cyber assistance ability to move quickly that Ambassador Fick was talking about.

But what we do – and what we do right now is often deploy FBI as one of the sort of key components. So that's sort of a second leg of the cyber capacity buildings stool , it's how we deploy FBI and sometimes other agencies as well to help with that investigation into what happened.

And I think – I think it's worth noting, in those instances, the private sector, private cybersecurity and technology companies are often really key in that investigation and also particularly key in the mitigation and recovery from those incidents. And so that is sort of another piece of the cyber capacity building puzzle.

And then there's a third piece that I think is not something we traditionally think about as capacity building but has become an increasingly important part, and that is helping partners and allies deploy digital infrastructure that is built using trusted and secure infrastructure, right? Because it is a lot easier to be resilient against attacks when your infrastructure does not have backdoors that allows the Chinese Communist Party to roam freely in your networks, right? So that is a – piece of capacity building that we don't really think about as capacity building but is an important part of that.

And I think a lot of those efforts really began under the Trump administration and have continued in the Biden administration, and I think we used to think about this maybe four or five years ago as convincing partners and allies to choose national security over price.

And I think that's still sort of a piece of it but an increasing piece of it is the sort of – the way that capacity building and digital infrastructure – secure digital infrastructure – are interacting, right? There are partners and allies who are concerned about cyberattacks as a form of coercion if they choose a non-Chinese vendor.

So when we engage in traditional cyber capacity building to make those partners and allies more resilient, they are then able to make additional choices that make themselves more resilient. Again, so it is sort of a – virtuous cycle as to how – the way those two are particularly interconnected.

SAKELLARIADIS: I want to go back to the theme of prioritization. Ambassador Fick, you mentioned that the demand has vastly exceeded the supply for available funds. Hopefully that will change with the new NDAA and the support fund.

However, – I'm curious, is there kind of a recurrent delta you see in engagement with foreign partners and allies between what they want and what the U.S. believes those funds would be best used towards? That's kind of an in-country question.

And as a related follow-up, kind of zooming out, looking at the geopolitical map more broadly, how do you think about prioritizing what will still be a limited set of funds across the globe?

FICK: Yeah, – I'm happy to answer those. First, may I – follow up on a couple of points that Annie made that I think are really important and maybe not always getting – the attention they deserve?

The first is this point about the convergence between secure infrastructure and cybersecurity. There was – a method to the madness of putting these portfolios together inside CDP –– and also the emerging tech element, again, is these data-rich technologies continue – to infuse both cybersecurity and – ICT [information and communications technology].

So on the – infrastructure piece, it's wireless networks but also cable and fiber, data centers, satellites. It's – all of the elements of a nation's communications infrastructure, it's all of the – think about it as the architecture of the Internet, right, the – pipes that get the Internet into your phone or into your home. If we're not dealing with a trusted foundation and all you're doing is cybersecurity, then you're ensuring that you have perfect integrity of packets that are going back to Beijing, right? And so it is important to have all of our cybersecurity efforts sitting atop a foundation of trusted infrastructure. So – so I – I do, I think that's imperative.

And also, the inter-relationship of the two, again, as Annie made clear, that when company – when countries are making a choice about a – tender, a bid on ICT, it is not uncommon for them to be concerned about retribution – if they make the trusted choice, and therefore, the security hygiene has to be in place ideally first. So it's a very important point, the inter-relationship, and I think that's not always explicitly discussed.

Second, on public-private, look, – I was a CEO in this space for a long time, and public-private partnership was one of those phrases that made my eyes glaze over. Usually, it meant I give the government data, the government classifies it, and I don't get anything back, which didn't feel like much of a partnership. That has changed fundamentally since January, February of last year, I think catalyzed by the – imminent and then – and then actual invasion, further invasion of Ukraine.

So lots of concrete examples – migration of Ukrainian enterprise to the cloud, proliferation of resilient satellite communications, the feedback loop that you mentioned among the Ukrainian government, other governments, private companies with large technology stacks widely deployed in Ukraine in order to deploy patches quickly and blunt cyber attacks. It's not that the Russian attacks weren't happening, it's that generally they weren't successful. And – that's a model that we need to maintain – and replicate in other places.

So thank – thanks for indulging me on this.

On – your question – I think generally, there's always going to be a delta, right, between – the ask and the answer, the bid and the ask – or the – you know – and – so that's –fine. I think – one of the points that is worth stating on that though is there are a lot of non-monetary benefits that the U.S. brings to bear in the course of its capacity building efforts.

In addition to just assistance dollars, which might be the headline value of the package, we – can bring really significant, true capacity building, the actual kind of left seat, right seat humans doing things, you know – I'll give you a – couple concrete examples.

In Albania, working hand-in-hand with Igli Tafa, – the cyber coordinator appointed in Albania to lead their response efforts and improve the overall hygiene and capacity in their government, lots of us in the U.S. government have

wrapped our arms around Igli – and are – helping him build his kind of global network in this space, helping him prioritize, develop a strategy, make hard decisions. You know, again, you don't have to reinvent the wheel. There – there's a lot of – there's value in that kind of mentorship but it's not captured in the dollar figure.

The second example – we can help these governments navigate their own technology choices, vendor decisions, negotiating bids, because the U.S. government has scale, you know? It – might be a – first time interaction for these governments but it's an iterative game for us at global scale, and so we have negotiating leverage, frankly.

And so, you know, in a $25 million package, maybe we can bring $50 or $75 million of value to bear.

SAKELLARIADIS: Mark and Annie, I don't think this has come up yet but one of the more controversial recommendations in the report – or I suppose, I suspect it will be more controversial – is that the U.S. government should start training allies and partners on how to conduct offensive cyber operations.

Why is that not a bad idea?

MONTGOMERY: So first, I – want to – make it clear what we do is we introduce the idea of – offensive operations as part of the cyber capacity building effort, and I think we're very clear that there are a few places where we would green-light work and a few places where we wouldn't.

And so I think we break it up into – and look, a lot of – we have – there are a number of countries, there's six or seven, that – in the world that publicly declare they have offensive capabilities, a few more that we know have offensive capabilities, but it's still a small number.

But countries are getting to that point where they have a reasonable capacity to develop it, and – then when countries get thrust into a situation like Ukraine is right now, they are developing a very ad hoc version of one.

What we argue for is there's two elements here – and as a former Marine, Nate will know what I'm talking to – there's force generation and force employment. Force generation's where you actually sit down with somebody and help them develop, you know, the personnel, the equipment, the – tools, the infrastructure – to do that.

And – our recommendation right now is, first, out of pure necessity, which is we are not properly developing our own cyber force enough, right? We don't have the capacity to develop the cyber force – cyber operating force we need.

The last thing I would ask – the U.S. military to do is to go do this overseas, and – and we don't do that. If – we don't have enough of a capacity, we are selfish enough a country to not go do it – in a third party country.

So we're not arguing for force generation, although I – do recommend – I think we do recommend in the paper that – one service be set aside to start thinking – we recommend the Army cause they're in the best position right now – be set aside to start thinking about how you would do it, what you would go train and what it would cost resource-wise. That's a reasonable study ask of – the service.

Now, where I do think we need to get involved in offensive cyber capabilities is force employment. Force employment, as – opposed to force generation, which is building the forces, force employment's using the forces.

Like, for example, with us, it's Cyber Command and the cyber – and the National Mission Force. There, if countries are developing it or have it, I think – and they are our ally or partner – and we're in a conflict together, we have an incredibly selfish need to know exactly what they're up to and make sure that they're doing this in an appropriate way.

So in that cyber employment – cyber force employment, we should be working with them, and what that would really mean, I think, is ahead of time, left of bang, be working with these countries to work, you know, basically with intelligence, Judge Advocate General, or legal and operational specialists from our country or – allies and partners who – acknowledge they have offensive capabilities, working with this country to talk about things like unintended consequences, collateral damage, sovereignty, you know – kind of the rule of law used to these forces, accidentally stumbling into espionage, you know, – those kind of things, and even about how you do – how attribution is done and things like that.

And – we can do that ourselves, we could try to work with the Cooperative Cyber Defense Centre of Excellence, the NATO Center in Estonia, who does this on the defensive side already, but start to worry about that.

And I think it's – it would actually be an error to not be working on this force employment training with allies and partners who we think are – facing an adversary soon – so Latvia, Lithuania, you know, or – excuse me, Estonia, Taiwan, countries we think might develop an offensive capability. Neither one of them has declared that. Japan would be another one – again, hasn't declared it. But to say if you're going to do this, let's talk about force employment so that we can work together, so you don't accidentally escalate us into a situation we don't want to be in.

So that – that's a very – that's a nuanced answer. We do recommend offensive cyber capability building but really in the force employment area, not the force generation area.

SAKELLARIADIS: Annie?

FIXLER: Just to sort of foot stomp the reason why we think it's time to really start thinking in this way, to – both think about and start building a capability to do force employ – sorry – yeah, force employment capacity building and to start thinking about how we would do generation, is really, again, because of what we're seeing in Ukraine, right?

The Ukrainians wanted to use offensive cyber capabilities and didn't have them. And so they use – they've turned to sort of a cyber IT army. Allies and partners may do that. And so they are going to turn to vigilante groups or ad hoc sort of cyber operators, and that's dangerous because those people may or may not have the skills, they – may stumble into something that is quite escalatory, they might get in the way of other military operations.

And so if partners and allies are going to want to have the capabilities, they need to understand how they would employ that effectively. And so – that's why we need to – we, the U.S. government, needs to sort of start thinking in that direction so – we don't leave our partners and allies to sort of fend for themselves and stumble through it.

SAKELLARIADIS: Did you have something to add or...

FICK: : Sure. So...

SAKELLARIADIS: I – do have a question. Sorry, I wasn't sure if you looked at me...

(CROSSTALK)

FICK: ... I – I will – add something but the – caveat, of course, is that this generally falls under the heading of military assistance. It's outside the remit of the State Department.

That said, you know, as someone who's been in this industry for a long time, on – kind of, both sides of that fence, I would say that offensive cyber and defensive cyber are more akin to offense and defense in the World Cup than they are to offense and defense in the Super Bowl. There – it's – it is more fluid. It is – gradations. And there are many elements of a good offense that inform a good defense.

So they're – not quite as divorced as maybe rhetorically we sometimes want them to be. I get a lot of requests – we get a lot of requests for offensive capacity-building. My general response is "that is top of the pyramid," as you're thinking about, like, the hierarchy of needs. That is top of the pyramid stuff. Let's not have that conversation unless and until the foundations are solid.

And then – maybe, finally, I think it's – and Mark mentioned this. I think it's really imperative that any place that we entertain this conversation, we need to have confidence that our partner is a strong adherent to the framework for responsible state behavior in cyberspace, – that we are working only with allies and partners who – buy in and have demonstrated by – their behavior that they are aligned with the – these principles governing responsible state behavior below the threshold of the use of force.

SAKELLARIADIS: Related question, but in diplomatic circles, is there any normative pushback?

So I know this idea is speculative. Maybe something will happen in the future, but the U.S. has been public, at least in doctrine, about taking a more forward-leaning – some would call it aggressive, others not – approach in cyberspace. Have you encountered pushback on that idea in diplomatic circles, or do you think the conversation is, kind of, changing and people are accepting that cyberspace is – you know, things like deterrence don't exactly apply?

FICK: Yeah. Yeah. I mean, look, diplomatic circles aren't monolithic, of course.

SAKELLARIADIS: Sure.

FICK: As a general comment, I – would say that the – that offensive cyber capability over the last 15 years has gradually come out of the shadows, as it should. It's not witchcraft. It's not, you know, the thing of which we shall not speak. It is a tool of national power like every other tool of national power. It's not intrinsically different from, you know, 155-millimeter artillery rounds.

So – I am of the view that we should think about it and we should talk about it as a – normal tool of national power, governed by the same rules of the, you know, governing the use of force. And it should be normalized in that sense.

MONTGOMERY: Can I jump in, real quick?

So two thoughts. So, first, I think Paul Nakasone would have a lot of great legacies from his five years-plus leading U.S. Cyber Command. But one will definitely be his push on the Defend Forward and persistent engagement concepts. You know, I think it allowed us – I was working in the Senate at the time, and we passed some legislation that enabled, you know, military cyber operations as a – as reconnaissance, approved them for reconnaissance, and eventually led to

an NSPM [National Security Presidential Memoranda] under the Trump administration that's been broadly adopted by the Biden administration. I think good comment there.

And also, Senator King, Angus King, our CSC [Cyberspace Solarium Commission] commissioner, would always say – you know, he always wants to get deterrence. I would say there is some deterrence in cyberspace. I mean, there's a reason Russia hasn't used what we know they – we know they have malware in our systems in the United States. They're not enabling them. Part of it is a belief that we would do something back.

But that offensive capability does in fact – it has allowed deterrence above some threshold. We're trying to lower that threshold, but, you know – in other words, push down the level at which deterrence kicks in. And, obviously, it's too high right now. A lot of bad things happen that shouldn't and are done by countries who are our adversaries and believe they can get away with it because we won't respond.

But, you know, that offensive capability has an important role, and in fact, if anything, it needs to be further – on a U.S. side, it needs to be further developed, and then responsibly – I think Nate hit it just right – responsibly developed by our allies and partners so that we're working together.

If we want to escalate, we need to choose to escalate, not stumble into escalation. And – that – and cyber is one of those mission areas, as opposed to conventional weapons, where I think you can much more easily stumble into escalation.

SAKELLARIADIS: I'm going to throw the next question to the panel. I want to ask about the lessons learned in Ukraine but I'm a little boring – or sorry, I'm a little tired of all of the discussion around that for the last year and a half, so I'm going to push the panelists to give me one lesson learned that I haven't heard a lot at least, let's say. So hopefully something that you think has been under-covered in that whole discussion.

And then relatedly – it doesn't have to be the same panelist – is there any lesson learned that you think would be risky to apply to Taiwan, where a lot of U.S. policymakers and officials are now kind of turning their eyes?

MONTGOMERY: I'll go ahead and take the first one. Look – and maybe this has been said – but, you know, a ––– you know, a – you know, a small investment now can give you a big payoff later, and we learned that.

We – the – Ukrainians had a cyber attaché here, Georgii Dubynskyi, who was fantastic, in 2017 and '18. He's now, I think, the Deputy Minister in Ukraine on – Cyber. But he – you know, he came to the Hill, he came to State Department, he came to everyone and said "we need" – not because of NotPetya but because of the two years of attacks on their electrical power grid – "we need help defending against these Russian malicious cyber activity."

And he ended up getting about $48 million worth of U.S. assistance over three years, which, from what I can tell, we helped approve it – you know, authorize it and then appropriate it, then you can't really see what happens. But, you know, from contracts, it looks to me like most of it went to pay U.S. companies to work side-by-side with the Ukrainians in – improving their cyber hygiene but also mitigating actual problems on the – on the – on their systems, particularly in their electrical power grid.

This was matched by a specific DOE [Department of Energy] program that helped the Ukrainians and then by the European – you know, the Union or Commission, kicked another, I think, $30 million in. That kind of, like, under $100

million worth of investment over three or four years had a dramatic impact on their ability. The –Russians got in and the Russians did a lot of attacks. A lot were parried and then a lot – there was resilience and redundancy in systems to rapidly get them out.

So I know we talk a lot about the post – what happened after February 22nd but that four years of investment was a serious positive thing, and I think that's where State, CDP can really be key in organizing the less costly, more efficient, and also, in the end, sometimes deterrence, although not in this case, you know, building cyber resilience ahead – you know, what we'd say, left of bank.

FIXLER: I'll jump in and pull a – thread that Mark mentioned, just that our allies and partners, particularly European allies but not exclusively, also Australia and Japan, also have cyber capacity building programs, and their impact in Ukraine was also important.

And so we have a very sort of narrow view when we think only about what the U.S. government – is doing. And so we're broadening that when we talk about the private sector, but still, I think we have a very U.S.-centric perspective on what capacity building looks like.

But our other partners and allies also do capacity building. And so when we talk about and when we think about making sure that our – we're deploying resources efficiently and there aren't redundancies, understanding that those – that our partners and allies also bring capacity building programs to the table will help us make sure we're sort of deploying these limited resources most efficiently.

FICK: So I – mentioned three things that – probably fall into the boring and often –repeated category, the cloud migration and the – internal defenses and the – SATCOM [satellite communications].

Looking out a little further, something that's occupying my and our mental space – that may not be getting as much attention right now is, at the end of the conflict, Ukraine is going to have one of the best trained and most operationally capable cyber armies in the history of the world.

And as we've seen in the kinetic space, demobilizing a capability like that can present a lot of challenges and we should be thinking now, need to be thinking now about what happens to all of that capability and make sure that it is channeled in the right directions, not the wrong directions. And I think there's an immense private sector opportunity to do that.

It's interesting to me that, of the many cybersecurity companies in particular that are – assisting in Ukraine, several of them are actually building products in Ukraine. Not just selling products in Ukraine but building products in Ukraine.

So that fact, coupled with the Ukrainians' demonstrated excellence in their Diia, Digital Governance Application, which, if you're not familiar with it, I would encourage you to learn more – basically it's easier to get a driver's license in Kyiv today than it is in Washington, D.C. It's easier to pay your taxes, it's easier to start a business.

MONTGOMERY: These are very, very low bars...

(CROSSTALK)

(LAUGHTER)

FICK: ... pick a different American but it is – a tremendous platform to have developed in the midst of a conflict. And Estonia actually is customer number one. They've purchased the Diia app and are building their digital backbone on it.

So this is a totally imperfect analogy, but in the same way that, in the wake of the Russian, you know, attack 15 years ago, Estonia went, in a relatively quick period, thanks to good leadership and investment, basically went from being a net importer of cybersecurity to being a net exporter of cybersecurity. Can Ukraine – can digital governance be really a pillar of the post-conflict Ukrainian economy in a way that both absorbs a lot of this technical capability and channels it in productive directions and also, you know, generates revenue in Ukraine? That's something that – I don't think it's premature to – be really leaning into some of that right now.

MONTGOMERY: I'll give you one Taiwan thought. I worry – you know, one of the good – great examples of resiliency was the – after the loss of the – of the Viasat, the –rapid introduction of – of Starlink. Taiwan's going to be different, much like we argue at FDD, for pre-positioning a lot of munitions in Taiwan, cause there's not going to be any C-17 flights getting in once combat starts.

There is – you know, anything IT hardware-wise that you want to have redundancy and resiliency in Taiwan needs to be on Taiwan before C-Day, you know, before, you know, kinetic events happen. And that is not something people actually have a lot of redundancy and they don't maintain a lot of IT hardware just laying around inefficiently because of the –, you know, 18 month – you know, the – Moore's law being applied to that– equipment.

So the question is how much is Taiwan willing to invest in constantly having that redundancy and resiliency for their C4i and their cyber systems?

And then one other thing I'd say is many of the Starlink-like products have an amazing amount of Chinese-produced hardware and – software in those systems. And I'm not 100 percent sure how Starlink products or other type of products like that or the senior executives who run them are going to be excited about going head-to-head with the Chinese at – conflict time.

I mean, it's something that's hard to – judge and – we'll see, you know, how flexible and agile those companies are in coming to Taiwan's defense in the same way they did to Ukraine when the adversary was a Russia with whom they had very few dealings.

SAKELLARIADIS: Didn't want to convey the impression that the conflict in Ukraine is over or boring. I hope that didn't come across as insensitive. What does Ukraine – need now? What should U.S. policymakers be thinking about in Ukraine today when it comes to cyber and digital assistance?

MONTGOMERY: Well, ATACMS [Army Tactical Missile System].

(LAUGHTER)

OK, no, no, no – that was – our meeting the other day. The – you know, I – think – first of all, I – want to say that the continued organizational support of the U.S. government and working with our private sector and engaging – this – look, you know, kind of to take from, you know, a dated reference, you know, more cowbell, you know? We need to continue to do what we're doing in cyber.

Look, there's a whole different discussion on other weapons systems, but in this, I think the United States, with its private sector companies, has been doing a lot and –I think –and I think that there's – you know, there's a, you know, there's a good track – there's a good plan for success.

The one area I talk about when I mentioned that force employment – at some point, you know, we may want to start talking with the – as they begin they're organizing the IT Army under government leadership, you know, probably started to talk to them about force employment, about collateral damage and things like that – it – to the degree that that's a functional thing we can do. It's hard cause getting people in and out of the country – you know – we are already spending a lot of effort getting trainers – getting people out to come to training and things like that. So, you know, I'm certainly – can't be virtual but, I mean, that's one of these things we have to think about.

But – I think more of the same. This is one of those areas where I don't think there's any accusation that the United States isn't providing exactly what they need to be providing.

FIXLER: Yeah, I'll just sort of – harping on the cyber assistance fund, that kind of programs – and learning the lessons about how quickly we could deploy may not particularly – may or may not affect Ukraine itself, cause we're sort of – already got a steady state there, but we've learned some lessons with regards to State, also with regards to CISA about how we need to be able to move more quickly.

So again, I don't know that it's going to particularly affect Ukraine but I think taking those lessons will help us with other partners and allies as – as well. So hoping there's some more there.

SAKELLARIADIS: I'm running short on questions, so unless there's something that the panelists have a burning desire to share – Mark, you just...

MONTGOMERY: Yeah just one – other one. In our paper, just cause we didn't get to it, the Department of Defense – and they are of course always a six to 800 pound gorilla sitting in a room – but I think in this area, they've actually been very good in the interagency.

And it – you know, to the credit, I think a lot of it has to do with its – its kind of – you know, the cyber employment is one – one organization. You know, its Cyber Command makes it easier to organize with the rest of the government.

But our Department of Defense does – it's – like the federal agencies, in the sense that – its work is spread across so many different aspects. But one of the problems we have here is that they tend to eat on each other – so – or feed on each other, and what I mean by that is, like, we all love – we're almost breathless when we talk about a Hunt Forward Operation. Like, there was a Hunt Forward Operation in this country and everyone's excited.

The problem is that Hunt Forward Operation comes often from – different teams that belong to the geographic combatant commander who should otherwise be writing a – you know, be working on breaking into someone's rail infrastructure or airport infrastructure or something, you know? And those teams get pulled off to do this side-by-side training and work malware detection with a ally or partner.

And – the way I know that this is a tough resource is we only spend about $63 million a year on Hunt Forward Operations. That's actually a very small number in DOD world. I mean, in some – you know, in some federal agencies,

that's everything, but at DOD, that's pocket change. And the – that money isn't going up aggressively – you're – you know, next year because the truth is it's pulling very limited resources from other high priority DOD taskings.

So I – love Hunt Forward Operations. We – like – I don't know if Nate would say it here but I would – I wouldn't mind renaming them. You know, I think Hunt's a tough word sometimes. But we have to recognize there's a limited capacity that – and rely on the other programs that DOD runs that are kind of more run-of-the-mill training and exercising programs that service multiple countries at the same time, in preparation for an event, and again, making that investment pre- a crisis.

And then finally, the State Partnership Programs but get – continuing to develop them. Right now, only about 20 of our states have, you know, inherently, you know, strong – you know, cyber trainable – units that can go out and do cyber training, and – and those State Partnership Programs, allied with our allies and partners, could pick up some of this load in the –low level – in the introductory and cyber hygiene – training.

So we want to make sure that DOD's being smart about how they use this and recognize that we can't tap into their actual primary responsibility, which is to do the operational planning of the environment, i.e. the – the targeting, for a future conflict with a – major adversary.

So, you know, that's one of those things – Hunt Forward Operations, love them but recognize there is a limited capacity.

FICK: I would just emphasize that, that the global – demand and support for Hunt Forward is very, very high. I – happen to agree with the renaming piece. I – mentioned that to General Nakasone personally. Call them cyber success teams, whatever, but let's make it as easy as possible for our allies and partners to consume them.

And they've gone through a couple of conceptual shifts that I – think are worth mentioning very briefly. One, they no longer need to be deployed forward. They can – do a lot of the work remotely, which from a budgetary scale kind of leverage standpoint's great.

Also they've – there's been a – I think a conceptual evolution from proverbially fishing to teaching to fish, and so they really are a key capacity building tool now, and a – very, very positive one.

SAKELLARIADIS: I just want to sneak in one final question before we go to Q&A. The international cyber strategy, I know you still have a couple months before the deadline comes due, is there anything you can share about where you're heading with that work or maybe lessons learned just in kind of the early drafting process?

FICK: Yes, just – I mean, at very, very conceptually – and it is a little premature to get into any details, but we view it as nested really and derivative of the National Security Strategy, the National Cybersecurity Strategy, and the NCS was really designed – that fifth pillar of the international pillar, I had partners come to me and say "looks a little thin"; that was by design.

It is – it's designed as an API to plug in a more robust international strategy, so – it is derivative, I don't think you're going to see it take us in any radically different directions, it's going to flesh out and kind of emphasize and put in – put in place some of the more detailed mechanisms to act on things that have already been laid out in detail in the National Security Strategy and the National Cybersecurity Strategy.

SAKELLARIADIS: Just editorially, I'm incredibly impressed you're using tech metaphors now in your...

FICK: I – well I won't do it again, I'm sorry.

SAKELLARIADIS: That was fantastic. Think we've got some questions. And if you could please identify yourself before you ask a question.

FRIEDMAN: Hi, Sara Friedman, Inside Cybersecurity. In the implementation plan there is a section on counter crime and defeating ransomware that requires international engagement plan related to ransomware and cooperating in transnational cybercrime that was due this quarter. Has that been made public and if not can you tell anything – tell us anything about timing and what's in it?

FICK: Is that for me?

FRIEDMAN: Yes.

FICK: Yes, I – so the – I can't – there's not much I can share, very little I can share, the White House owns the initiative and – so I think – we're aware of the commitments in the timeline and have been involved in the dialog but it would – not be my place to answer.

FRIEDMAN: But you're the leading agency for that, aren't you?

FICK: In coordination, so.

VISNER: Hi, Sam Visner with the Space ISAC. I'm interested in what other countries are doing in terms of their own policy development. What lessons are we learning from our partners and allies? I was on the phone the other day with our friends in the UK, they've declared their space systems to be critical infrastructure as with the E.U.

Are we looking at other countries' policy initiatives as models that we might adopt here, essentially for our own capacity building? Thank you.

MONTGOMERY: So I'll start only because I was at an event yesterday on this. And so I mean these are two different things. This – Ambassador Fick's strategy is about our work with our countries, and part of this question is what are other countries doing?

I don't – there are other countries doing international capability but – capability building, first NATO holistically does it through the CCDCOE [Cooperative Cyber Defense Centre of Excellence], but in addition the Australians are out in the – Pacific Islands, Southeast Asia, the Japanese are starting to reach out, we're seeing real effort by them on strategic capability building, so we're seeing other countries out there, but these are – and these are good, I mean I think the last thing the United States would ever say is knock that off, right, because it's – it's take – it's allowing us to apply our resources elsewhere.

I do think the NATO efforts are reasonably well coordinated. There is this weird thing in NATO: When you're trying to join NATO, you're in what's called a member of action – a military action plan, a MAP; all the security – all the assistance you could possibly want flows into you from the treaty organization. The minute you join NATO, they snap the chalk line and you're done.

And – so Montenegro, North Macedonia, Albania, they joined the alliance, they're – once you join the alliance, the Russians don't send you a thank you note and say "game over, you win, they double down on their attacks on you."

And so at the exact moment that they're most under attack – so we'd need to work with NATO to try to figure out how we help those countries most under siege from Russian influence operations get at this issue. So I – that's where – I think that we could – the one place – ask I'd have with NATO is I understand you have this thing, but in the real world of they're under attack right now, it's not cruise missile attack, it's not fighter planes, it's cyber, continue to provide them that assistance for the first few years until someone – intelligence says they're on their feet.

And so that's the one area where I'd ask for more international assistance. Everything else is real value added.

SMALLEY: Hi, Suzanne Smalley from The Record. If this was answered in the beginning, forgive me, and don't repeat yourself, because I have an alternate question, but I'm wondering about the cyber resilience funds going to high income countries and how that is justified when they have their own money, and really given the drumbeat of cyber events should be spending their own money?

I'm also wondering if there are any countries you've identified at the top of the list to get the first available funds?

FICK: So I would draw a little bit of a distinction between capacity building and funding. There can be significant needs in high income countries, and it may not always be an issue of money, it's an issue of capacity and urgency, particularly in the context of other sort of geostrategic priorities, I – mean the example I mentioned is NATO. There's uneven capacity across the NATO alliance, they're all generally high income countries, or at least high-middle income countries, and in some cases there's compelling need because of the way the risk federates across the alliance.

So we need to be able to engage there and engage quickly there.

In terms of prioritization overall, I think that – it is not the case that there's a –one to 193 sort of prioritized list. I think it's a – it needs to be a little bit more dynamic and fluid than that, but we have a good sense and I don't think it would surprise you– based on other strategic priorities, kind of the nature of relationships, assets and strategic geography; sometimes it's the fact that a particular tender on ICT is near-term.

There are a lot of factors that go into it. So it's a constant prioritization and reprioritization effort based on many variables.

MONTGOMERY: I would be really surprised if an OECD [Organization for Economic Cooperation and Development] 30 country received – I think almost legally they won't receive Security Force assistance. What they will receive is if we're doing training on strategy or norms...

FICK: Right.

MONTGOMERY: ...of course we'll work on it together, and sometimes that looks like it's an assistance program when in fact it's a shared development...

FICK: Expertise.

MONTGOMERY: Yes, expertise. And so I think that's useful.

What I would say on prioritization, it's – it need – I would tie it back to what I said earlier on military mobilization and – it'd be like if Portugal and Estonia both need air defense assistance against Russia. I'm pretty sure we're going to work with NATO to get it to Estonia and not Portugal because one of them more realistically, you know, has that – thing , you know, coming at them, but that – again, I – would be very surprised if any DOD or federal agency money was going to a – security assistance program for a country in the top 30 OECD.

CRESPO: Hello. Catalina Crespo, the Embassy of Costa Rica.

The U.S. has been working successfully the last year and a little bit of – few months on cyber with Costa Rica. My question is how is the U.S. – or what are they doing on making this sustainable, not only for Costa Rica but how are you thinking of – of doing – expanding through regions? Regional training hubs? Training the trainers? How are you going to make this sustainable when there isn't a lot of money?

So it – I wanted to see if that's something – that's been thought about because – we're talking – I think somebody over there said we're talking about developed countries and what we're doing, but what happens with developing countries, which are the ones that have the – the lowest capacity building – and the money to fund all these?

FIXLER: I'll jump in on a different – sort of partially perhaps answer your question and then the Ambassador may have more details. But I think there are models of regional capacity building that are starting to develop that we can think about ways to replicate.

And I think particularly about the Abraham Accords and what we're seeing about the expansion of that into cyberspace and the way that those – countries are actually working together to develop platforms, to develop capabilities to help each other defend against attacks, so there may be ways to sort of think about not quite hub and spoke but regional collaboration groups, where we're seeing – where we have perhaps a – more capable partner collaborating with less capable partners, and where can we sort of emphasize –– and add to that regional capability?

So I think there's some models we can look at – to sort of start to build that out.

FICK: I think the – question's really fundamentally important. And as you know, I had the opportunity – to go to San Jose just a few weeks ago to have, in part, this discussion. And we need to think about these assistance packages not as the initial instantiation of something that's going to be indefinitely recurring but rather as a catalyst for – a security posture that's going to be more enduring and sustainable.

I think there's a – there's a regional leverage aspect of that. There's a real care in vendor selection, making sure that you're kind of steering the – package – to working with a vendor that is fit for purpose in a particular geography. There is some – there's – an incredibly capable pool of cybersecurity talent obviously in Costa Rica, which makes the problem significantly easier.

But – at a conceptual level, I think the question's absolutely the right one. It's something we have to ask and answer before the first dollar gets deployed because the nature of software, right, is that– the pace of degradation is very high.

And so, you know, you can – you can spend $25 million, not pay attention to – to Patch Tuesday, and pretty soon, your – your investment is – basically gone. So – it is baked into our thinking and the planning from day one.

LOOMIS: Hello, my name's Will Loomis with the Atlantic Council's Cyber Statecraft Initiative. I have a question for Ambassador Fick. In the implementation plan, one of the actions tasked for the State Department was to lead creating interagency teams for regional cyber collaboration and coordination over the course of the – next 16 months.

To the extent that you feel comfortable talking about this, can you walk through kind of how you are planning to approach that action and any potential roadblocks that you've identified or see in the future?

FICK: So no roadblocks actually. I think that, again, this is one of those areas where we have a – you know – a pretty – genuine spirit of collaboration across agencies, coupled with, again, bipartisan support.

So – it's really just a question of how to do it in a way that is most efficient, sustainable, scalable – and that's going to endure – and make sure that, you know, again, like in the – in the early days of crafting these new structures, let's – my bias, given my background, –– in a 16 month timeline to fully implement, is let's pilot, see what works, and then scale. Let's not come up with the ideal solution on paper, push it out across the entire world and across our whole government, and then realize we got something wrong.

And so I think – the art of this is going to be piloting, iterating quickly, learning, and then scaling. And I think we're – off to a pretty good start.

Our effort to put a trained cyber and digital officer in every embassy by the end of next year is a key piece of that, because again, also – building all of the interagency capability – and the vertical expertise in Washington is not nearly the whole problem. We need to – devolve the expertise – and the collaborative structures down and out and put them on the edge, which, you know, again, you know, for State, the superpower is the fact that we've got 200, you know, interagency organizations all around the world that are already set up to do this and we're going to use them.

SAKELLARIADIS: So – I think I'm – going to take the moderator's prerogative to close things up. And first, if we could all thank Ambassador Fick for showing up today?

(APPLAUSE)

FICK: ... I'm glad to be here.

SAKELLARIADIS: And not to be forgotten but the folks at FDD for putting on this event and Mark and Annie for a great report.