FDD Media Call: Building the Future U.S. Cyber Force

September 9, 2025
Featuring Dr. Erica Lonergan and RADM (Ret.) Mark Montgomery
Moderated by Joe Dougherty

DOUGHERTY: Greetings and thank you for joining us for today's call. My name is Joe Dougherty, I'm Senior Director of Communications here at the Foundation for Defense of Democracies, a nonpartisan research institute focusing on national security and foreign policy. We're grateful that you've joined us today as we detail the findings of a new report from FDD's Center on Cyber and Technology Innovation. The report "Building the Future US Cyber Force: What Right Looks Like" effectively gives the Pentagon a head start in an organized and thoughtful way of how best to build a US cyber force and doing it without harming existing capabilities during the transition. The embargo for the report lifts tomorrow morning at 6:00 AM Eastern and we will get you the link to the report shortly after this call concludes.

Joining us on today's call are the two authors of the report, Rear Admiral (Retired) Mark Montgomery, Senior Director of FDD's CCTI, and Dr. Erica Lonergan, Adjunct Fellow in FDD's CCTI.

Before we get started, a couple of housekeeping items. Today's call is on the record. We'll share the transcript and the recording of the call within 24 hours, hopefully much sooner. If you'd like to ask a question, you may type it into the chat feature and I'll be happy to read it aloud for you. Or you may use the raised hand feature, and we'll unmute you and you can ask your question directly.

We'll begin today's call with Mark, who'll provide a larger picture framework. And then we'll go to Erica who will provide some specific and key findings and recommendations of the report. Mark, over to you.

MONTGOMERY: Thank you, Joe. Thank you very much for having me. It's great to be here with Erica.

Look, it's a pretty straightforward issue. What we're trying to answer is the how you build a cyber force. That's what right looks like. This builds on work that Dr. Lonergan and I did early last year on why you need a cyber service. Erica has previously been at the Army Cyber Institute at West Point and has a deep knowledge of how services build cyber warriors. And so she and I were a good team to address what was going wrong in the performance of the military services and doing the cyber mission.

The conclusion we came to is that the reason we need a cyber service is to address the force generation challenges that each of the military services were experiencing. And by force generation, we mean recruiting, training, maintaining, and retaining cyber personnel. Each service might be good at one of those four elements, none were good at all four, and at least one service was bad at all four. In the end, that meant we were having insufficient force generation.

As part of this process, there was interviewing of about just under 100 cyber warriors across the rank structure from E-5, E-6, up to O-7, O-8, so from mid-grade enlisted to generals and admirals, across all the different military services at the time. And 100% of them said something's wrong. Now, 100% didn't say you need a cyber force, but 100% said you need something different than the status quo. And so that became the basis of this paper.

And look, Congress has looked at this issue a lot. This is not an issue of, Oh my gosh, no one saw this coming." Josh Stiefel, who is a former professional staff member at the House Armed Services Committee, studied how many pieces of legislation had been passed about trying to fix the readiness problem, the force generation problem in the various military services. And the answer was 50 to 60 pieces over eight or nine years. And you compare that to when we started SOCOM and SO/LIC, the special operations issues, they needed about 15 pieces of legislation over 20 years.

So clearly Congress was looking at this and saying, "You're not doing this right." And they weren't. To be honest, if you go to service chiefs and ask them, "Is cyber a priority?" They'd say yes. And then you say, "Well, which priority is it, in your top 13 or 14?" And the answer is always like 11 or 12, or 13 out of 13, or 14 or 15. And that's what I would call traditionally a bill payer, not a resource enabler.

So what we decide is determine how you do it, look, the reason Erica and I pushed this forward... And we're both part of a task force that'll take a long-term look at this. I acknowledge there's a congressionally mandated study that should be done in 18 to 24 months. And the task force that Erica and I are on separate from that, probably be done in 6 to 12 months. There's a chance that President Trump makes the decision in 6 to 12 weeks. And if that's the case, someone needs to have done a blueprint. And I couldn't have thought of anyone better to think about the vision, the mission, and the functions of a future of a cyber service... So when we say US cyber force, we mean a dedicated cyber military service. I can't think of anyone better to think about that, write about that, and discuss it, than Dr. Erica Lonergan from Columbia [University]. So, Erica, I'll pass it over to you to talk about some of the details from our study.

LONERGAN: Great. Yeah, thank you so much. So I was really excited to work with Mark on this part two of our effort to not just make the case for the creation of a cyber force, but then also articulate what we think it should look like based on the idea, as Mark said, that there's a chance that the decision is made to create a cyber force and then we don't want to be scrambling to build the aircraft as we're flying it, but to have some sort of ideas thought out in advance to guide the implementation. And so what we are trying to do in this monograph is really articulate a set of core principles and philosophies and vision that should guide the building of this service. There are a lot of additional decisions that will need to be made if a service is created, but our hope is that this product can provide the blueprint to help guide whatever team is responsible for ultimately making those tough decisions.

And just so for some additional context, I think obviously we have experience with creating new services, right? We created the Space Force in 2019, the Air Force many decades ago. But the creation of a cyber force presents a really unique challenge, which is why it's so important to think about these issues in advance.

One challenge is that unlike the Space Force for instance, which was created basically out of personnel and capabilities from the Air Force, a cyber force is ostensibly will be drawing in personnel from across all of the existing services. And part of the motivation for why we think we need a cyber force is because all of the services, not only are they not prioritizing cyber, but they have different standards for recruitment, for training, career progression models and compensation, and MOS definitions, and so on. And so a cyber force is going to have to figure out how to take all these disparate personnel across five existing services and form them into one with coherent standards, a common culture, and so on. So that's why thinking through this in advance is really important.

Another reason why it's important to think about this carefully is because the cyber domain presents really these unique challenges around who are the right personnel that we need for warfighting in the cyber domain. They probably look a little bit different from what you might need to excel at warfighting on the land, the maritime domain, and so on. And so how do you structure a service that has a culture, and that has a force structure, and that's defined a career progression model that's matched to maximizing our effectiveness in cyber conflict, which will look different from all the other services?

And the other reason we think it's important to think about this now is because the cyber domain, as we know, is this dynamic environment. The technology evolves, the nature of the threat environment evolves, the requirements and the missions change. And so we wanted to set out a set of principles that should be the North Star for building and growing this force over time, but one that takes into account the fact that specific decisions may adjust over time, where we need a flexible adaptive model and constantly have periodic assessments and reassessments to make sure that we're achieving the objectives we set out to.

So with that said, what the paper does is it outlines this core vision and mission for the cyber force. It defines what things the cyber force, what things we think the cyber force should do, what its core mission should be, and what we think should be outside of the scope of the mission set of the cyber force. And we think it's equally important to define what it should do as well as what it shouldn't do because cyber is such a... There's so many things that relate to cyber and cyberspace and cyber security. The cyber force can't do it all. So we identify three core missions for the cyber force to organize, train, and equip personnel for defensive cyber missions, offensive cyber missions, and cyber as it relates to intelligence.

And the last one is really essential. We need capabilities for foundational cyber intelligence so that we can have a better understanding of our adversary's cyber capabilities, their leadership, their strategy, their centers of gravity, their vulnerabilities, and so on. So we tend, I think, to focus a lot on cyber defense and cyber offense, but the intelligence piece is just as important.

And then in terms of what the cyber force won't do, what we define as being outside of the scope of the cyber force, I would say the first really difficult but important cut line will be the defend versus the protect mission. So while the cyber force will be responsible for generating capabilities for cyber defense, we think it's outside of the scope of the cyber force to generate capabilities for cyber protection, right? So DISA's mission, we think the cyber force should not be responsible for building, securing, operating, maintaining, sustaining the entire DOD network. If the cyber force has that responsibility, the reality is it will dwarf all of its other missions, especially in the beginning.

We also think the cyber force shouldn't be the information warfare service. While, obviously, there are some cyber equities and information operations and the cyber force will play some role in generating capabilities that are relevant for that, overall, the information environment is much broader than just cyber space. So again, we don't want the cyber force to get bogged down by that mission.

And then relatedly, the cyber force won't be the AI service. The cyber force will have some equities in developing or acquiring AI capabilities that pertain to its cyber missions. But AI is a general purpose technology, lots of DOD stakeholders have equities in AI.

So that's, broadly speaking, what we see as the core missions and being outside of the core missions. And from that, we go into quite a bit of depth in the paper about what's in versus what's out that follows from the definition of those missions. I won't get into all the details on this call, but we have a couple of basic propositions I just want to underscore for the purposes of this conversation. As Mark already mentioned, cyber force would be a new Title 10 military service established, we think it should be established within the Department of the Army, but it's important to note that it will look different from existing services in terms of things like proportion of civilian to uniformed military personnel. We think there's a really important case to be made for the role of the Guard and Reserve components, especially thinking about non-traditional Guard/Reserve models. That's one key, one key finding.

The other is in terms of its relationship to Cyber Command. Cyber Command would of course continue to exist. Right? It would continue to be the primary force employer, and now it would have a corresponding force generator. But the Cyber Force would also generate capabilities for other combatant commands that have equities in cyberspace, so SOCOM and Space Force and so on. So, just like the other services, the US Cyber Force would generate capabilities for the full complement of force employers in the cyber domain.

And then the other sort of cut line question, what's in, what's out, pertains to the existing services. Right? So, just like when the Air Force was created out of the Army, the Army retained aviation capabilities, so does the Navy, the Marine Corps has aviation, and so the same would be the case in cyberspace. And so there would have to be decisions made about what cyber capabilities would be service retained and what would be the primary responsibility of the Cyber Force. We think each of the services could define, recently defined some areas where generating cyber capabilities are uniquely relevant to their core missions. Right? So for the Army, EW, Tactical Cyber. Any transition team responsible for standing up the force would have to make those decisions.

And then we also, we have a table that I would turn your attention to in the paper that outlines for various cyberspace operations forces, groups, as well as other kind of elements and organizations across the DOD enterprise, what we think would be in, what we think would be out. The main point is that we argue the cyber force would assume force generation responsibilities for the Cyber Mission Force, as well as the various joint force headquarters and the newly renamed Department of Defense Cyber Defense Command. And then when it comes to other organizations, we have recommendations for how to think about how to draw those cut lines.

And then finally, I just want to turn your attention to the design principles that we've articulated to inform building the service. Again, these are the Northern Stars, guiding lights that we see as shaping those more sort of specific tactical decisions as the service is built.

The first design principle is quality over quantity. This really gets at the fact that personnel, specifically quality, technical skilled personnel with domain mastery are essential to maintaining our advantage in cyberspace. And so, how do we assess personnel coming from across the existing services for fit for joining the Cyber Force? We shouldn't assume that everyone who's currently in a cyber role, per se, will necessarily automatically transfer over into the Cyber Force. Instead, we propose that there has to be an accessions process that takes into account the divergences across the existing services. But the key thing is recruiting and retaining the right people to perform the mission.

The second is an expertise based career progression model. And so, this is where we argue that the model should adopt some common practices that exist across the private sector, rather than the military's kind of up-or-out model where you have to get, after a certain... First of all, where there are time and grade requirements and where if you don't get promoted, then you're out. Instead, highly skilled individuals should be able to pursue a career in a technical role for the duration of their career without necessarily having to get promoted. And your progression should follow from your demonstrated expertise, rather than a time in service. Right? So, just thinking about different career progression models that really optimize recruiting, retaining, and promoting the quality personnel that we're looking for.

The third is establishing an iterative and adaptive force structure, I alluded to this earlier. We really need to make sure that the force structure that we establish reflects the dynamic nature of the cyber domain. This is different from the current CMF Force structure where you have a set number of personnel organized into a team structure. Instead, we argue for some smaller, more specialized elements that can be combined and put together in various ways that match the requirements of the mission, the changing nature of the threat, the changing technological environment, and so on.

The fourth is a phased transition. Really making sure that we take due care in standing up this service, not to disrupt ongoing operations. This is a real difference, another difference between establishing a Cyber Force versus prior services, right? Cyberspace is an environment of constant engagement and competition, and so we need to make sure that we carefully phase the build to take into account ongoing operations. But that shouldn't be a reason not to establish a service, because the reality is that there is no time where the US will be not engaged with adversaries in cyberspace. So, it's better to do this now before a major crisis or contingency or conflict with a peer rival, rather than during one or after the fact.

And then finally, and this is really a key point I want to emphasize, and then I'll turn it back over to you both, is organizational leadership and culture are really essential. I mentioned this earlier when I talked about bringing in personnel from the existing services. This will be a real challenge, is how do you foster a distinct organizational culture, a service culture that reflects the unique nature of the cyber domain, that also reflects broader military culture and can be integrated within the joint force? So, you need to make sure you have the right leadership, especially the first chief of cyber, who can set the tone and figure out how to instantiate a distinct organizational culture for the Cyber Force. That links back to recruiting and retaining the personnel that you need, ensuring flexibility and adaptability, given the dynamic nature of the environment. But really, leadership and culture are no fail propositions.

So with that, let me turn it back to you.

DOUGHERTY: Thank you very much, Erica. Thank you, Mark. Very much appreciated. We're going to switch over now to the Q&A portion of the call. If you would like to ask a question, you can do so in the chat feature and jot that down, you can also use the raise hand feature. And my colleague in the background doing a great job, Krystal Bermudez, will unmute you and you can ask that question.

I will get it started with a question here and this goes to Mark, and we'll start going to one of the key counter arguments to your research. Why can't Cyber Command take care of all this?

MONTGOMERY: Yeah, thanks, Joe. First, I do want to say one thing that Erica mentioned I should have mentioned too. We do believe this should be in the Department of the Army. Not everyone agrees with us, neither the study that Congress started or the CSIS task force, we'll start with that as a starting point. But Erica and I reached that in the "Do we need a Cyber Force?" discussion last year. So, we maintain that.

And I'll just say really quickly, one of the reasons we believe that is first of all, we are trying to keep costs down and setting up a new service secretary, it would've been easily the highest cost. Two, we saw from the expansion of the Department of the Air Force to be the Department of the Air Force and Space Force, it actually worked. And as you may know, the Department of Navy has the Marine Corps. I certainly knew that over a 32-year career. But the Department of the Army has an opening there. Also added bonus, the Army is shrinking, so its service secretary was actually set up for a slightly larger force than they have, and it's shrinking without the Army being willing to acknowledge it. So they're not shrinking the Secretariat. So actually, getting this under them wouldn't matter. And I'll be honest, of all the services, I do think the Army has been the least worst at doing this, and that's how I would fairly describe it.

Now you asked, why not a Cyber Force that's a great... Why not put this at Cyber Command? And the answer is, they're the force employer. It isn't like PACOM's got its own Navy, Air Force, and Army. No one ever says that like, "Boy, PACOM would really be able to kick ass if they only had their own services directly to them." Instead, they have component commanders from services. Right? So, you need COCOMs or force employers. In fact, one of the big challenges we have right now and I think the press ought to be really digging into, is we have moved procurement and acquisition to a combatant command, the Cyber Command. And I was guilty of that, myself, Representative Jim Langevin, and others. So tired of the services screwing up procurement, cyber procurement, that we created cyber procurement authorities at the combatant command. So one of the things I would do over time is pull those authorities back and put the tool development, because that is part of force generation in the cyber service.

So, Cyber Command is built to employ forces to go usually overseas, 99% of the time overseas, and impose America's will on adversaries in order to serve US national security interests. And I would just say, I don't believe that any combatant command can also be a military service. And a perfect example is SOCOM. SOCOM cannot generate its own military forces. SOCOM, Special Operations Command, does not run Navy Special Warfare training in San Diego, the Navy does in that case. And we can get into later on why uniquely Special Forces are different than Cyber Forces. But the core reason that you don't have Cyber Command do this is that they are a force employer.

If I could add one other thing, they're currently a force employer and also the National Security Agency. So I'd say gently that the answer to, when should we split NSA and Cyber Command is, let's add Cyber Force into the mix. That's not the answer, is not to give that person a third hat.

LONERGAN: I would also just to quickly add onto what Mark said, is this issue of civilian oversight too, right? This is the structure that we've set up, it goes all the way back to Goldwater–Nichols, right? But a really important part of the role of the services in organizing, training, and equipping, is that we have robust civilian oversight of the military. And putting those responsibilities within a combatant command, obviously there's some oversight and we have this new Assistant Secretary of Defense for Cyber. We have new civilian roles in the Defense Department, but it's not at all the same as having a service, a military service. And so, I think that's another key part of this argument.

MONTGOMERY: And in fact, while when we wrote the ASD for Cyber language, the Defense Department in general not supporting it, and specific, didn't allow it to have much oversight responsibility or any of acquisition and procurement at Cyber Command. So, following what DOD said there, it's clear that they understand Cyber Command is not the place to have this kind of service-like entity actions going on. So, we need an independent military cyber service.

DOUGHERTY: Very good. We do have a couple of questions in the queue. David Jones, we'll get you in just a moment, but we're going to start with Mark Pomerleau. Mark, over to you.

POMERLEAU: Hi, can you hear me?

DOUGHERTY: We can. Thank you.

POMERLEAU: Super. I'd like to maybe dig a little bit more into the why now discussion. I think you both got into that a little bit, but I know that some have been concerned with how Space Force was stood up and I'm wondering if you can elaborate a little bit on that and draw some distinctions to how you possibly want this to be a little bit different and why now is the right time for this type of a blueprint or framework, if that makes sense.

MONTGOMERY: Yeah, I'll start and pass it to Erica on that. So the why now is because we are year over year falling further and further behind our adversary. And let's be clear, we set up... I was part of the team that did it. We set up each service contributed to the Cyber Force back in 2010, around 2100, 2000 personnel. That's Army, Navy, Air Force, Marines caught like three or 400. That 6,400 became the baseline for our cyber mission force. And that number in the ensuing decade, or now 14 years, has changed about 3 or 4% to maybe 6,600. By comparison, the Chinese offensive cyber operations, it's very hard to put an exact number on it, but it's increased somewhere between 600 and a thousand percent, six to 10 times they've enlarged, and they're now significantly larger than the United States. That doesn't mean they're better, although quantity does have a quality on its own when you have this many malicious cyber actors moving around your systems.

And I would say the threat, the Chinese, Russian and Iranian threat and their network sizes have increased significantly over 15 years, certainly more than 3%. Now, why is it only growing 3%? It's only grown 3% because the services don't want to give up more people. I remember very clearly the dictum going into those meetings was don't come back with having given up more than 2000 or 2300 people. I'm sure each of the services had that same dictum. The idea is that you come in and out of these meetings with about a number. And its services aren't going to give more because if you had to give another thousand or 2000 from the Navy, that would be unmanning four or eight destroyers. If you had to give that from the Air Forces, unmanning three or six squadrons. From the Army, it's two or four battalions. The services, that's not their number one priority, cyber. Their number one priority is the ships and submarines, the planes and artillery and infantry and armor, not cyber. So as a result, it won't grow. So the reason you do it now is we're falling behind in the current system.

I'm not worried. Someone told me the other day, well, China's in our face right now. I'll just tell you gently, China's going to be in our face until China's no longer a threat to the United States. The idea that the cyber threat from China is going to somehow magically be negotiated away. We learned that in 2015 in the Rose Garden that that wasn't true when Xi told Obama he was going to back off. He just backed off while they reorganized for four months and then came back. And the final thing I hear is, why right now, is I do think Space Command has a lot of good... Excuse me, the setting up of Space Force has a lot of very good lessons for the United States Cyber Force. One is you don't do it at the end of the administration. You don't get delayed and take your time because you don't want to hand this problem over half cooked. You want to get it fully cooked in one administration, get it done. It doesn't matter which party is in power.

This has nothing to do with politics, it has to do with consistency and focus. So you do this right now in the first year of the administration and you get it done over three or four years. You wouldn't have nagging issues like the Space Guard hanging over things or the location of Space Command, which was related to that whole issue that's played out now for almost six years. Attack it in the beginning of the administration, get it done, get your focus on it, and then assess it, iterate it, assess it, iterate it, assess it, iterate it, and eventually have a great Cyber Force at the end of that.

LONERGAN: Yeah, I mean I don't have too much more to add to those excellent remarks. I would just say that when we think from a military innovation perspective, and just to put my academic hat on for a brief moment, what the military innovation literature tells us is that it often takes defeat in war for military organizations to change because bureaucracies are resistant to change and change is hard and so on. I would argue that that's not optimal. And there is a consensus that the United States has a serious readiness challenge in cyberspace, whether or not you agree that the solution is a Cyber Force, right? So everyone agrees that there's a readiness deficit. Most experts agree that cyberspace will inevitably play a role in great power conflict in the future. We know all of these things to be true, and so the best time to carefully figure out how to design and build a service is before we reach that threshold, rather than, as I said earlier, during it or afterwards.

And I think the reason there's so much pushback is because we know the history tells that these kinds of changes are difficult when there isn't some obvious crisis or conflict. And cyber is sort of this kind of continuous competition, slow burn, which can make it difficult to generate the political capital needed to make significant change, but I do think there is an opportunity in this moment to really implement something that will be significant and carefully considered.

DOUGHERTY: Mark, that was a great question. Thank you. And you'll have an opportunity for a follow-up if you'd like to do so. First, we're going to go to David Jones and then we have a question in from Lauren Williams. But let's start with David. Over to you, David.

JONES: Hi. You can hear me okay?

DOUGHERTY: We can. Thank you.

JONES: Thank you. I'm trying to understand whether this is replacing technologies and capabilities that we already have or just kind of taking them all from disparate departments and putting them together or exactly what the role of this Cyber Force would be. Would it take the place of just the military side or would it protect critical infrastructure or would it incorporate NSA capabilities or things that CISA does? Can you put that in perspective for me?

MONTGOMERY: So at its core, it's about who provides the force generation for the cyber mission force and some other elements that Erica and I pick out in the paper and talk about. Let's just say about, and this is a rough number, and it'll move year over year. It starts out around, I would start it out around 12 to 16 to 18,000 people. Those are the people in the Army, Navy, Air Force and Marines and Space Force Guardians who are already doing the kind of on-net operator mission and some of the tool development. So you're taking people who already exist to do it. Now look, when you build these units together, you're going to get some efficiencies, it's going to allow you to have more units doing it, and with less repetition between the four services. You combine the training commands into one, the HR management into one, things like that. So you'll get some savings. I don't advertise savings. This is at best cost neutral. There should be savings, but that's not how the military works. Whenever you think there's going to be savings, you come out cost neutral.

But the idea is you do this. Now you're asking about new tasking. And first, let me finish that thought. This force generation supports the force deployment done by cyber command and the other combatant commands, PACOM, SPACECOM, EUCOM. You got it. What you're asking about is an interesting element to this, which is that, and we don't go into excruciating detail in the paper because our job was not to do that. There will be further papers that talk about what does a Guard and Reserve look like? We allude to it in the paper. But long-term, when you hear people say, "I want to be more offense on the defense," And you look around what can do it, you can't use active forces that often, you can never use the intel forces, you can't really use law enforcement. How do we defend... And CISA, there's not much there there in CISA. So you think about how you defend your domestic critical infrastructure networks. What comes to mind to me is the National Guard.

And if you want to make the National Guard really effective in cyberspace, have a Cyber Guard because a Cyber Guard, and we haven't talked about it yet, and we might in a future question, a Cyber Guard's personnel makeup is not going to... I mean, a Cyber Force's personnel makeup is not going to be like current military services. When you go into an army battalion right now, it's about 98% uniformed people and about 2% civilian, usually contractors doing things. On a Navy ship, there'll be two or three contractors out of 300. Very small numbers. But when you go into a cyber mission team now, I think it's about 80/20 uniform, civilian. I think long-term, if I had a cyber service, I'd make it 50/50 military and civilian, with the civilians having very specific skills. They don't have to go through military development, leadership development, all those kinds of things at the same way that the military demands it, the military people still need to do that, but then these military [people] and civilians can move as they leave the cyber service to join the Guard or a Reserve and be important elements of a domestic response capacity that we don't have.

The National Guard has a lot of missions, and just like a service, the cyber one does not get prioritized. There are cyber people and non-cyber jobs in the National Guard because there wasn't a cyber billet available for them. So what I'd like to do is, personally, as I did this, I'd stand up a Cyber Guard, pull it from the Air Force and Army units, Air Guard and Army National Guard that are currently doing it, and then make it, again, civilian-military balanced, and then I'd have a Reserve, both the military Reserve and a civilian Reserve, that operates alongside it. To me, that's the only way to get it... What your question was is about how do you increase domestic support with this would be with that Guard and Reserve component. I still think your cyber mission teams that are at Cyber Command and the CoComs are generally overseas. They may be disrupting things that are coming to the United States, but they're disrupting them overseas. They're not sitting on US domestic networks. There's a title 10, title 38 issue there that comes very sticky every time you do that.

DOUGHERTY: Following question is from Lauren Williams, and it's related to that, Mark and Erica, so you may be able to flesh that out even more. Lauren asks, "How would the Reserve and Guard components fold into the Cyber Force, especially as different states have different levels of capabilities? Also, how would their cybersecurity missions with state and international governments fit in?

MONTGOMERY: I'll keep going on it, is that okay, Erica? And then I'll pass it to you. I'm excited about this issue. Erica's excited about all the boring stuff. I'm excited about the Guard, I guess. So the Guard is, look, I kind mentioned there, the Guard's going to be really important in my mind. The Guard is your way to get onto our domestic networks. Previous National Security advisor, Mike Waltz, said, "We need to be more offensive in the defense." You've heard President Trump avert to being more offensive. Well, the way you do that is not going to be your intelligence community, your NSA or CIA. It's not going to be active duty military. I say that there's an unusual use of active duty military these days, but it's not going to be active duty military. To me, the most likely people doing this are going to be the National Guard.

And yes, you're right, we have to reorganize the Guard. When you bring them together, the Air Force and Army Guards operate their cyber forces in different manners, so I would have one... Obviously when you create a Cyber Guard, you get one consistent operational manner. I'd probably set it up regionally to make sure you had a critical mass for those states that don't have a lot of cyber operators naturally in their Guard, but I'd set it up regionally, but you want to be in the location. You want to have the relationships with the electrical power companies, the water companies, the banks, everyone that's in that area, in that region, in the Guard unit that's supporting that region. There's a real advantage to that, so I think that would be useful.

Whether I use these in state partner programs overseas, I'm not sure. First, I'd want to get the Guard right domestically, the Cyber Guard right domestically, and then again, I put alongside it in the Reserves. The fantastic idea here is a Cyber Reserve that's mostly military traditional, where you leave and you're in the Reserves and you can come back and help and we can bring you back for a year or two years of activation, but also the civilians. And in both cases, they're going into the private sector working, getting smarter, maintaining their clearances, but coming back to the military, to the cyber service and then being farmed out to the different commands to share that information that we're learning within the private sector. It's going to be a lot easier with a Cyber Reserve and a Cyber Guard aligned to a cyber service.

It's not working. What I just described does not work well currently with the Army and the Army Guard and the Army Reserves, and you can have this kind of performative art where four very senior software people become lieutenant colonels in the Guard like we had the administration do two months ago. To me, that does not make individual cyber units more effective. That might help in advice on procurement to the Secretary of the Army, but I don't believe it gets at this core issue we have of not being in a position to provide support to the defense of our national critical infrastructure.

LONERGAN: Just really, really quick, to add to that because I know that the Guard and Reserve is one of Mark's passionate topics, in considering how to build a Cyber Guard and a Cyber Reserve, I think in terms of principles and design principles and values that we outline in the paper, really reducing the administrative burden to enabling those, facilitating those on-ramps and off-ramps, thinking about more non-traditional models will be essential to making sure that actually instantiating these concepts will be effective so that we can capitalize on the tremendous talent that resides across the nation, especially in our critical infrastructure sector. So there are lots of hurdles and impediments right now, especially in the Reserve component, and for the Cyber Reserve, we need to figure out how to make those less onerous.

DOUGHERTY: Thank you. Mark, a question that popped into my head as you were talking. You have met with high level officials in both Ukraine and Taiwan on defense issues including cyber. Have those discussions influenced how this report came out and what your thinking is on this?

MONTGOMERY: Both those countries may or may not run offensive cyber operations teams that would be aligned with this, so I haven't really thought about it from the offensive point of view, but in terms of defending your critical infrastructure, you bet. In both cases, they're under serious attack, Taiwan from China on a daily basis that is not enhanced by kinetic operations, and then Ukraine from Russia on a daily basis that is enhanced by kinetic operations. In both cases, the aggressiveness, the capability and capacity of the defending forces, the government's role in national critical infrastructure defense is much greater than originally postulated.

So whatever we think our role is right now, when we get into a crisis or combat, we're going to be expecting so much more from our governmental capacity, which is largely in the intelligence community in the military. And when it comes to defending our critical infrastructures, we just have some stringent laws about Title 50, which is intelligence forces, being allowed to be on our domestic networks. There's just very severe restrictions on that, not impossible, but very hard to get to. So then it becomes Title 50 forces, and so in my mind, getting more effective Title 50 forces that could then become part of the Guard and the Reserve, and if necessary, used, I thought it would become... I thought to my mind, that's why I was pushing so hard on the Guard and Reserve element of this.

But look, I want to get back to our fourth generation capacity. The current system is going to keep us tied down around 6,600 on net operators, and by the way, 6,600 is the authorized number. They have slightly less butts in seats, people in the billets, and even less people properly qualified for their jobs they're in. When Eric and I wrote that original report a year and a half ago, we had anecdotal reporting, which is anecdotal but true, that services were moving talented people around between cyber mission teams in order to get the team certified, in other to get certified with Jim and Jane who are both wicked good on net operators, and then they'd move Jim and Jane to the next unit that was being assessed.

That stopped, but it was wholly inappropriate but driven by desire to drive up perceived readiness levels because of all the criticism that was going on. I don't believe we've solved the core problem of generating forces properly.

DOUGHERTY: Erica?

LONERGAN: Yeah, so just I guess some concluding thoughts here. I think really getting the organizational leadership and culture right is imperative, and one of the challenges in building a new service is that you don't want early choices to lock you in to suboptimal outcomes, and so that's why we articulated this vision and these design principles, so that even as a particular force structure may change or certain concepts may change, the reference point should always be those design principles that we articulate in the paper around quality of personnel, organizational leadership and culture, taking an iterative and adaptive approach, really focusing on expertise, thinking about a force structure that is more... smaller elements that are more specialized and adaptable.

On the one hand, we think it's an imperative to create this service and to do it now, but just creating it is not enough. We also need to be really careful about how we do that and how we set the conditions now so that the service can be deliberately built over time, so that we really are solving this readiness problem that we all agree we face.

DOUGHERTY: Excellent. Mark and Erica, I'm going to give each of you 30 seconds to summarize your thoughts as we wrap up the call here. I just want to give a friendly reminder that you can reach the media shop here at FDD at press@fdd.org. If you'd like to arrange a conversation with either Mark or Erica or both, happy to do that. Also, a reminder at fdd.org, you will find all of our research, including the research of this report tomorrow. I will be sending you the link to the report. The embargo lifts at 6 AM. Again, if you'd like to chat with either one of them ahead of time, we can happily do that. Again, reach me at press@fdd.org.

To wrap things up, let's go first to Erica, then we'll wrap up with Mark.

LONERGAN: Great, yeah. So those are some of my wrap up thoughts but let me add a few additional ones. I think that defining the cut lines will be essential because cybersecurity touches so many aspects of the DOD enterprise, so how we carefully scope what's within the remit of the service and what's beyond it will be essential so that the cyber force isn't biting off more than it can chew and can really be effective in what those three core missions are, which are general organizing, training and equipping for cyber defense, cyber offense, and cyber intelligence.

And then I guess I'll really just come back to the quality of the personnel. We need to figure out a way to recruit and retain the right people. It is true that our principal adversary, being China, has an advantage in scale and quantity, and that does provide a quality all its own, but America's comparative advantage I think is in quality and in our innovation edge, our technical edge and the quality of our personnel, so how do we maximize that and really make sure we get that right? So for me, it all comes down to people.

MONTGOMERY: All right, thanks. Joe, I'll go. So look, first, this report's about the how, we described the why 15 months ago, and this is how you do it. Things are not getting better. It's time to take action. I love how Erica said that it's iterative, plan it, execute it, assess it, adjust it, replan it, re-execute it, assess it, adjust it. That's okay. That's how every service works. We haven't had a 400-ship Navy every year for the last 200 years. It changes, things change, so iterate it.

The final thing I want to say is people sometimes say, "Hey, Mark and Erica, if you do this, isn't cyber going to fall apart during the transition?" I'll just say gently, we established a Space Force and I'm not aware of any satellites colliding with each other, things spiraling out of control. If you do this correctly, if you have allowed one administration, one set of leaders to execute it over a couple of cycles of plan, assess, iterate, plan, assess, iterate, you'll be in great shape. If you wait and squeeze your hands and suck on your teeth, yes, things will get worse, and if you do it with one year to go in the administration, it will be a crazier execution. So my best military advice is do this and do this now.

DOUGHERTY: Erica, Mark, thank you very much for your expertise today. Krystal, thank you for your great work in the background and thank you to each of the reporters on today's call. This does conclude today's call.

LONERGAN: Thanks, everyone.