

March 12, 2025

Featuring Chris Inglis and John Costello

Moderated by RADM (Ret.) Mark Montgomery

Introductory remarks by Dr. Samantha Ravich

RAVICH: Welcome, and thank you for joining us for today's discussion hosted by the Foundation for Defense of Democracies. I'm Samantha Ravich, chair of FDD's Center on Cyber and Technology Innovation, or CCTI. On behalf of FDD, I'm pleased to present today's conversation on the future of the Office of the National Cyber Director, or ONCD.

Five years ago, I had the honor of serving on the congressionally mandated Cyberspace Solarium Commission. One of our key recommendations was the need to create a locus within the White House on cyber policy. "One throat to choke," as Senator King liked to say. We looked at models relying on the National Security Council staff to fill this role but realized that the scope of the effort required working with the private sector and budgetary oversight, neither of which are great fits for the NSC. So, we argued for the creation of the ONCD, and Congress agreed, establishing the office in statute. President Trump signed that bill into law during his first term.

Four years and many cyber, too many cyberattacks by adversarial states later, this administration has a unique opportunity to ensure the efficacy of ONCD. But effective government agencies are not the end goal, merely the means to achieve a national priority. In this case, securing our nation against threats from China, Russia, Iran, North Korea, cybercriminals, terrorists, the list goes on. Each of these malicious actors uses cyberspace to achieve their nefarious goals. And the role of ONCD is to help federal agencies, critical infrastructure, private companies, and the American citizenry defend themselves against growing cyber threats.

I can think of no better experts than those we've assembled here today to talk about these issues:

First, we are joined by Chris Inglis, the inaugural National Cyber Director. Chris and I served together on Solarium. He was always clear-eyed on the challenges as well as the methodical steps necessary to improve national cyber resilience. President Biden's best decision was naming him National Cyber Director to run a startup in the White House and begin to implement a vision for a coherent cyber policy making. Chris is now a strategic advisor to Paladin Capital, a visiting professor at both the US Air Force and the US Naval Academy, and a member of the Huntington Bank Shares and AIG boards. Prior to Solarium, he served as the deputy director and chief operating officer of the National Security Agency and spent thirty years in the Air Force.

We are also pleased to have John Costello with us for today's conversation. John served as Director Inglis' first Chief of Staff at ONCD. I got to know John during our time together on Solarium, where he served as Senior Director and Task Force Lead focusing on resilience and supply chain security. John has also served as deputy assistant director – secretary of intelligence security at Commerce, and director of strategy, policy and plans at the Cybersecurity and Infrastructure Security Agency.

Finally, there is nobody more appropriate to moderate this discussion than FDD's own Mark Montgomery, CCTI senior director. We recruited Mark to join FDD following his time as Executive Director of the Cyberspace Solarium Commission. From his perch here, he continues to direct CSC 2.0, an effort to preserve and continue the Commission's important work. Previously, Mark served as policy director for the Senate Armed Services Committee. And before that, Mark served for thirty-two years in the U.S. Navy, retiring as a Rear Admiral.

Before I hand today's conversation over to Mark, a few words about FDD. For more than twenty years, FDD has operated as a fiercely independent, non-partisan research institute, exclusively focused on national security and foreign policy. As a point of pride and principle, we do not accept foreign government funding. For more on our work, please visit our website, fdd.org, and follow us across social media, including YouTube, X, and Instagram. Wherever you're tuning in from, thanks for joining. Now, over to you, Mark.

March 12, 2025

Featuring Chris Inglis and John Costello

Moderated by RADM (Ret.) Mark Montgomery

Introductory remarks by Dr. Samantha Ravich

MONTGOMERY: Thank you very much, Samantha. And I'm really glad to be here with Chris Inglis and John Costello, two friends and shipmates for the last five years of this process. And John, I'm going to turn to you in a minute and talk about your paper on U.S. cyber governance and the future of the National Cyber Director. Before I do that, I want to go to Chris first with a bit more setup.

Chris, Samantha mentioned, you know, a favorite quote of Senator King's, "one throat to choke." As someone who was that throat for more than a year, what does that mean in practice? And what's the role of the NCD?

INGLIS: Yeah, so first, thank you to Mark, Samantha for creating this venue and to John for a really good paper. I very much enjoyed the paper. You wouldn't be surprised that I, kind of, support just about all of what's in that paper. You and I kind of live that dream together, so it's a delight to be here talking about what might come next. So, Mark, it's a great question. I think it's the right first question. I'm a fan of the "one throat to choke" kind of premises, but I think we need to first kind of consider what the nature of this domain is. So, there are three realities about this domain.

One, is cyber is wider than it is tall. What do I mean by that? I mean that all the people who have a vested interest in this comprise all the people, kind of their individual users, business users, national security kind of communities, all who depend upon digital infrastructure.

Two, the operations that actually then ensure that that digital infrastructure, cyber, meets our expectations, those operations are typically conducted at the edge and they're very hard to actually drive and control, at least granularly, from the center. Kind of asking the right questions oftentimes requires kind of a contact with the – either application of the moment or the adversary of the moment. And so, you need to be somewhat generous in terms of what degree of control you exercise from the center.

And the third reality of this domain is that while cyber may be used as an offensive tool, it's only one of many instruments that can impose consequences on adversaries. And so, for purposes of offense, that's probably better integrated from the government perspective at the National Security Council.

So having said all of that, my sense as to what the 'one throat to grab' is in the form of the Office of the National Cyber Director or the National Cyber Director, kind of him or herself, is that what you want from that person is to be the coach, not the quarterback. The person who establishes the game plan, ensures that the roles are assigned, that those roles are performed kind of according to what some larger strategy might indicate. And that at the end of the day, that the sum of all those parts that are dispersed across a fairly broad set of players, that that all adds up to something greater than the whole. If you get that right, then there's probably going to be three bins of activity that the National Cyber Director takes on.

In the first bin, you want to make sure that there's the strategic setup: define the strategy, assign roles, ensure that responsibilities are understood, and that there are goal assignments for each of the players. Two, align resources. Make sure that in that first box that all of those players have the right authorities, the right resources, whether it's dollars or people. Again, assessing performance means that you've got to have an active participation in how that's all being done. You might want to, in that first box, the strategy box, do a periodic update of what the priorities are because we can't do all things against all perils.

In the second box, which is the day-to-day box, the tactical box, I think the National Cyber Director keeps a pulse on what cyber events are taking place. Again, don't step in and micromanage those, but ensure that they are in fact well-managed. Maybe that's the sector risk management agencies in the federal enterprise. Maybe it's the ISACs, the information sharing and analysis centers doing a proper job in the private sector but just make sure that's going well. And if the White House

March 12, 2025

Featuring Chris Inglis and John Costello

Moderated by RADM (Ret.) Mark Montgomery

Introductory remarks by Dr. Samantha Ravich

needs to step in with resource or policy guidance, or perhaps kind of tip this to the National Security Council, I think the National Cyber Director is expected to do that.

There is in fact a Cybersecurity and Infrastructure Security Agency known as CISA. They're the on the field quarterback that should be actually calling the plays in terms of redirecting resources to shore up some defense or provide meaningful assistance to the – kind of, the affected party. But the coach remains the National Cyber Director.

Closing, I think there's a third box which is perhaps these things that happen in the background that I would say that the National Cyber Director is the 'one throat to grab,' is best place to do regulatory harmonization, ensuring there's a solid connection between the federal enterprise and the state local tribal territorial [governments], conducting periodic exercises just to perhaps see if we're in the right place, things like Continuity of the Economy, making sure that we've got a proper focus on the workforce development, you know, do the skills that we need in this space kind of have the right moxie. And maybe one last thing I'll throw in, which is there was a Cyber Safety Review Board created under the Biden administration, consistent with a recommendation by the Solarium Commission, in part because the Office of the National Cyber Director didn't have the resources at the time necessary to staff that. And in part, because the Department of Homeland Security wanted it so badly, that then flowed to the Department of Homeland Security to stand up and manage. I think that's more appropriately homed within the Office of the National Cyber Director. It is somewhere between the strategic kind of activities that I talked about in box one and the day-to-day activities I talked about in box two. But its proper home is in the Office of the National Cyber Director. All in all, I would say that if you asked me for a one-word definition of what that one throat to grab would be, it would be 'Coach.' And it would be coach for the defense across a very broad population of players, from individuals to national security agencies, and businesses in between. Back over to you, Mark.

MONTGOMERY: Thank you very much. I love your use of the word "coach". I mean, to me, "Coach" impugns accountability. And that's exactly, you know, what you went through there, when you brought together in one big vision is someone who's accountable, and that's different than quarterback, it's different than a lot of other things. So, really great analogy there. And at the end there, you did list everything hard in the government. So, thanks. All right, John. Now we've had the expert. The real subject matter expert, describe what NCD is supposed to be. Let's talk about your paper and how you work to ensure that the ONCD really emerges into this cohesive center, this coach for the U.S. cyber government activity, particularly as it relates to defensive cyber policy, just like Chris said. Tell us why you wrote this paper and then some of your key findings and your favorite takeaways from it. And then you'll be critiqued heavily in a few minutes by Chris.

COSTELLO: Absolutely, excellent. So, first of all, thanks Mark and certainly to Samantha again for such a great venue and Chris, I, you know, appreciate your expertise, your time and, you know, the dialogue and your perspective on what the National Cyber Director could be and what the National Cyber Director is. Obviously, it's not crazy that a lot of the things that we discussed, and a lot of your perspective directly influence this paper. So, the background behind this paper is very simple. It's intended to give, I think, the Trump administration, this administration, a fresh look on issues of cyber governance. And some of the key findings that came, informed this was, you know, fast forward, Solarium Commission put forward a rash of new legislation, and there was a rash of new executive activity at the beginning of the Biden administration and a rash of new policy activity. And while I think each piece part of the federal enterprise has done as much as they can do within their statutory authority to increase, to do policy activity, to do operations, it still appears as though there hasn't been an overall increase in strategic unity. Or there is certainly a gap, I think, to overcome. And part of the things, I think part of that has been, I think, the second finding here, which is the NCD, at least during Biden's first term was a new office just getting its legs from under it. And could have played, I think, a much bigger role. And looking forward, the question is, is how do we instantiate, how do we affirm an appropriate role for the National Cyber Director consistent with the Solarium recommendation, while respectful and acknowledging things like the NSC's preeminence and

March 12, 2025

Featuring Chris Inglis and John Costello

Moderated by RADM (Ret.) Mark Montgomery

Introductory remarks by Dr. Samantha Ravich

primacy on issues of national security? So those are, I mean, that is essential, the basic premise of the paper. And it looks at, I think, key elements or key segments or key mechanisms related to the NCD and the White House and the roles that it could play, and looks to essentially establish those, I think, either more formally or by convention, but just simply by practice, and the pull and inertia of the NCD doing a role and fulfilling that role for an extended period of time.

So, you know, I think some of the key, sort of, takeaways from this paper, I think number one and the simplest and most direct is clarifying and reaffirming the role of the NCD in executive order. If you look back at the history of Senate-confirmed positions in the White House, USTR, director of OSTP, director of ONDCP are all, you know, a good sort of predecessor, not predecessor, but good, roughly equivalent positions. And certainly, ones that we drew upon and drew lessons from in the – Solarium did – in crafting the position of ONCD, of the National Cyber Director. Generally, if they didn't have or didn't benefit from an executive order before they were established in law, usually between one to four years after they come into being, they get an affirming executive order that provides more clarity and provides more, I think, concrete detail on how that position is intended to interact with the broader fabric of the federal enterprise. And some of the things it certainly should focus on, as mentioned in the paper, is reaffirming a lot of what Chris said, is focusing on its budgetary review and assessment role, which is a huge deal programmatically. And reinforcing its position to work with federal departments and agencies in creating plans and creating procedures to prepare for cyber campaigns of significant consequence and respond to those. Those are sort of a few of the key things that we mentioned in the paper that really are fundamental to the ONCD's role.

We also call for the dual hat of the federal CISO. That was an arrangement that Chris himself pioneered with Chris DeRusha at the time that worked wonders. It was a great example of synergy of the federal CISO coming in as a deputy national cyber director and bringing the resources and expertise of the ONCD to bear, fully empowered with OMB authorities. And that's a convention that worked really well and can certainly work again.

But you know none of this would work if it isn't clear, if the relationship between the NSC and the ONCD isn't made clear and that's another, I think, recommendation is clarifying the roles and responsibilities between the NSC and the ONCD. Now look, the NSC is prime on national security issues. That's never -- and that's the way it should be. They are the ultimate convening body on national security and cyber certainly fits into that. The idea that the ONCD would compete with or make redundant any of the NSC's functions is a false issue. The question here is, what is the best marriage and ideal arrangement between the ONCD's expertise and its mandate and resources and the NSC's focus. The NSC works best when it is broad and dealing with core central national security issues: foreign policy, intel, military issues, emergency management. The ONCD can work this from a procedural, operational standpoint while still allowing the NSC, when things reach a certain threshold of importance, to take that on as a core policy issue.

A few other things, just more mechanically, is number one, establishing a formal national cyber community for the Office of the National Cyber—for the National Cyber Director. Right now, if you had to ask what are the core agencies that really form this community the ONCD has worked with, the ones that have the authority, the resources, and the remit and visibility to really make change in this space, that'd be a difficult question to answer. And we're looking to things like ONDCP, which has the National Drug Control Program, a defined list of programs in which their budgetary review authority is derived, and the same thing with the Director of National Intelligence. That focuses the ONCD and gives a core constituency to make more formal policy and more formal procedure within that community.

Another is establishing annual national cyber priorities, creating something that is more long-term than the national security issue du jour, which can shift month to month, and a national cyber strategy, which takes place over a number of years. How are we adjusting and helping align agency efforts in-year, within a budget year, year to year? And that's what that is intended to sort of address.

March 12, 2025

Featuring Chris Inglis and John Costello

Moderated by RADM (Ret.) Mark Montgomery

Introductory remarks by Dr. Samantha Ravich

And then finally, as Chris said it best, harmonizing cybersecurity regulations. ONCD has a major role to play here. You know, there is no mechanism, there is no formal body that has the visibility and has the suction with independent federal agencies to bring them, and to make sure that as we create new regulation, they're done with a consistent set of standards and that they're done with the mind of streamlining and reducing conflict or redundant requirements or conflicting requirements between sectors.

And so those are the major, I think, major takeaways from the paper and certainly eager to talk about them. Back over to you, Mark.

MONTGOMERY: Thanks, John. Before we come back to you, I'm going to talk to Chris. I do have to say, whenever you say dual hat in a cyber document, you kind of you know, create antibodies one way or the other. And I know the dual hat you're speaking about are some of the neat little work that that Chris did with the OMB director over the federal system.

INGLIS: Yeah, Mark, can I just jump in on that just to give a further explanation? So, when we got to the Office of the National Cyber Director, one of the first fights that we were urged to pick was to reach out to the Office of Management of Budget and pull the federal CISO into the Office of the National Cyber Director, which we didn't pick that fight. What we did was we went there, and we said we would like to give the federal CISO some formal authority. It's kind of a position that traditionally has been in the Office of Management of Budget, but it was not established by law, and it therefore didn't have any formal ongoing authority. So, what we offered was, let's kind of deputize the federal CISO, let that person continue to live in the Office of Management and Budget, deputize them as the Office of the National Cyber Director's Deputy for Federal Cyber, and therefore connect those two missions so one plus one can equal three. What we didn't realize is that the additional benefit of that aside from having some degree of conformity of how the ONCD and the OMB addressed the federal CISOs, of which there are more than one hundred and fifty, was we were able to then align the budget. OMB being responsible for budget then gave us greater access to an understanding of how that money was allocated across the federal enterprise. And so, we got one plus one equals four. That's the kind of harmonization I think you get from dual hatting, not by diffusing responsibility, but perhaps giving extent responsibility, greater leverage.

MONTGOMERY: Yeah, thanks. That's a great explanation. So, Chris, you've clearly read John's paper and heard his discussion right there. I was hoping I could get some reaction from you on which of his recommendations strike you as most important. And then perhaps, and this might be a different answer, which do you think are most likely to happen?

INGLIS: I think the recommendation that says let's actually define, five years on, precisely what we want that role to be and writing it down in an executive order or some other similar mechanism is, I think, the right step forward. As Eisenhower once said, you know, "The plan is nothing. Planning is everything." That will cause people to work their way through, "What are my expectations of these various roles?"

I think the greatest challenge that I experienced, not just on the Solarium Commission, but in standing up the Office of the National Cyber Director, was not the threat from moment to moment, but it was the incoherence of the defenders. Who's doing what? How do we actually align all of these resources so that we actually can create something greater than the sum of its parts? So, I think that's the right first step going forward.

MONTGOMERY: Thanks. That's good. I agree with that. And I do think that – I do like the dual hatting potentially with the NSC as well. I think that to me that'll kind of lock in the comfort factor that National Security Advisor Waltz would have with really giving the defensive mission up, which, judging by who he's organized on his team so far, director-wise, strike me as three people with offensive cyber backgrounds, four with the intel person as well, really oriented that way in a much different way. So, I hope you're right.

March 12, 2025

Featuring Chris Inglis and John Costello

Moderated by RADM (Ret.) Mark Montgomery

Introductory remarks by Dr. Samantha Ravich

So, for both of you, I want to take another moment to hammer this home. What is the one sound bite on how President Trump and his team, his apparent nominee, Sean Cairncross – how can this relate to the new office -- it's still a new office by federal government terms – get up and running to its full potential? John, we'll start with you.

COSTELLO: Seek clarity. Seek clarity immediately and do good things. I think Chris is right. Asking the question of, "what do we want this role to be," the sausage making and figuring that out is worth all the gold in the world. You know, it ends up in executive order, ends up in agreement. But more important than that is just continuing the good work. There is a normative norm that's established just by the office going and doing the things it has been doing and the good work in pulling the defenders together and creating unity from chaos. I would say just full – I mean, it's exactly what Chris did, which was let's get in there and let's do good things. A simple answer, but I think a direct one.

MONTGOMERY: So really get the executive order done. This is what you're getting clarity there. Chris, over to you.

INGLIS: I think I would have to say that I give the Trump administration credit for having already done this thing, which is to let's assign some responsibilities that naturally complement one another, don't conflict with one another. Now, under the Biden administration, no shame. They actually had to plan to stand up that administration in a world that did not have an Office of the National Cyber Director or a National Cyber Director, because that came into being about two months after the election, slightly before the administration took office. But they had to have all their plans in place, which is why they put such a strong element in the National Security Council that I think would have been better placed in the Office of the National Cyber Director.

The oncoming Trump administration has in fact nominated somebody to be the National Cyber Director. And what they appear to have done on the National Security Council side of the house is to install folks who can actually think about how to integrate all the instruments of national power. And if cyber lives there in some manifestation, it's going to be how does that actually kind of live alongside all the other instruments of power that we use to impose consequences. That is then naturally aligned between those two components, I think that, you know, that's the picture that you see on an org chart. The video can then in fact be coherent as you come off freeze frame and you have those two parties act with one another, hopefully in a collaborative fashion as opposed to a strict division of effort. But I think we're on the right course at the moment.

COSTELLO: Yeah, Mark, I'm going to piggyback on Chris's comment. I completely agree. The Trump administration, at least the emerging view, is that they've taken into account the existence of the ONCD and planned accordingly and had those people at the NSC laser focused on, like Chris said, the core higher level issues of national security in which cyber is a constituent part. And the defense and security, I think, piece, the procedural programmatic role that the ONCD can play gives them a green pasture to go and to fully, fully fulfill that role that was designed for them. Again, no shame on the Biden administration, but it seemed to have been a clash of models, you know, not accounting for the ONCD and the ONCD, in fact, being there. But it looks like the Trump administration is headed to a certainly more cohesive model.

MONTGOMERY: You know, thanks. The thing I think about when I look at this is people and getting people hired. Look, there's a handful of these jobs, ten to twelve should be Schedule C's. So political appointees that are fairly rapidly in place, they should actually be putting those in place now. People that the incoming NCD is comfortable with. Get them in. And then there's about thirty-five newly empty jobs that were previously Schedule C, Schedule A that could become, which is to say generally political appointees or close to political appointees. They should be put in USA Jobs and hired as civil servants. I mean, to my mind, that's the right way to get it, and then get the office back up to eighty to eighty-five people. You know, it's down around thirty-five right now, which is, um, thirty-four more than when Chris took the job. Um, so, um, and thirty-three more than what you came over, John. So, my gut reaction is they're in great, they're in good shape. And now they get to pick a team to the missions they want. That's a mix of, the right mix of Schedule C and non-Schedule C. And I think if we could do that, we'd be in great shape.

March 12, 2025

Featuring Chris Inglis and John Costello

Moderated by RADM (Ret.) Mark Montgomery

Introductory remarks by Dr. Samantha Ravich

INGLIS: Mark, I think that's exactly right. That's exactly where they are. They have some positions that endure across the transition of the administrations. They're there ready and willing to, at speed, serve the needs of this administration's views on what that role should be, and a number of positions that are open that can be filled so that we that can fine tune it and send it in the direction that they prefer. I still remember showing up. I remember a reporter asked me on my first day, "what are your plans?" And I remember kind of somewhat jocularly saying, "well, we're going to double the organization, double it, double again. That'll make eight of us." And the reporter said, what does that mean? I said, "Do the math." They're not in that place. They can actually start at speed across the broad front in the moment.

MONTGOMERY: They just have to say double it once. Hey, that's great. Thanks. So, John, as you remember from the Solarium Commission, we recognize that some of our recommendations weren't going to happen. I mean, Jim Langevin was locked in on a single cyber committee in the House and Senate and didn't take long to get Senator King right there with him. I think a lot of us who working the issue, kind of knew it wasn't going to happen. I mean, short of like a major cyber event, where the burning ember of blame, finger of blame, was pointing at Congress, which is not considered, not likely would we get Congress to reorganize, and committees to give up their parochial self-interest—that just doesn't happen. Jurisdiction doesn't transfer that way. In your report, you've got, I'd say ten or eleven, there's some that repeat between sections, but ten or eleven really solid recommendations in here. Which one of them is not going to happen?

COSTELLO: That's a good question. If I had to, if I was a betting man, I would say the National Cyber Community. It would require, I mean, there's an executive version, executive order version of that. But for really, for it to be powerful, you need essentially the authorization of a "National Cyber Program" or a "National Cyber Mission" with a very defined list of programs that the ONCD would oversee. And that would form the basis of the community. That is, I think, far too mechanistic. I think it's far too hard for this Congress to consider. I think there is a version of this that you could do just purely on an executive level that gets a small core constituency on pure cybersecurity and defense issues.

One thing that I'm hoping for, though, is cybersecurity regulatory harmonization. That does require legislation. Only Congress can force independent regulatory agencies to participate in a body and to do so meaningfully. And that's what you need here. It's one thing to get the regulators within the executive branch together and to get them to agree to use a common framework, to work with each other to harmonize their requirements or de-conflict their requirements. But that means very little if the independent regulators aren't at the table and aren't required to participate. Now, anything legislation is harder, but this came up last Congress. So, I'm taking a little bit of leeway with your question, saying one thing I really hope for, that may be hard, is a cybersecurity regulatory harmonization piece.

MONTGOMERY: Well, in theory, I mean, the Republicans control both chambers and tend to look for less regulatory environments and harmonizing regulation by design does that. We'll see. Chris, what did John, did he miss something in the paper? As we've had this discussion today, is there something you'd want to highlight specially, recognizing the paper was pretty constrained to cyber governance in the NCD?

INGLIS: Yeah, so first, let me not damn it by faint praise. I think it's a good paper. But it's hard in any paper to say enough about the role of the private sector. So, I think that we can expand on that.

Given that the Office of the National Cyber Director, we think, and I imagine under this administration will be focused on defense, that there is an ample opportunity to allow the private sector to come into that and to help in the decision-making about what the priorities should be, and to help in terms of maybe even the tactical decision making about what we should take on in what order. There was a moment, I think it was about eight years ago, when the FBI, probably the Department of Homeland Security as I recall, but, a large swath of the private sector took a look at some cyber threats and said, we think we should kind of act to take them down in this order, not in a provocative offensive mechanism, but essentially defensive mechanism. And a fellow by the name of Dmitri Alperovitch, who's kind of very persuasive in this area, talked about that being a golden moment of collaboration between the private and the public sector. I agree. And I think we can

March 12, 2025

Featuring Chris Inglis and John Costello

Moderated by RADM (Ret.) Mark Montgomery

Introductory remarks by Dr. Samantha Ravich

get to that place. We can get closer to that place as we go forward. But the private sector is on the front lines. They build, operate, sustain, and largely defend even critical infrastructure. So let's figure out how to get them into the play, at least for defensive purposes.

MONTGOMERY: And I agree, the NCD is probably the one senior position in government that can do this, the kind of CEO-level outreach that's required. The National Security Advisor could do it, but he's too busy. The Chief of Staff at the White House could do it, but she's too busy. Other than to field gross complaints from very, very senior CEOs, and they'll always take that call on a theory of there's a potential future donation here. And then I think CISA right now is probably head down on a lot of issues and I just don't think they're going to be that person. So, I like that. I like that highlight on the private sector.

All right. Here's an interesting thing. It wasn't the goal of your paper, but we've averred to offensive here a little bit for both of you. I've heard Mike Waltz say when kind of confronted with, "Hey, what do you think of Salt Typhoon, Volt Typhoon?" He said, you know, "We've got to get more offensive." What's that mean to you, Chris? And here I should remind people you were the deputy director of the National Security Agency as well. So, you've got some strong bona fides here. What's that mean to you? And then, John, I'll come to you after Chris.

INGLIS: Well, in a general sense, offense to me means you're going to impose cost on a transgressor. Now, hopefully you're going to use all the instruments at your disposal, not just cyber cost, but financial cost, sometimes kinetic military cost, kind of diplomatic, but apply the pressure such that you're imposing cost on transgressors. And in a larger vein, I think what you're trying to do is to change the decision calculus of those transgressors such that they're not going to come at you tomorrow because they've suffered a cost today. What I hear this administration saying, and maybe it's wishful thinking, but I do think I hear this, is not so much we're going to substitute offense for defense, but we're going to align the two. We're going to bring offense up such that if there are two ways to change the decision calculus of an adversary, one is we're a harder target. That's a focus on defense. The second is we're going to impose cost on them if they still come at us. Aligning those actually makes for a stronger defense. So, in that case, offense actually becomes an extension of the defense.

I think without a proper defense, you're kind of shooting in a glass house, right? What the Marines say is true. When the enemy's in range, so are you. So, I think we have to do both of those. And so, what I hear this administration saying is that we need to bring offense up to the line and have it play its full and fair part.

MONTGOMERY: Thanks. John?

COSTELLO: I mean, it's hard for me to follow Chris Inglis on this topic. I would say, you know, I would agree with Chris. I think this administration, they're not looking for, this isn't a zero-sum game between offense and defense. I think they're looking to continue a lot of the things that the Trump administration and Biden administration have done in strengthening our cybersecurity and cyber defense ecosystem. That includes uh, stronger partnerships with the private sector. But I think it also, there's a presumption here that the United States has not fully leveraged its technical and operational capability in cyberspace, or financial constraints that get imposed on an adversary to the extent that it possibly could, and that there's a greater gap to fill there, hopefully, in changing the cost calculus of our adversary, making it so that either their operations take longer amounts of time, are costlier to them, and thus they can do fewer of them. They take fewer risks, or they have a higher risk calculus when they engage in a particular operation, or they stop it altogether in certain circumstances. Things that we've identified or, you know, signaled squarely as off the table.

That's what I think the Trump administration is trying to do, is they're trying to make sure that every part of this, from the cost imposition outside of cyberspace, sanctions, indictments, et cetera, to cost imposition inside cyberspace, whether it's military or intelligence operations, to create friction, to fully utilize those in parallel to defense so that we can get to a better place than where we are now.

March 12, 2025

Featuring Chris Inglis and John Costello

Moderated by RADM (Ret.) Mark Montgomery

Introductory remarks by Dr. Samantha Ravich

INGLIS: If I could add...

MONTGOMERY: Go ahead, Chris, yeah.

INGLIS: Mark, I just want to add. So, I would say that what you should expect out of this Trump administration is going to be an extension as opposed to a cold start out of the first Trump administration. All of us can remember kind of in the age of, say, from 2014 to 2017, that our own restraint in not exercising cyber on cyber responses to cyber aggression. We now believe we're escalatory. Wanna Cry, Not Petya, the kind of authored by the North Korean regime and the Russian regime, respectively, had a very significant effect on critical infrastructure around the world, which is why in 2018, I thought that the trifecta of policy changes under the first Trump administration were completely appropriate.

First, the Congress defined, and it wasn't necessarily in this chronological order, but I'll do it in policy order. Congress defined cyber operations as a traditional military activity, no longer requiring special permission on behalf of the president. Two, U.S. Cyber Command, the Department of Defense defined something called Persistent Engagement, Forward Defense, which are not provocative offensive measures, but rather solid basis of defense that says, I'm going to figure out what my adversaries are doing at the earliest possible moment, and I will hold them accountable with the highest possible leverage as far forward as possible. Again, not provocative, but again, being fairly proactive in the defense. And third, while the contents of this are still classified, the White House authorized something called the National Security Presidential Directive-13, which at the unclassified level we can understand as authorizing kind of envelopes within which various instruments of power, to include U.S. Cyber Command, can operate to hold an aggressor, a transgressor at risk when they're holding something we care nearly and dearly about in cyberspace. So I'll just hypothetically imagine the possibility that if there's an adversary that is kind of holding our critical infrastructure at risk, we can authorize kind of various instruments of power to actually do something about that in the moment without having to call a national security meeting every moment to figure out what are we gonna do tactically in response to that. That, I think, is being more proactive. It might look like we're being more aggressive, perhaps we are, but it's actually saying we're going to use our offensive capacity to actually sustain and extend our defense in ways that are appropriate. I look for more of that under this administration.

MONTGOMERY: You know, I love that, and you're absolutely right. Number one and number three, the law change and the NSPM-13 were certainly linked. I was working for Senator McCain at the time, and we had, you know, the law change happened, and with definitely the willful engagement of U.S. Cyber Command and the National Security Council. And two weeks later, reportedly, the National Security Presidential Memorandum-13 was signed. So certainly, the linkage is there. And I think that if you're exactly right, if this administration continues the trend where they left it in 2020, I think that, you know, that bodes well.

I will say the Volt Typhoon thing drives me batshit. Because here's a country going in, they're putting this malware or other malicious cyber activity that lives off the host in a bunch of our critical structures that we know are key to military mobility, economic productivity, even a little bit of public health and safety.

If we had found a thousand satchels, each with explosive in it, strapped to the same transportation, ports, aviation, and the satchel said, "courtesy of the PLA," we would be in a condition either of war or just short of war, and we would certainly have retaliated in a significant, meaningful, measurable way.

But in cyberspace, we're like, "well, good job, boys." We're treating it like it's espionage when it's not espionage. You know, I get the hat tip for espionage idea--

INGLIS: I strongly, strongly agree. Strongly agree. I mean, this is different in kind. Look, I think it's improbable. I don't think it's likely that we're going to have a kinetic war with another major power. I hope to God we do not. We all suffer in that regard, but if it comes to it, so be it.

March 12, 2025

Featuring Chris Inglis and John Costello

Moderated by RADM (Ret.) Mark Montgomery

Introductory remarks by Dr. Samantha Ravich

But if that were to happen, I think historians, when they look back from the year 2050 to say, when did this thing start? It would start before the moment that we're in at the moment, right? They would say, when we began to see the seeding of our critical infrastructure with malware, whose only purpose it is to hold our society at risk, that's a problem.

MONTGOMERY: Well, Chris, John, thank you both very much. I think you've given us a lot to think about. I think the audience appreciates how you two have been so direct and concrete today. And we really have NCD employee number one and NCD employee number two. I know there's some temporaries in there, but really – the two of them and you've been giving us a lot of thought.

And I hope NCD employees number you know 107 through 134, who are about to be hired over the next over the next three to four months, are watching this podcast to get the idea, they read John's paper – I don't agree with everything in John's paper, I suspect Chris doesn't agree with everything, but I think it's a great summary of the challenges in front of us.

So, thank you both for joining us. And thank you to our audience for tuning in. Look forward to broadcasting out to you guys again soon.

COSTELLO: Excellent. Thanks, Mark.

INGLIS: Thanks to you, Mark, and to the FDD for your advocacy going forward. Good luck to us.