Strengthening America's Cyber Resiliency: A Conversation with the National Cyber Director, June 2, 2022

Featuring National Cyber Director Chris Inglis; RADM (Ret.) Mark Montgomery, CCTI senior director and former executive director of the Cyberspace Solarium Commission (CSC); and Dr. Samantha Ravich, CCTI chair and former CSC commissioner.

RAVICH: Hello. I am Samantha Ravich, Chair of the Center on Cyber and Technology Innovation here at the Foundation for Defense of Democracies. Thank you so much for joining us.

For more than a decade, report after report has documented the growing number of unfilled cyber positions, both in the U.S. government and nationwide, while offering strategies and recommendations to address this shortfall that often go ignored.

The Secretary of Defense has stated that the Pentagon is in desperate need, desperately short of people with cyber skills in all services and we have to address it. That was in 2010 and that was the Secretary of Defense Robert Gates, and that was one year after CYBERCOM was created, and that's when Amazon had a workforce totaling 34,000. Last year, Amazon had a workforce of 1.6 million people. So the need has gone up and the difficulties in attracting people and talent has gone up as well.

The congressionally mandated Cyberspace Solarium Commission, what we call CSC, published a white paper on the cyber workforce in September 2020 identifying systemic barriers that were stymying existing workforce development efforts.

These barriers include a lack of centralized leadership, insufficient coordination across the federal government, a non-existent federal strategy to guide priorities and resources, and ineffective organizational structures, which all combine to limit the potential of the very programs designed to strengthen and diversify the federal and national cyber workforce.

No clear focal point for interagency coordination existed at the time of the commission's report but the July 2021 confirmation of the first ever National Cyber Director, or NCD, has created a new opportunity to overcome these pervasive barriers.

Looking to continue and build upon the work of the Solarium Commission, the commissioners recently established CSC 2.0 housed here at FDD. Though -- through CSC 2.0, experts published a thorough report looking at how the National Cyber Director could lead the federal department and agencies in growing and strengthening the federal cyber workforce.

The report notes that in many cases, the NCD will need legislative support, so it also recommends actions that Congress can take to support federal efforts to grow the cyber workforce. These actions include extending the Federal Cybersecurity Workforce Data Collection Act, establishing a federal cyber workforce development institute, and authorizing a federal-excepted cyber service.

While these recommendations focus on the federal cyber workforce, the federal and national cyber workforces ultimately draw from the same community of professionals. So effective approaches must address both.

The report also outlines actions that private sector leaders can take to support national cyber workforce development more generally. We are fortunate today to have two very relevant leaders and experts on that exact issue.

First, I'm very pleased to introduce Chris Inglis, the inaugural National Cyber Director. Chris was confirmed less than a year ago. He came directly from teaching at the U.S. Naval Academy and serving as a fellow commissioner on the Cyberspace Solarium Commission. Prior to that, he was a career National Security Agency leader, rising to the Deputy Director of NSA. Chris also flew C-130s and retired as a Brigadier General in the U.S. Air Force Reserve.

We also have Mark Montgomery, one of the authors of the report I just mentioned on cyber workforce issues. He is a senior director of the Center on Cyber and Technology Innovation at FDD and served as Executive Director of CSC for the past three years. Prior to that, Mark worked for Senator John McCain on the Armed Services Committee and served in the Navy for 32 years, retiring as a Rear Admiral.

So a few quick words about FDD before we get started. FDD is a non-partisan research institute exclusively focused on national security and foreign policy. FDD houses three centers on American power that promote the use of all instruments of American power and produce actionable research and develop policy options to strengthen U.S. national security. FDD proudly accepts no funds from foreign governments or corporations.

For more information on our work, we encourage you to visit our website, fdd.org. You can also follow us on Twitter, @FDD. The CSC 2.0 project and the workforce paper is available at [cybersolarium.org].

And with that, I am pleased to get started. So Chris, it's great that you're here. I -- we've missed you, I've missed your strong voice in our meetings and since you left the team to serve as National Cyber Director. It's been about 11 months since you started. You're kind of running a start-up -- not just a start-up but a start-up in the White House. So maybe take a few minutes and tell us how that's going.

INGLIS: In a word, good. There's an old joke that goes with that -- I won't complete the joke -- but that being said, it has been about 11 months. First, let me just say how grateful I am for this venue and for Cyberspace -- or for the Cyberspace Solarium Commission 2.0. It might not surprise you, I'm a fan of 1.0. You might say that I'm a byproduct of 1.0. But that foundation has been extremely useful to us.

In terms of how's it going, I would say I'm a big fan of the preset that form should follow function. In this case, we kind of stuck the form kind of in place and tried to figure out what would that form do, what would the National Cyber Director do, and so we've been working very

hard for the last year to establish some of the principles that should underpin that and perhaps lead that.

First and foremost, I think that we -- and when I say that, I mean the federal government and a growing consortium of collaboration between the federal government, state, local and the private sector -- I think we can say that we agree that cyber is more than technology. I think the fact that we're having a discussion today about the people component reflects that cyber is far more than technology.

There's at least three dimensions to it. There's the technology, of course, that's the visible piece. There's doctrine, roles and responsibilities. Solarium addressed a lot of that, but we've been working through that over the last year within the federal government.

And then finally, there's the people piece. And often times if you're an adversary you think about those in the reverse order. I think that we have, in this first year of the creation of the National Cyber Director, focused on those latter two pieces, given the due to necessary to the technology piece, but focused on those latter two pieces.

Having said that, we then begin to put some life forces in play of, how do we actually get some better definition of roles and responsibilities? That's principally what I'm accountable for, is getting the roles and responsibilities right, not just across the federal government, but between it and the stakeholders and the larger cyber ecosystem, the private sector, state, local, academia.

And then finally, how do we get those doctrines, those roles and responsibilities properly supported by the people piece of that. That, I think is a work in progress. I'm delighted to have an opportunity to discuss that today. But, I would say that we've established a solid foundation of roles and responsibilities, we now need to make sure that we fill those roles and responsibilities with people that whose skills are up to the game, up to speed.

And in that regard, to just give you a preview of my own remarks on this, which is I think we should be concerned about the jobs that have cyber or I.T. in them that go unfilled. There's a lot of focus on that. It's only 550,000 at the moment within the United States of America, but we should be equally and perhaps more concerned with -- does everybody who plays a role in cyberspace, that's everybody -- does everybody have the skills that they need in order to take full advantage of cyberspace.

Because most of us -- the vast majority of us are not digital natives, we're app natives and therefore we need to make sure that we have the skills necessary to take full advantage of the positive aspects of cyberspace. That's an all problem. We need to make sure that everyone has the skills necessary while we focus on the other end of that spectrum on filling the jobs that have cyber I.T. in their job title.

How's it going? I think well, because those are understood to be really important problems that only we can share and we can solve as opposed to pointing to some poor soul in the corner and say that's your problem, you've got to solve that.

RAVICH: Just to follow-up, but for you yourself, the Office of the National Cyber Director, how are you doing on staffing?

INGLIS: We're good. So, when --

RAVICH: That will work.

INGLIS: -- I started I remember some reporter, a really good reporter, so I won't mention that person by name, but was kind of poking me pretty hard, saying, so how many people do you have? And what authorities do you have? And what have you done today? It was literally the first week that I was there.

Of course, when I showed up we were authorized, not appropriated, the money showed up in November. And I described it this way; I'd rather not talk about where we are, but rather where we're going. We're going to double the size of this organization, double it, double it again; we'll be eight at that time. And the person said, but how many is that now. I said, do the math. But we're now 40. All right, we're 40 people heading to --

RAVICH: Yes?

INGLIS: -- probably a high end of about 95 to 100. In a cyber kind of world, where you're doing operations, that's a small organization, but that's not our job. We're the quarterback, right, you know? I mean, we're the coach not the quarterback. We're not on the field essentially micromanaging cyber operations. We're making sure that the role assignments are right, that they complement one another. That all those parties have the authorities, the resources they need to do the proper job on that field.

So, within the White House, an organization of 90, 95 people is going to be huge. And we've begun the lines of effort that are necessary to actually get some reality to that. We've got a Workforce Education Initiative that comprises fully one-fifth of this organization.

We've got a focus on supply chain. We've got focus on open-source software. We've got a focus on all those things that you would are the kind of the foundational building blocks necessary to ensure that the roles and responsibilities are proper. That we've properly championed the pieces in that system and our principal modality is to work by, with and through. So, I think that we're in a really good place that way.

RAVICH: So, let's turn to the issue at hand, the Workforce report and the challenges that the federal workforce in cyber faces. Mark, you just wrote a terrific report with Laura Bate about the challenges of recruiting fine talent, of training, of developing, retaining. Kind of give us a sense of the challenges and the size of them.

MONTGOMERY: Well, thanks. And first, I do want to, again, acknowledge Laura Bate was the core writer of this and was a terrific part of the CSC 1.0 and 2.0 teams. And I'm glad that she's now moved onto the Department of Treasury, where she can help the government more directly.

So, I mean, this is a challenging problem. You mentioned, you know, three reports. I can go all the way back to 1999, when the -- when I worked for Dick Clarke and the National Security Council and we wrote a national infrastructure assurance plan and we laid out 10 big workforce tasks.

Seven of those are replicated in the recommendations that we have today, which means the government solidly achieved three out of 10 in 22 years and even at the most progressive schools a 30 is not a passing grade. So, the government has a lot of work to do.

You know, the big -- and there are people working hard. I do want to acknowledge, there's a group called NICE or the National Initiative for Cybersecurity Education at NIST, the National Institute for Standards and Technology at Commerce, which is commerce. You know, and they're doing great work to try and figure out, you know, code, jobs, explaining what skill sets go with what jobs and how many different types of cyber security jobs are out in the government. They've done a great job with that.

There's a great team at National Science Foundation, running the Scholarship for Service Program, which I'm sure we'll talk about during this. There's good people at CISA working in education and training areas. And good people at OPM, although they're drowning slightly. And there's a good people sprinkled throughout -- or sprinkled throughout the federal government. But the reality is, the overall progress, the -- that is not to overcome the barriers we're facing. The number one barrier that we identified is the lack of data.

Government cannot make good decisions without good data. We all understand that. Despite the fact that we actually have a legal -- you know, a statute saying collect the data. We do not have good data. And there's a lot of things that are responsible for that. The data -- the provisions not written perfectly, I get that. But, even as written, it's being ignored or carried out inconsistently among the 101 federal agencies. So, that lack of data is critical.

And I state that before the next thing, which normally any military person would say is your number one thing, which is a lack of strategic leadership. But, if you don't have data it doesn't really matter if you have leadership. But, once you have that data you need strategic leadership. Someone at the White House has to be the hand of God. And, you know, the person we're recommending is sitting to the right of me. Not as the hand of God, but as --

INGLIS: How far to the right of you?

MONTGOMERY: I think that makes me God, so I have to be very careful with this. But, the National Cyber Director, and I know we'll talk about that. But, the -- and he's the coach, to use his own analogy. He’s the coach. The next thing we're missing is we're missing a quarterback. We don't have coordination among the federal agencies and that coordination should be led by OPM.

Much like, I think Chris calls Jen Easterly in CISA his quarterback for public-private collaboration, his quarterback for federal cyber workforce is going to be at OPM. And that --

that's just not there. There's no one there standing, you know, there's more likely Heinicke there than Brady, you know, to use a Washington analogy.

And so, that's the next thing. And finally, there's these kind of statutory barriers which is, you know, the federal government can't get its head around. And sometimes a job is about certain certificates and experience and not about bachelors and master's degrees. So, understanding that sometimes the person you need may not have a bachelor's degree but they still need to be a GS12 or 13 as you hire them in.

Those kind of barriers really hit -- and a finally thing is it really -- it all leads into a diversity traffic jam. And what I mean by that is there is a significant diversity problem in our federal cyber workforce. The most egregious example is among women where there are only 21 to 24 percent or excuse me 24 to 28 percent of our federal cyber workforce and there are only about 11 to 15 percent of our federal cyber workforce leaders.

And those two numbers are both completely unacceptable for the way -- as we look forward. So I kind of think that's the big challenge that Chris or whoever's the hand to God is going to face in this.

RAVICH: Chris --

INGLIS: The right hand of God.

MONTGOMERY: Right hand of God.

RAVICH: So, Mark, put a lot on your plate. First of all do you see the challenges the way that Mark in the report with Laura laid out?

INGLIS: Yes, I broadly agree with Mark's framing of this. One I would start with, there are some really impressive pieces, component not least of which in the private sector. But let me just mention again what Mark cited in the federal government.

Right, you've got NICE the National Institute for Cyber Education. You've got the National Science Foundation CyberCorps for Service. You've got the Centers for Academic Excellence. You've got cyber talent management system over at CISA.

All of those are pretty interesting deep and sharp pieces that could make an even higher kind of leveraged difference if they were connected to some larger strategy. What's missing is not so much some of the piece parts. There's some more to be done there. What's missing is the strategy. that we would then use that strategy to figure out how do we connect those, give those the highest possible leverage, kind of amplify their efforts not within those stovepipes but broadly across the federal government and join arm in arm with the private sector.

Because the government can't solve its end of this problem, you can't filter one end of the pole. You've got to actually solve the national problem in this regard if not something even bigger than that.

And in that regard I would then say we have to do two things: We have to make sure we first have a strategy that defines what's missing. We then have to make use of all the parts that are already there and connect those to that strategy. And that strategy, to Mark's point, needs to be driven by data, it needs to be somebody who's accountable for using that data to define that strategy and then driving that execution across all those piece parts.

I think if we were to do that we could make rapid progress. We'd find ourselves reexamining everything. I don't think that we've appealed to a broad enough population, I don't think that we've got a diverse enough kind of talent pool that's thinking their way through "could I play a role in this." We've not actually balanced that aspiration to that destination by actually tracking people along that progress.

I think we've mis-specified the destination in many regards. Sometimes we require a bachelor's degree in computer science when what's really required is critical thinking skills. Not that they're divorced from one another. But let's think very creatively about what we really need. Let's think more broadly about where we can get that and let's manage that space in the middle with all of those excellent programs.

Strategy and data are I think going to be that interstitial thing that connects all those together.

RAVICH: So, Mark, I mean, you kind of cut right to the chase with the title of the report, right? The title of the report is "Workforce Development Agenda for the National Cyber Director." Because when we look back on the reports that have been written and the people – Karen Evans – who have been involved in this for decades, many of the pieces have been there for decades and people are very frustrated that the problem is just growing and staggering, and people want things done.

You cut right to the chase with your title, "Workforce Development Agenda for the National Cyber Director." What do you think that National Cyber Director specifically should be doing on this issue?

MONTGOMERY: Well thanks. First you're right and I want to acknowledge that Karen and the NAPA team did an excellent report on this as well and so I think we're -- there's a lot of violent agreement on what's wrong. I want to first agree with everything Chris said about how he sees his job. Data and strategy, if you just left it there that would be a success.

I'd probably add in budget oversight. Which is -- I'm hoping through the relationships that the National Cyber Director has built with the Office of Management Budget where Chris DeRusha is seconded as a Deputy National Cyber Director as well. That the NCD will have the opportunity to look at the individual agency's budgets in a lot of ways. But one of them would be, "Are you spending enough on your workforce?"

And I'll tell you no surprise is the answer is going be, "If you don't have cyber in your of your agency it's highly likely that the answer to are spending enough is 'no.'" And I'll exempt the Department of Defense from this because they have unlimited pockets.

But for the 101 federal civilian departments and agencies, the vast majority when it comes down to budget crunch time and it's "Does the Department of Agriculture buy a few more food inspectors or does it buy the I.T. administrators they need?" They're going to buy the food inspectors because that's in their job jar that their cabinet member sees.

So it takes OMB and by extension with OMB the National Cyber Director oversighting those budgets and getting it back. So I'd add that in.

And I agree completely on the strategy. I'm going to assume for a moment that the National Cyber Director writes the national cyber strategy. So we'll just assume that for a moment and then say there should be annexes to that. And I think one of them would be this workforce annex that go right in there and say -- and because, as you said Chris, there's three legs to this tripod -- to this success: technology, doctrine and policy, and personnel.

And so having an annex on personnel, having a National Cyber Strategy Workforce -- a federal cyber security workforce strategy would be really helpful, so I'm excited to see those.

INGLIS: Those are eminently sensible recommendations -- sitting here reminds me of why I missed working alongside of you so much, right.

So let me just give a larger context for the Office of the National Cyber Director. We put out a statement of intent in October and it was of course about more than the workforce, but the workforce is at the core of any viable strategy in cyber. And it laid out four broad responsibilities for the National Cyber Director. By mutual agreement of all the parties, right, who are involved in this.

First and foremost, to drive coherence both within the federal government but also between the federal government and the stakeholders in the larger cyber ecosystem. So things like private-public collaboration kind of are natural extensions of that.

Two, to focus on future resilience which is about inherent resilience in people, in doctrine, in technology and I think likely in that order has got to be our priority. We can bend technology to our purpose if we get those first two parts right. If you don't know what your roles and responsibilities are and people have no well-defined skills, then technology -- it's a fool's errand to try to get that alone right.

And that future resilience is not about what we do today, which is responding to two- and three-alarm fires, it's about actually getting to the left of these events. Again we can do that if we think our way through, "What should the properties of this system be?" Not least of which most importantly the people properties.

The third responsibility we have is performance assessment. How do we make sure that we understand that all of the application of that time and material -- roles and responsibilities are stuck in the middle of those two -- are in fact delivering results that we find acceptable or preferable.

And we'll take a fairly broad kind of brush to that and not simply consider the dollars but consider the assignment of roles and responsibilities and whether the skills that our people have are up to snuff. And then use that -- not simply to make reports for vicarious purposes -- but to then drive the implementation of our budgets and the implementation of our time and attention to get that closer to right.

Right, there's then a fourth piece which we're going be then accountable for, which is really down in the details of implementation to oversee that -- get the roles and responsibilities right. But when you add all those up and you consider that people, right, are at the core of two of the three dimensions of cyberspace, doctrine, and the literal people skills. I think that that gives a context within which we can define strategy whether it's called strategy or whether it's simply the implementation of broad strategic concepts.

And we can begin to make the progress necessary to have the data and to have the -- kind of the interstitial material necessary to make use of all those good parts.

RAVICH: There's another actor involved in making all of this work, that's Congress. Mark, you and Laura's report called out some specific legislative and appropriations potential recommendations for Congress. Maybe you could summarize some of those.

MONTGOMERY: Well, thanks, you know, one of the successes -- the Cyberspace Solarium Commission 1.0 I think was successful broadly, and one of the reasons was is that we wrote legislation early on.

You know, some of our Congressional leaders, Representatives Langevin and Gallagher, and Senator King, you know, told us, "Hey, look, we need -- we don't want recommendations, we want legislative provisions that are tied to recommendations." And I think that -- I think you two as commissioners would agree that that was really critical to our success.

And so, one of the things we try to do in this report is continue that tradition in CSC 2.0. We've done some water provisions recently, and in this one, we have some workforce provisions. So we do have some recommendations for Congress. We have three specific legislative provisions.

They're -- one's reasonably easy, two will be hard, and then we have some appropriations recommendations. But in the legislative provisions, the first one, the one that really has to be done is we have to extend and amend the Federal Cybersecurity Workforce Assessment Act.

That's the one that directs data collection. It will actually sunset soon, and then our poor data collection will dribble down to a zero data collection if we're not careful. At least, you know, legally dictated data collection.

And I think we can help the National Cyber Director in his role as a coach if we can amend -- if we can extend that, I think at least out to 2027, and probably have to extend it again after that. But also amend it because one of the things that's missing is any kind of forethought.

It doesn't say what are you going to need three to five years from now or two to three years from now in your federal cybersecurity workforce. And as we all know, things like the National Science Foundation Scholarship for Service aren't hiring this year's workers, they are hiring three years from now workers, right.

And most of our programs, and hiring programs take two, three, four years so we really need to understand that. So the first thing is amend and extend that provision. The second is one where we have to figure out how to -- I used to say how you go from apprentice to journeymen but now I think the right terminology in the government is how do you go from entry-level to mid-career?

And it can't be that we're poaching people, you know, from other agencies or from the private sector. That doesn't work for us. We need to grow our people, and to grow our people we need to have a training environment to do that in.

And so, we recommend a Federal Cyber Development Institute, it's not brick and mortar, it's where you go while you're working for the government to get job skillsets and to get certifications to move on. And I think that -- that's probably harder than the extend and amend of the previous act but it's probably doable.

The third one is the Rosetta Stone, if we can crack this we're really going to understand the -- the system. And that's -- that we -- we really do have to come up with a new hiring mechanism. We're recommending a Cyber Excepted Service, we give three different options to the National Cyber Director to work on, obviously, he can go off of that sheet and come up with a fourth or fifth.

But the one that'll really make the most difference, the one that's really helped DOD is having a Cyber Excepted Service. This'll be tough, there will be people who fight this both in Congress and in, you know, federal government organizations. And it's going to cost money, but I think no one ever thought fixing federal cybersecurity workforce was going to be a cheap endeavor.

And I think having a federal Cyber Excepted Service is probably the key. I do want to mention a couple of appropriations, we do need to bump up the National Science Foundation's Scholarship For Service program. Right now it's cruising in around 55 to 65 million every year over the last two to three years.

That's producing about 400 workers a year. And they're popular, I know they're popular because at the fair -- at the matching fairs that they do in the spring NSA and CIA are -- are the two organizations taking the most people. And they can hire anybody and they come and hire these kids, so I know they're the right ones.

But we got to get that Scholarship For Service up to about 1,000 graduates a year, it's currently at 82 colleges, universities, and community colleges. It needs to be spread to a few more. NSA's identified I think 370 schools through the CAE program. So we know there's schools to go to.

And I really strongly push this ROTC-like program over other initiatives. There's one in Congress now on a cyber defense -- Digital Cyber Academy or Digital Service Academy. I think

this is a real mistake. First of all, a brick-and-mortar institute is going to take us years to build and suck money off of all the other programs.

But second, it's not going to contribute to the private sector, right. When we run these scholarship for service programs, ROTC-like ones at 80 to 100 to 120 private universities, many more than our graduates -- than the people we take into the federal service are benefiting from the professors we fund at those schools.

You know, we're producing two- or three-fold numbers of workers going directly into the private workforce. So we really have to kill this idea of a Digital Service Academy and move forward with full funding for the Scholarship For Service program. And there's a few other appropriations I'd do and they're in the report, but I think those are the big ones.

RAVICH: Yeah, that's fantastic. And the level of specificity that Mark and Laura put into the report, can really show you why Cyberspace Solarium, CSC 1.0 was as successful as it was. Because it's based on the specificity of making real the recommendation.

So Chris, let me get you to comment at least on a couple of some of the recommendations that Mark just spoke about. Specifically, the Cyber Workforce Development Institute, and the government-wide excepted cyber service, and any of the other ones that you'd like to comment on.

INGLIS: I'll talk about those things specifically, let me just talk more generally though about what I think are three broad aspects that underpin Mark's remarks, all of which I think have some sensible and actionable recommendations inside of those. There are three kind of stretches where initiatives go to die.

First is this kind of stretch that I call “aspiration to destination.” We all know how many jobs we'd like to fill but there aren't any vehicles or many vehicles that essentially would take that aspiration in essentially meaningful -- meaningfully assist folks to get from that “hey, I'd sure like to vie for one of those jobs,” to get them into one of those jobs.

People who show up today at the front door of a government organization with a Bachelor of Science in computer science but no experience in hand typically are turned away. Because we say, “You've got to have the experience.” We need to figure out how do we actually do the internships, the co-ops, right, the cyber clinics to get them that experience, to get them from aspiration to destination.

So more flexibility, and more investment in that actual stretch along that first kind of part of the highway. Second, once they get in the game’s not over, right? We have all this poaching going on, so we don't have career tracking where we continue to make the investments in those people.

And continue to make them feel like they're part of a larger community of interest. And so, we need to bring those barriers down between the various kind of entities that would hire these people. And we need to also kind of make sure we're investing in them not just to get them to that initial job but throughout their careers.

I worked at NSA for 28 years, I had what looked from the outside world to be nine very different jobs, but I was always an NSA employee. I always felt like I was along a single career track.

So how do we take computer kind of personnel, IT personnel, cyber personnel and give them that sense that they have a very rich career field in front of them and they're not being poached from job to job but rather they're being progressed from job to job and getting all the stronger as they make their way from one responsibility to the next? And so in that regard, something that actually cuts horizontally across the federal government, I think will be extremely valuable.

Finally, to Mark's point about, you know, these institutions that might then assist in that regard, we have to make sure that those institutions, whether it's a service academy that I was a benefit from, need to have a parent -- they need to have a parent service that says, "I'm the person or the party that will kind of ensure that I have a sense as to what the standards and the requirements are for whatever this service is set up to do and I will then employ, right, what then becomes of that."

If you lack either of those two dimensions, it's probably a good idea in the corner, that lacking the parent that would actually define the requirements or then accept and employ, right, the beneficiaries who kind of derive kind of the education for that institution, they'll fail.

ROTC programs essentially do something that's magic in the middle, which is they actually kind of take the resources from a parent that says "Hey, if you make these investments, I will hire the result. I'll just be that instrument in the middle," but they've solved the problem by actually marrying that aspiration to destination. We need to make sure that we do that.

RAVICH: Mark, if I'm not mistaken, the deficit shortfall in the federal cyber workforce kind of tracks with what we're seeing, you know, in the private sector cyber workforce. I'm wondering if you learned anything during the research for the writing of this report on the federal stuff that is actually -- can illuminate, you know, a way forward on the private sector side?

MONTGOMERY: You know, you're exactly right. I mean, it's this -- it's the -- it's mathematically very similar program -- problem -- about 70 percent of the jobs are filled, 30 to 35 percent of jobs are empty by the CyberSeek, which -- while the numbers may not be exactly right, I think the general trends are correct in that data.

And they're struggling too. There's a lot of poaching going on in the private sector. This failure to develop from entry level to mid-career really exists just as heavily there. And so we've got to figure out how to incentivize the movement, you know, of people from entry-level to mid-career.

Chris talked about incentivizing, getting them right. In the entry level, I think that's true too with the apprenticeships. I want to give a shout out -- Microsoft's got a good program they're working with community colleges. They advertise a pretty big number, like maybe $20 billion with it, I suspect that that's a lot of intellectual property being counted a few times. But they're certainly sharing a ton of curriculum and data with a 1,000 community colleges. I cannot tell you how important this is.

And there are other programs doing this. You know, there's other opportunities out there for certification and job training programs that specifically target entry-level cyber skills and the movement from entry-level to mid-career, when you've gotten the experience, and -- and we need to acknowledge those, support them, and ensure that they're -- the -- you know, that they're -- they're being replicated throughout the country.

One other one -- I'd say IBM's got a program they're working with Historically Black Colleges and Universities -- I think it's successful as well. But we've got to get it so that at -- particularly at the community college level, kids are leaving -- graduates are leaving with the certificates they need and experience from an internship, which is -- or a work study program that would be -- you know, that would be highly useful in transitioning into a full time job.

So I think they're the same problems, I think they probably have a little more flexibility around pay and hiring than the federal government does. I mean, who doesn't have more flexibility in hiring than the federal government? But the -- I think they still face the same challenges.

RAVICH: Yeah, they may also have a little bit more flexibility in terms of where they get their workforce from -- all due respect to -- to Mr. Musk, I think people aren't going back to the office as much in the -- you know, in the private sector, in this space. They can get now people from around the world to fill their employee roles. So maybe maybe it'll open up more ability for the federal government to recruit since the private sector can recruit from a larger pool, but we shall see.

Look, before we turn it over to the audience to ask their questions, I wanted to ask Chris about an issue that is near and dear to my heart. On the Cyberspace Solarium Commission, we recommended and it was approved in the National Defense -- 2021 National Defense Authorization Act -- which is Continuity of the Economy planning, or COTE -- Continuity of the Economy planning -- which looks at how do we prepare for and recover from a major cyber attack that rolls across our economy, not just targeting one organization, one sector, but multiple at the same time.

So how is it going? The act -- you know, legislated, as you know, that the administration was providing a plan by the end of 2022, which is rapidly approaching.

INGLIS: Yeah, so I must admit that my horizons have been expanded a bit since I was on the Solarium Commission. Now, when I first thought about that Continuity of the Economy assignment, I thought about it almost entirely through the cyber lens. Of course, there are many hazards that kind of hold an economy at risk -- or many resources, both materiel and often digital infrastructure and virtual that are required to actually make a kind of an economy run smoothly.

And so you have to actually have a broader kind of lens to look at that through than cyber or -- cyber alone. So it's not something that has fallen naturally to the Office of the National Cyber Director. It falls more naturally to the Cybersecurity and Infrastructure Security Agency, working hand in glove with what's called pound resilience, but the National Security Council component that worries broadly about societal functions.

And so they've now got that and are working their way through that to try to determine how do you actually cut across all of those critical activities that constitute a viable, running economy? I think when we're all done, you'll look at that and say, "That was about far more than cyber, about what it takes to get that done, and it's frankly more about the horizontal than it is about any particular vertical."

RAVICH: Well, we will stand by to see what is rolled out.

So I think we're going to take some questions from -- from the audience. Yes?

STAFF: That's correct. We will have a question-and-answer period right now. If you will raise your hand, we'll identify you and then ask you to stand up, introduce yourself, and then ask the question.

(CROSSTALK)

QUESTION: Thanks. Sam Visner with MITRE and the Space ISAC. Always good to see you, Chris, Mark, Samantha. An observation not so much as a question, but whatever can be done to bring good, young people into government and give them something meaningful to do.

As you know, I am an adjunct at Georgetown. I've sent my students to the Executive Branch, to the military, to the IC and to the Hill. And it's pretty much a dog's breakfast. Occasionally, they will come back and say, "You know, I've had something interesting to do." Some have come back and said, "It's a toxic work environment, I don't want to stay there a moment longer." One left the federal government to take a job for $60K more in the private sector but would have stayed in the government for the mission if the work environment had been suitable.

What can we do to provide an environment in which these people are not locked into "well, it's -- you're a GS-7, GS-8 for the next few years, you have to do something meaningful before we decide -- meaningless before you can something worth your time?"

These are people who are highly motivated, they want the mission, they want to contribute to the mission, they want to be part of something larger than themselves, and they don't essentially want to be locked in the basement eating gray meatloaf as a GS-8 for the first four years of their careers.

So hopefully we can find a way not only to develop the workforce by getting these people on board, but to develop the workforce by giving them something meaningful to do so that they stay on board and continue to contribute. Thank you.

MONTGOMERY: I'll take the first point, OK, just -- only because, Sam, you had...

INGLIS: A lot to say about it because I don't like gray meatloaf any more than Mark does, all right?

MONTGOMERY: Yes. The -- first, you did have a student come work for us here at FDD, hopefully they came back with positive thoughts.

QUESTION: They did.

MONTGOMERY: OK, good. The -- so look, agreed that it's tough -- it's -- you see this in the military, you've entered -- you don't enter as a lieutenant colonel, you enter as an ensign or Second Lieutenant. And you have the...

INGLIS: A few ensigns become lieutenant colonels.

MONTGOMERY: Yes, there you go, that's true, fair enough, yes. And then maybe the Space Force someday. The -- so -- but I would say that the key to this is having what Chris described as nine jobs within NSA that felt different; I felt the same way in the Navy -- I was a Navy officer, had about 14 assignments, only one or two were the same. They were vastly different every time.

I -- we're starting to see that. There is a cyber workforce, there's an act has just passed that's going to allow some movement between agencies. I think that's the beginning of it.

There are different ways in the federal government to get job satisfaction and to get that psychic pay that covers down for the slight loss in physical pay that you might experience as a federal government employee, but I think having some movement between jobs will be good for the government employee, but also be good for the agencies as you get cross-pollination of ideas between different agencies.

So I'm hoping we're going to tackle that. It's certainly a concern, and whether there's a toxic work environment is probably point by point and that should be solved at the place it's at. But the idea of having some flexibility in your job movement is a good one and one that Congress has started, and we're going to have to see how this pilot program goes and see if we could push it fully into the federal workforce.

INGLIS: I subscribe to your general thesis, which is that culture should be our principal focus as opposed to being beholden to the administrative aspects of it. We're always going to follow the law, we're always going to follow administrative procedures within the extent of the law. But I have never been in an organization where I was compelled to essentially bend, right, to the strictures of a particular kind of role assignment or the strictures of some gradations. I've always been in an organization which had the authority to install culture and to hire not employees but owners, to give them a full piece of that responsibility on day one, to let them make a difference on day one.

And frankly at NSA, which -- that's the majority of my work life experience -- we never had a problem with retention of the kind that is broadly described across cyber circles now. Our retention was on average about 3 1/2 to 5 percent attrition, meaning everybody else stayed, which was unnaturally low for an organization that has to turn over every 20 to 25 years.

And why was that? It wasn't because we had swell parking; we did not. It wasn't because we had the best color in the world, we had lurid green inside of our hallways. It wasn't because we had this wonderful pay system, we were GS kind of pay. It was because we gave people feedback and said you can make a difference on your first day. Here's the feedback associated with that, and when we did that, those people would come and stay and stay and stay. So I take the point that it's about the culture that should not be beholden or subordinate to the administrative system. Ultimately that form should follow the function, but we need to drive the function first.

QUESTION: Hi there. Sean Lyngaas with CNN. Thanks for doing this. Chris, I wanted to get your response, as you know, General Nakasone, this week, confirmed that Cyber Command has taken the full spectrum operations in support of Ukraine. I'm wondering a couple things.

First of all, have you all seen any response from Russia in cyberspace to that activity? And more broadly, are you concerned at all that the Russians might see rightly or wrongly those activities as escalatory, given we've seen everyone and their mother participate in cyber operations in Ukraine. There's been hactivists, there's been people using U.S. infrastructure that might be -- opens up the door to misattribution. What can -- what's being done to make sure that isn't misinterpreted? Thanks.

INGLIS: Yeah, I can't speak to any Russian reaction associated with those remarks. Or for that matter, any operations that may or may not be taking place in cyberspace. But let me address what Paul Nakasone -- what General Nakasone said. The White House affirmed those remarks I think as recently as yesterday, in saying he's correct in what he said, which was not in any way, shape or form breathless. It was just a statement of fact.

The statement of fact was that cyber is an instrument of power. And to the degree that we're applying many instruments of power to assist in the defense of Ukraine, cyber is one of those instruments of power used in our -- from our perspective in a defensive kind of modality. Meaning that while they might impose affects or have kind of -- might make a difference to the receiving end of that, whether it's financial sanctions, whether it's lethal materiel applied kind of in military ways across the Ukraine, what we're trying to do is to assist the defense of the Ukrainian people, right.

And I think that cyber then, as an instrument of power, can and should play a role in that. That's what I heard Paul Nakasone say. And I haven't heard anything that -- from that day forward. A couple days ago I would say it's been provocative. Most people that I think understand the nature of this domain have said that makes sense and anything less that that wouldn't.

MONTGOMERY: If I could pick up on that? It reminds us that this cyber capacity building, which we're effectively now doing -- apparently doing after the war starts, it's also something that we should focus on left of boom, you know, before the crisis and, you know, in Ukraine specifically like we had USAID run a program for four years doing cyber capacity building, about $39 million.

There's a foot -- fingerprints of CYBERCOM doing, maybe not defend forward operations, but support to the Ukrainians and the time leading up to the conflict, which now has been acknowledge by General Nakasone.

So, it's those efforts -- that cyber capacity building for our key allies and partners who can't afford it themselves. So, probably not for the U.K., but for countries like Ukraine, Georgia, Taiwan, you know, that we should be thinking about these things left of boom and making those deterrent investments at the same time we that we make the ones right of boom.

STAFF: Next question.

QUESTION: Yes, hi. I'm Derek Johnson with SC Media. Mark, you mentioned a law that we're going to need to extend and reform, I didn't catch it, in order to kind of address this problem.

MONTGOMERY: Yes.

QUESTION: And that you said that you expect pushback in Congress and from some of the bureaucracy about that. Can you talk about that a little bit more in terms of what kind of pushback you're expecting? And then, if you or Chris, can just talk about how you kind of navigate this issue, where you're trying to stump for elevating the importance of cyber hiring while kind of dealing with all these agencies who -- you know, without diminishing the roles or jobs that kind of others do we think are also important -- how are you all sort of navigating that issue?

MONTGOMERY: Sure. So, I'd probably mush together a couple of laws there, I mean, because I don't think the extend and amend of the Federal Cybersecurity Workforce Assessment Act will get too much pushback. It's just getting it and finding the right vehicle to get it done. Sometimes the problem isn't anyone opposes it, it's that the process is cumbersome to do something like that. So, we have to find the right vehicle, you know, whether it's the NDAA, National Defense Authorization Act or another one. So, I'm hoping that will get done.

Some of the other ones, the digital, having a digital workforce institute or cyber workforce developmental institute or having a Cyber Excepted Service, those will get pushback. The way we'll work -- that this should be worked -- is through the appropriate congressional committees.

And I'd say, this one of these interesting things. Jim Langevin used to always tell the three of us, like, "We need -- my big issues is we need one cyber committee in the House and the Senate." And everybody kind of roll their heads. But, after a while he got Senator King on board, but all the rest of would roll our heads back, like you're never going to get this off.

I said, I will say, we put an amendment in, a floor amendment in and it was killed in 30 minutes, which was a record -- speed record for killing a floor amendment. You know the -- but the idea of one cyber committee would make this easy. We don't have one cyber committee.

But, I would start in House Oversight and in Senate Homeland Security and Government Affairs, HSGAC. In the House Oversight, Congress Maloney, who was critical to getting the National Cyber Director done with the support of Jim Langevin and I think also Gerry Connolly has done a great job working on OPM and federal workforce issues in general. And John Katko from the Republican side, on the Committee of Homeland Security, you get those kind of voices talking about this -- we might be able to get those second two pieces of legislation done.

In the Senate, Senators Peters and Portman have been very bipartisan on how they tackle things. So, if this can get on their agenda, I think they'll deal with it. The problem is, they have a long agenda of things to get done in cyber this summer and fall. And you can imagine, there are not too many legislative vehicles moving through town.

And so, if we can't get it prioritized and into the National Defense Authorization Act, it will kick a year. That extension cannot kick a year. We need to extend and amend that act this year. And so, that's the one you'll probably see the biggest push on from those kind of leaders. And it's really bipartisan, bicameral, that this is not an issue that should be subjected to any kind of partisanship.

INGLIS: I would just add to that, you've asked how do you get that on the kind of the agenda, the radar screens of the decision makers. I think you have to establish, you know, broadly two things. First and foremost, that cyber is neither delegable nor discretionary, right.

It's not something you can kind of hand off to the technologist, or the folks who have I.T. and cyber in their name and say, "This is your problem, this is your job. It's like the motor pool, just make the darn thing work." It is therefore not delegable, it's not discretionary. And why do we say not discretionary?

If Jeff Moss were, he's the guy that kind of heads up Defcon and Black Hat fame, he would ask this question up front of the cyber talk: "Why do race cars have bigger brakes? So they can go faster." Why do we have cyber? Not for its own sake, but so that we can do those things that individuals, organizations, societies chose to do with digital infrastructure. So, it's not discretionary.

If you establish that, then you get to the second question of, "What is it? How do I actually have cyber resilience?" I think broadly you need to make sure that you have inherent resilience in your doctrine roles and responsibilities. Do we know who's accountable for what? Your people skills. We've had a long discussion about that today, appropriately. And, of course, technology it needs be inherently resilient and robust.

To Mark's point, we need to get left of the event. This needs to be a capital expenditure, not an operational expenditure. So, we need to make those investments in the formative phase, right, of these kind of systems that we build and deploy for the purposes that we use them for.

And finally, what will result in that, I mean, this is not going to be an inherently secure, perfectly secure system. That would be lovely. But, none of these systems are. They always have some frailties, some kind of fraught nature attended to that. Not least of which is because

people are inside of them making choices all day. So, what results is going to encounter the occasional problem. And our response to that can't be a division of effort where you defend your side of this, I'll defend my side of that, as if we're in this sailboat and if the hole's in your side of the boat, good luck to you. It needs to be that we have a collaborative, collective defense.

Those two things -- resilience by design across technology, people and systems, kind of the doctrine, and the kind of collective, collaborative defense -- can make a dramatic change, right, in our fortunes in cyberspace, but only if leaders foremost -- first and foremost say that it's their responsibility to deliver that and no longer assume that this is delegable or discretionary to some population in the corner that happens to have IT or cyber in their job titles.

STAFF: Over to Sara.

QUESTION: Sara Friedman, Inside Cybersecurity. We're coming up over a year since the cyber executive order was put out and now we're coming into the implementation phase. I wanted to find out how -- Chris Inglis, how you're involved in that and how you see that moving forward and to helping the government become more secure?

INGLIS: Yeah, so first, I think you're talking about Executive Order 14028, which I think was issued on or about the 11th of May, 2021, so it's been just over a year now. And I think that that has been, in a word, boldly successful.

Why? Because it actually declared that the federal government was going to make a -- kind of a fairly significant commitment to the foundational attributes that any digital infrastructure should have to achieve some degree of inherent resilience and robustness.

Now, the execution of that, in terms of the percentages of systems that have met the specified kind of requirements of everyone has to have multi-factor authentication, every system has to attend to encryption for data at rest or in transit, and so on and so forth -- there's a whole bunch of other technical mechanisms in there, right -- we've made significant progress in that regard. We're not at 100 percent.

Why? Because 100 percent might not be the right goal, it might be that some of these systems actually don't warrant that, they don't have a public facing attack surface, or it might be that some of those systems have compensating controls, right, that are a proper substitute for that, that we don't use those in ways that are security relevant.

But that being said, the first and foremost goal was to say, "We fundamentally commit to doing these things so that we have an inherently resilient and robust architecture," and it's the department heads and the deputy department agency heads that are accountable for that.

My role in that is to oversee the further execution of it, right, to ensure that we're tracking those statistics and that we drive those to a proper conclusion, which in some cases the knee of the curve might be less than 100 percent but entirely appropriate, given the needs of the system and the -- kind of the threat that we're up against.

Kind of a preview is that we won't be tracking Executive Order 14028 forever because we've actually got something already on the street that will supersede that. It's called the zero trust architecture. We've asked all the agencies and departments to say "using Executive Order 14028 as the foundation, that first cut of what right looks like, now let's go further and let's have a zero trust architecture which has some very specifically assigned attributes associated with it and plan across the fiscal cycle, which goes two, three years richly into the future, in terms of some detail, tell us how you're planning associated with that, tell us how you're budgeting associated with that, and we will then begin to track that, which is a super kind of set of the things that show up in the executive order."

RAVICH: I think we have time for one more quick question before we -- some wrap up comments perhaps?

QUESTION: Hey. Adam Janofsky from The Record by Recorded Future. Thank you both for your time today. I wanted to ask about -- a lot of attention has been given to Russia and cybercrime but it's not the only threat. Yesterday, FBI Director Wray talked about the threat from Chinese hackers and said that that country's cyber operations were bigger than all other countries combined -- I assume not including the U.S. -- but I wanted to ask if the U.S. government has seen an increase in cyber threats from China, especially in relationship to Taiwan, or any sort of posturing in that area? And if so, what's being done about that?

INGLIS: Well, first, I would say, with respect to China -- oh ...

(CROSSTALK)

(UNKNOWN): Yeah, just one more question to add to that ...

RAVICH: It's a two-fer.

QUESTION: Thank you. Katrina Manson at Bloomberg. I know you've spoken before about the review of NSPM-13. I was very keen of an update to understand where that is coming out. And also, just a follow up on General Nakasone's remarks and your response to them, when you talk about cyber as an instrument of power in Ukraine, are you seeing those operations as solely taking place on Ukrainian networks or are they going further afield into third party countries or Russian networks? And is that the same argument that you put forward as instrument of power, given it may be Americans with their fingers on those particular cyber tools? Thank you.

INGLIS: There can be a lot of choices. That's like eight questions ...

(LAUGHTER)

... inside of all of that but -- but all good questions. Let me start with the first question. The denominator, right -- when you're talking about anything China, the denominator's large, right? And so, you know, given a population of in excess of a billion, then any commitment of some portion of that population to the use of cyber as an instrument of power on behalf of that country, it's going to be big.

I don't think that we've seen any significant diminishment in their aspirations to use cyber as an instrument of power. I can't speak specifically about any particular application of that, not least of which Taiwan, but to say that we do remain concerned about China's use of cyber as an instrument of power in disinformation, right, in kind of the surveillance that they would do for non -- you know, for purposes that we would find non-security relevant -- that is, you know, not those things that actually aid and abet stability of nations or the -- kind of the interaction of various nations. We are very concerned about that.

And so therefore, we -- while we're focused on the clear and present danger that is kind of obvious in the Ukraine, we have to keep our eye on that larger set of activities, and certainly China remains kind of in that.

NSPM-13, I think the administration's on record of saying "we did review that." It's now, what, four, five years hence -- its -- its original introduction, four years hence, and therefore, kind of a proper kind of -- you know, kind of system would say, "Let's take a look at that to make sure that, in terms of what its purposes are and what its kind of implementation, kind of what its SOPs would be, is it still kind of doing what we expect the way we expect?"

And they've made some adjustments, none of which I would say are significant in terms of the intention of why NSPM-13 was created and none of which I think kind of, in any way, shape or form, diminish the value of the work that would take place according to the processes defined by NSPM-13.

The internals of that, of course, are classified and I can't say anything -- any more -- I wouldn't say any more to that but -- but we're largely in a place, we say, it still works, it's still viable, and it -- and it's still efficient and effective. Both of those properties are important.

And -- and the last bit of your question?

QUESTION: (Inaudible) Russia (inaudible)?

INGLIS: Yeah, so I -- it's a bit of a -- you know, Intelligence Community's great at secrets, not -- not so good at mysteries, and -- and it's a bit of a mystery as to why we haven't seen more, right, vis-a-vis cyber and the Ukrainian kind of situation.

Why haven't the Russians been more successful in using cyber against the Ukrainians? Why haven't they perhaps kind of at least visibly done more kind of outside of that against all the predictions that they would use not just disinformation but cyber broadly to hold not just the Ukrainian society at risk but any of those who would aid and abet them?

And I think that there are many kind of reasons why we might imagine that it hasn't been what we expected. One of those that comes foremost to mind is the Ukrainians are actually quite good at cyber defense. They've been trained richly by a partner just to the north of them for the last eight years to be good at cyber defense.

It turns out they are. It turns out that the kind of activities of the private sector and the public sector combined has created a more resilient kind of infrastructure, both in terms of it's inherently more resilient and robust, and when we find a flaw in it, we can add scope and scale, deploy patches, or interdict those threats on the fly.

It turns out the Russians have not been as aggressive in holding things outside of Ukraine at risk, using what we might call cyber kind of offensive methods, as we might have expected. I can only surmise that, you know, some of that is because they're busy, some of that is because they kind of understand that there are thresholds -- they don't know quite where those thresholds are and they don't want to cross those -- but I'll leave that to the fullness of time, in terms of how to properly understand that.

The situation for us remains we need to make sure that we are resilient and robust by design, that we do that in the largest possible domain of interest, the international domain. We have allies. We need to make sure that we're doing capacity building and that we're defending common kind of resources -- the Internet being one of those -- using the common assets that we all bring to bear, and that, for the moment, if the Ukrainian people need our further assistance to defend themselves, as they have the right to do, that we bring the full resources to bear within the limits of the law, right, to do that.

Now, you've asked about whether kind of something beyond that, kind of a self-organized militia that might be kind of described as a group of vigilantes, whether that's appropriate or authorized -- it is neither, right? It might be, at the moment, useful but it is not appropriate or authorized, right, to have individuals stand in the role of governments. We need to make sure that we do that in the proper channels, using the proper modalities, which I think have been richly deployed.

RAVICH: Well, we've run up and over the hour. I think you can all see why we are so proud to call him one of our own on the commission. National Cyber Director Inglis, Brigadier General Inglis, Chris, thank you so much for taking your time to be here. It was a fascinating discussion. There's a lot more to dig into on the report that Rear Admiral Mark Montgomery and Laura Bate wrote. I encourage you all to take a look at it -- cybersolarium.org, fdd.org.

And with that, I wish you a good afternoon. Thank you.

INGLIS: Thank you.

(APPLAUSE)

END