FDD EVENTS

Exploring The Potential of A U.S. Cyber Force

March 25, 2024

Featuring Rep. Mike Gallagher (R-WI), Dr. Erica Lonergan, and RADM (Ret.) Mark Montgomery
Introductory remarks by Bradley Bowman

BOWMAN: Welcome and thank you for joining us for this important virtual conversation hosted by the Foundation for Defense of Democracies. I'm Bradley Bowman, the senior director of FDD's Center on Military and Political Power.

The United States boasts the most capable cyber forces in the world. U.S. Cyber Command and the professionals there are doing incredible work to secure our country. Our men and women in uniform have defended our homeland and military forces. Our cyber professionals have helped our allies and partners uncover and defeat cyber threats and their networks, including in Ukraine. They have helped other partners respond to and recover from attacks by Iran, and they have defended U.S. elections against Russian attack.

The problem is that our cyber – the cyber threats to our country may be outpacing the growth in our nation's cyber capabilities. As a result, the margin of safety for Americans may be narrowing. So what's to be done?

Our panelists today have an answer in a new FDD monograph titled "United States Cyber Force: A Defense Imperative". They argue that the United States should create a new, independent armed service, a U.S. Cyber Force, alongside the Army, Navy, Air Force, Marine Corps, and Space Force. They argue that the status quo creates a, quote, "inefficient division of labor between the Army, Navy, Air Force, and Marine Corps and prevents the generation of a Cyber Force ready to carry out its mission," end quote.

This report draws on the expertise of the authors and more than 75 interviews with U.S. military officers, both active duty and retired, with significant leadership and command experience in the cyber domain. The authors address counterarguments and identify what a Cyber Force should look like.

So, who are the authors? They are Dr. Erica Lonergan and Rear Admiral (Ret.) Mark Montgomery, and they will be joined today by Congressman Mike Gallagher. Let me introduce each of them.

Congressman Gallagher has represented Wisconsin's 8th District in the U.S. House of Representatives since 2017 and served as co-chair of the congressionally mandated Cyber [Space] Solarium Commission [sic], or CSC. He continues to serve as co-chair of CSC 2.0, an initiative housed at FDD that works to implement Solarium recommendations.

In addition, Congressman Gallagher is the Chairman of the Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party and Chairman of the House Armed Services Subcommittee on Cyber Information Technologies and Innovation. He also sits on the permanent Select Committee on Intelligence. All committee positions that are very relevant to today's topic.

Congressman Gallagher and I are both recovering Senate staffers, and I'm proud to say that he was previously a national security fellow here at FDD.

Dr. Erica Lonergan is an assistant professor in the School of International and Public Affairs at Columbia University. She has an impressive experience in strategy and policy, having served as a lead writer of the 2023 U.S. Department of Defense Cyber Strategy and the congressionally mandated Department of Defense Cyber Posture Review. I have something in common with Dr. Lonergan as well. We both previously served as assistant professors in the Department of Social Sciences at West Point.

Last, but certainly not least, is my great FDD colleague and friend Rear Admiral (Ret.) Mark Montgomery. He serves as senior director of FDD's Center on Cyber and Technology Innovation and directs CSC 2.0 having previously served as an executive director there.

Previously, Mark served as policy director for the Senate Armed Services Committee, coordinating policy efforts on national security strategy, capabilities and requirements and cyber policy. He served for 32 years in the U.S. Navy, retiring as a rear admiral in 2017.

Before we dive into our discussion, a few words about FDD. For more than 20 years, FDD has operated as a fiercely independent nonpartisan research institute exclusively focused on national security of 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 on X, @FDD.

That's enough from me. Congressman Gallagher, over to you.

GALLAGHER: Well, thank you, Brad. Thank you to FDD for hosting this critical conversation today and for the work that your experts do every day. Your research and analysis and the solutions you articulate, informed by this research, are some of the best I've seen.

And the topic that brings us together today, as Brad outlined, is the readiness of our military forces to conduct cyber operations.

We ask a lot of our military cyber operators. These men and women in uniform secure operating networks and weapon systems. They support functional and geographic commands. They conduct reconnaissance and operational preparation of the environment, and they hold our adversaries at risk, and they can even assist the private sector with their interaction with the defense industrial base. A variety of critical tasks.

I am most concerned – having studied this as co-chairman of the Cyberspace Solarium Commission, working extensively with Mark and Erica – I am most concerned about the chronic issue and force readiness that affects those efforts. The question is, is the tip of the spear in cyberspace as sharp as it needs to be? I'm concerned about the recruitment, training, and development of our cyber warriors.

I worry about insufficient intelligence support to cyberspace operations and the shortcomings and the acquisition of cyber capabilities, all of which continue to plague our ability to effectively conduct cyber operations.

But most of all, I'm concerned that these problems aren't new. For the past decade, my colleagues in Congress, both Republicans and Democrats, working together, have tried to address force design and readiness. We've passed dozens of pieces of legislation to try and fix the problem in the military cyber workforce acquisition and overall force readiness.

And yet, we are seemingly no better off because of it. So, I'm looking forward to talking with our Cyber Command leadership about these issues after this recess period is over. But in the meantime, I'm going to treat this discussion a little bit like a hearing, asking the experts to explain the topic in front of us.

And like a hearing, I expect our experts to keep their responses brief. Especially you, Admiral Montgomery. We know you're smart, but you're going to be time limited. Don't try and filibuster us. But while you don't have a light in front of you, I'll cut you off if you exceed your allotted time.

And additionally, the military is notorious for acronyms. But I will enforce another of one of my rules, which is that we will speak in language that the average American understands, not the Pentagon military jargon. We will not tolerate that.

So, first, Mark, at a high level, Brad provided us an explanation of the paper you have out this morning. Walk us through the problem in a bit more depth. What are we seeing on force generation for cyberspace?

And I realize that I'm getting dangerously close to jargon with the term “force generation.” So, first, please explain, what do we mean by force generation and force employment, and what does it mean in the cyber context in particular?

MONTGOMERY: Thanks, Representative Gallagher. Thanks for being here today, but also thanks for your leadership on cyber issues over the past five years in Congress, with me and Senator King.

So, first, I'll go on the force employment, force generation. Just you're right. You need to explain what those are because they're very distinct things.

And force employments, you know, it's how the joint force uses military forces to execute mission. This is normally done by combatant command. So, Indo-Pacific Command, European Command, Central Command are the three we kind of hear of a lot, but U.S. Cyber Command does that as well.

So, our force employment is done by U.S. Cyber Command. And I'll talk about that later on. But – you know – I could say right up front, that is not where we saw the problem. It's where the problem evidenced itself, not the causal factor.

Now, force generation, that's different. Force generation is how military services recruit, onboard, train, develop and retain forces. This paper is a criticism of the current system of force generation in cyber. The Army, the Navy, the Air Force, the Marine Corps, even Space Force. Now, that system's not working, and I'll start at the very first part of it, which is recruiting. We're recruiting the wrong people for cyber force.

The most – what we're getting is the most cyber relevant people the service happened to have recruited, the services which are struggling. We both heard from the Army and the Navy. The Army quantitatively had the biggest miss in recruiting last year, but as a percentage of the need, the Navy was even greater. They just tucked in under the Army and you don't hear much about it. Both services come up short.

They need to be recruiting aggressively, and what they're doing to recruit is the right thing. They're going for the kids that are physically fit, mentally able, and that means they're sitting outside the basketball locker rooms, the men's and women's soccer locker rooms, the football locker room. I get it. But if they're recruiting the right Space Force, excuse me, Cyber Force, they would be sitting outside the robotics lab, the e-gaming basement, hub, whatever it is, at the school.

And what we're having – what's happening now in the services are, we get the best, most cyber relevant person the service happened to have recruited. Unless, of course, that person's needed as a special operator, a nuclear operator in the Navy, or an AEGIS technician in the Navy. Then even though they have these great cyber skills, they're going to those other ones. That's where the money is. But also, that's where the service's greatest demand is.

We're also training differently, across different standards, at redundant training facilities for the Army, Navy, Air Force, Marines. And we're renumerating them differently. I mean, you'll see from the report. In the report interviews, there's two kids sitting next to each other. They're both E-5s. They both have six years of service, and they're both equally certified. And they're getting vastly different based pay renumeration based on bonuses, special duty assignment pay, and other things.

And then they're utilized in different ways. Some services use officers in some roles, other enlisted. It's different. This poor force generation is leading to poor readiness. And we lay that out in the story. One apocryphal story in there. We saw it from two different squadrons. So, I feel it's true. There are units that do, like, complex work with malware development, and less than 10% of the unit is doing 90% of the work because they're the only ones who are qualified to do it.

Can you imagine going to an F-22 squadron and having the CO (Commanding Officer) say, "hey, I know I got 25 pilots in here, but I just use two of them." I mean, that's just not an allowable thing. And the final thing I'd say is, this readiness challenge is generated by the force generation issue, is coming, just as FBI Director Wray testified to you, along with Director Easterly, Director Coker, and General Nakasone, that we have an adversary conducting an aggressive operation against us, Volt Typhoon, where they're working their offensive systems, their offensive operators are aggressively installing malware against us.

And we need to keep up. We're at the point now where we really having an effective force employment means you can't take the luxury in force generation. So, kind of the final thought I'd have is that, we can't grow our force if the force isn't even ready at the level it is now. In other words, if they can't meet the readiness for the force at – today, how could you possibly grow them? 15 teams, 20 teams?

And so, we're stuck kind of at our 2012 force levels. I know that's a long answer, but that's where it's at.

GALLAGHER: Just a quick follow up before we get to Erica. OK, so if I were to say to you, I get your point about recruiting the nerds, not the jocks. I can say that because I was a nerd, right? You would not have found me if you were waiting outside the football locker room, you would have found me in the library, not talking to women in high school. But there has to be a single standard, particularly as a Marine, right? We sort of rebel against this idea that you would have a separate pathway, even for someone with exceptional talent, to address that pushback because I get that a lot when we talk about this.

MONTGOMERY: So, my answer on this is, I'm not talking about they're not going to wear – the crazy uniform things has already been taken by Space Force. I don't think we have to worry there at Cyber Force, you know. But I don't think we have to worry about that. I think they're going to be recruited to Army – if we had our way – to the Army standards in terms of drug usage, ability to get a clearance, all those kind of things, that's not going to change. What I'm talking about is going for people that you probably don't even show up at the door if you haven't learned Python, if you haven't learned basic coding. That's the problem.

And look, the Marines can't afford to do that. The Marines can't say, hey, we're going to take, “recruiters, stop recruiting at 92% of your name and your last 8% needs to be going out and finding Python recruiters.” That's – to me the Cyber Force, having the standard of what you need is actually easier across a single force. And by the way then you get into a critical mass number wise you know, several thousand a year recruited in. That's probably executable.

GALLAGHER: Erica, we'd love you to comment on anything that that Mark said. But I think what's unique about this paper is that you have done such extensive interviews with active duty military officers. I'd be curious for you to summarize what the – what was the feedback you got from that interview process and how did it weave its way into the report?

LONERGAN: Yes. Thanks, thanks, sir, for asking that question because I actually – I really do think that that's something that distinguishes this report from a lot of the other great writing and conversation that's been happening in Washington as you know, for many, many years now about the proper sort of organization of the military for cyberspace. You know, we – it was a priority for us to hear directly from those men and women who are out there in the cyber fight every day and to hear from them in their own words and to do our best job to capture kind of what their takeaways and reflections were from their own experiences.

And so that's why we make these interviews the center of our report and the driving force behind our recommendations. So as you noted you know, our findings are based on interviews from more than 75 active duty and also recently retired personnel. Together they have significant operational experience, command experience, in the cyber domain. And they're also – we really made a concerted effort to make sure those interviews were representative across the services.

So in the report we have a breakdown of some of the more specifics but it's about 30% from the Army, from the Navy, and from the Air Force, respectively. And then the remainder you know, you know, proportion to the size of those services are from the Marine Corps and the Space Force, and then a handful of senior civilians.

And I think it's also important to emphasize that the interviews are representative across rank and grade as well, and in all the way from E-7. So to avoid your military jargon, and equivalent to a Sergeant First Class in the Army, all the way up to One Star General Officer. And so it's not just diversity across the services but also across rank and grade.

But I think it's important to emphasize that the preponderance of those interviews did come from field-grade and above officers which means as you know, that they're coming in with more than you know, a decade-plus of significant military experience. So these are people who have been steeped in cyber careers and they can really speak to those experiences in those interviews.

So with that said, let me sort of briefly highlight some of the key findings. First, I just want to emphasize that we found overwhelmingly that these individuals are passionate about and dedicated to mission. Not surprisingly, they all care deeply and express their concern about the future of U.S. military cyber readiness.

And I think it's also important to underscore that these interviews were not – they were not about people's personal gripes, right, so these weren't complaints about their time in service. They really reflected their deliberate and considered conclusions about the lessons that they drew from their own professional experience.

And the consensus was nearly universal. And I would say it was overwhelming in that everyone who was interviewed agreed that the status quo is not sustainable. And everyone expressed serious concerns in different ways about the current state of readiness.

And I would also add that the vast majority of the interviewees attributed that lack of – that lack of readiness to the very challenges that Mark was just talking about a few minutes ago which is the fact that responsibilities for force generation in cyberspace are fractured across all of the various services, who in turn understandably don't necessarily always prioritize organizing, training, and equipping personnel for cyberspace because the services have their own significant big missions needs and priorities and so cyber doesn't easily fit within that for any of the services.

And so while not everyone we interviewed necessarily agreed that the solution is to establish an independent uniform cyber service, everyone agreed that the status quo is not tenable, that it's not working, and something has to change.

And so just by way of example obviously we don't have the time here to share all of the quotations and reflections from the interviews, but I just wanted to highlight one quote from the – a general officer who was interviewed. And I'll keep the specific service anonymous to protect their contribution. But this person writes, quote, "Our strategy of relying on the existing services to build the cyber expertise and capabilities required is inefficient, ineffective, unlikely to succeed despite years of investment and the best efforts of our service and service members Without a doubt the only viable path forward for USCYBERCOM is to establish a new service focused on organizing training and equipping forces required to fight and win in cyberspace."

So I think that really sort of brings home the general point. And I think it's representative of the 75-plus individuals who contributed their perspective to this report.

GALLAGHER: So let's stay on that because this is the heart of it, right, and this is what ...

LONERGAN: Yes.

GALLAGHER: ... the headlines are going to be. And this is what the debate should be about. It's your recommended, the creation of a new military service for cyberspace, a Cyber Force if you will.

I will confess at the start of this debate I came in skeptical, right because as Mark had alluded we've just created Space Force. We don't need more different uniforms. The risk is you create more bureaucracy, and it isn't an efficiency over time. But you both have now written something so powerful that it's challenging my priors. And I agree with what you said that the status quo is unacceptable.

So just – status quo is not acceptable but talk us through what would it – for those who are a little nervous about creating another thing, so soon after we did Space Force, what would this look like, and how would it – how would it be an efficiency over time?

LONERGAN: Yes. Great. So let me jump in on that. And then Mark, I'm sure you'll have some thoughts to add to after my comments but I think it's – it's important to emphasize what we were – what we were trying, to the core sort of proposition of this report was to articulate sort of the problem with the status quo and provide a justification for why we think a Cyber Force is the best and most appropriate solution to the problem.

We do offer our sort of notional ideas of what a Cyber Force could and should look like. But I do think that – and I think Mark would agree with me here that there should be a more complete independent study of this question, right. We were relying on you know, a significant number of interviews and our own expertise and backgrounds to make these recommendations but an independent study that has the appropriate remit and access to really deeply examine this issue and offer some recommendations based on that I think would be essential.

So with that said you know, and we talk about this more in the Report but our basic proposition is that you don't need a huge service, right, for the Cyber Force. You know, we propose that it would comprise about 10,000 personnel. And if you compare that to the Space Force, which was you know, as we know just recently created, that's just – I think the Space Force is slated to grow to about 15,000 or so personnel this year.

MONTGOMERY: Space Force is 16, 17 thousand …

LONERGAN: Yes.

MONTGOMERY: ... and I think we'll grow to about 25 over time.

LONERGAN: Yes. So I think – so one kind of thing to emphasize is that when it comes to cyberspace quality is more important than quantity. That's something that came out of our interviews, that a single operator can have effects that are really disproportionate to their size, right, being just one person. And you know, the nature of operating in through cyberspace means that having a small and agile but highly technically skilled and proficient force is really the goal. So that's sort of the number that we propose. So not some big giant bureaucracy.

We also envision that sort of the initial builds for the Cyber Force would comprise those billets that are currently in the Cyber Mission Force which right now is about 6,200 personnel. The CMF, of course, is slated to grow so it would be 6,200-plus as well as some additional billets for supporting staff administrative roles and so on.

And I think it's important to underscore that this wouldn't require a complex or burdensome shifting of personnel. And to your point about efficiencies this would reduce the redundancies and the duplication that already exists across all of the services because everyone, every single service, is you know, organizing, training, and equipping to their own service needs and requirements. And so you have duplication that exists that would be in theory – in theory gotten rid of.

And so when we think about – so a question that we consider was, OK, what would be the primary role and responsibility of the Cyber Force in this vision? It would be responsible for organizing, training, and equipping personnel for offensive cyber operations, defensive cyber operations, and then of course you know, the portion of the DOD Information Network that would – that the prospective Cyber Force would own and operate, and then their own IT infrastructure.

That means that the existing services would still have some responsibilities in cyberspace. Those wouldn't all go away. They would retain responsibility for organizing, training, and equipping personnel for those defensive cyber operations that are specifically linked to their domain-specific warfighting competencies, and also those portions of the Department of Defense Information Network that existing services own and operate, their IT infrastructure and so on. So it wouldn't be sort of a wholesale gutting of existing cybersecurity responsibilities from across the services.

And then a final note is that we do propose that a Cyber Force should be initially stood up within the Department of the Army, similar to how the Space Force is within the Department of the Air Force; the Marine Corps is within the Department of the Navy.

You know, that said, I think it's important to emphasize that it will be critical for a new Cyber Force to have the autonomy and the space to develop a distinct service culture, one that reflects all of the things we've been talking about, the unique nature and requirements of operating in cyberspace.

And so this will need to be deliberate especially for the Cyber Force because unlike the Space Force, for example, which essentially was created whole cloth out of personnel from the Air Force, a Cyber Force would be drawing in personnel from across all of the existing services. And so really being able to cultivate that unique cohesive and integrated cyber service culture will be essential.

So – but let me turn it over to Mark, if there's anything I missed on that.

MONTGOMERY: Yes. I agree that you know, Space Force is about 90%, Air Force 88% but effectively the Air Force – this other one would be 30/30/30/5/5 kind of thing.

You know, the other couple of thoughts I had, one was you know, the – you can't just take all the cyber responsibilities away. There's you know, between 150 and 200,000 people doing IT kind of – IT administration, cyber management, in the services. We're not talking about touching all that. We're talking about the CMF which is historically been about 6,200 – by the way not changed much in size over 12 years while the Chinese and Russians have changed – the threats changed quite a bit.

Some training commands on the offensive side particularly in some elements of the defense and the recruitment, things like that, you're going to need about 10,000. If I had my guess, it would grow and settle about 17.

By the way, the only way this is going to grow and settle is to have a unique Cyber Force. We've noticed over the last 12 years, trying to grow it by going to services and saying, could you man one less destroyer or one less F-35 squadron, or one less battalion, and give us the troops? They're not going to do that. And I understand, the services feel they slap the table a decade ago on a commitment and they're there.

And the only way you're going to raise this is a Cyber Force commander, joined at the hip with a Cyber Command commander, going to the Secretary of Defense or the Chairman and getting it.

And one other thing I want to mention that's kind of funny is the – yeah, everyone is like, oh, there's a SOCOM [United States Special Operations Command] model out there. We can do that. You know, SOCOM does this. And this isn't SOCOM, you know, I get it. If I'm sitting on a submarine as a captain and I'm told, blow up a train trestle 50 miles, you know, ashore – you know, swim 50 miles ashore, blow up a train trestle, I’m not looking for, like, the Air Force special ops pilot. I’m looking for a Navy SEAL, right? And he goes off and he gets a James Bond thing, he goes and does it.

In cyber, it’s different. You say, take out that train trestle. It could be an Air Force cyber operator, Navy, Marine Corps, it doesn’t – it really doesn’t matter. The SOCOM model is not near as appropriate here as it is in SOCOM. And so I think, you know, we need to take that, you know, I’m afraid we’re kind of barreling along towards that solution, and I think that it’s not applicable, and it's another 5 to 10 years finding out it's not applicable when the Chinese and Russians aren't waiting.

GALLAGHER: And if you need someone to write a book about that operation, definitely call it the Navy SEALs. Just kidding, Dan Crenshaw, I'm just kidding. OK. So you've talked – you've explained the broad contours of what a Cyber Force would look like. Does this mean that Cyber Command is not doing its job?

MONTGOMERY: Not at all. In fact, it's the reverse. And you in the last four years have kind of indicated that with the legislation that you and Mike Rounds, and Joe Manchin, and Jim Langevin, and then now Ro Khanna have passed, you know, in the –- in this HASC [House Armed Services Committee] cyber committee. And SASC [Senate Armed Services Committee] cyber committee said. I mean, the Cyber Command is doing, you know, doing a good job with what it's given. Our argument is they're not given the right force generate, you know, they're not given the right forces to, you know, to generate the force you need to employ.

In fact, I would say, you know, you can go back to General Alexander, Admiral Rogers, General Nakasone, particularly in his extended tour, and General Haugh, we've had the right people that we've had the people to do – we have good leaders there and good things. In fact, we're almost making a mistake. The last couple of years in the HASC and the SASC, we've put forward – we've transferred – and really, because Cyber Command whispered in our ear and asked us to do it. They told us, the services aren't building the acquisition. The tools you need, you know, the cyber infrastructure and tools you need, they weren't doing good enough a job to get Cyber Command operating, you know, up and running properly.

So they came and whispered in ears and said, we need acquisition authority. We've actually transferred what should be naturally service-retained acquisition authorities to Cyber Command. And I worry a little bit. It was the right thing to do given the abject failure we were at. But now, we've lost that kind of civilian oversight you expect. In fact, one of the reasons I would argue for a Cyber Force is so that it can do the acquisition as well with the Department of the Army’s oversight. Except now, instead of being the Department of Army acquisition being twisted between an army budget, you're pulling things out of an Army budget.

You'll have a separate cyber budget for which you, you know, you'll decide how much goes to acquisition, how much goes to personnel growth, how much does the budget need to grow independently. And it won't matter how many battalions you have or air defense requirements or submarine acquisition. This will be a decision done in a uniquely cyber environment.

So I actually think Cyber Command has done the best job it could have possibly done dealt the cards it had. But if it's going to do the job we expect it to do, you know, three years, five years, 10 years from now, we need a new model. In my mind, that new model is this kind of independent Cyber Force.

GALLAGHER: Erica, any additional thoughts on that Cyber Command question?

LONERGAN: No. I mean, I would just echo Mark's comments that, you know, what really came across from our interviews was that the problem lies with how the services prioritize their needs and where cyber falls along that prioritization. Again, I – and so I guess I would just echo that the challenge lies with the fourth generation model existing across the services, but we also understand why the Army may not prioritize organizing, training, and equipping personnel for cyberspace, and the Navy and the Air Force and so on, right, because those the unique sort of requirements of operating in and through the cyber domain may not sort of maybe mismatched with and not aligned with the priorities of the existing services. And so I would just add that it makes sense given the way the structure currently is that we have these problems, right? And so then the question becomes, what's the right path forward to fix them? And, you know, and we obviously think that it's creating an independent Cyber Force.

But, you know, I agree that from what we know about how Cyber Command has matured and grown, you know, in the years, in the, you know, decade, almost 15 years since its establishment, it's been doing, you know, phenomenally well with the structure that currently exists. But the question is, is that – are we content with leaving – content with things as they are, knowing how the threats are continuing to evolve in cyberspace.?

I mean, you look at, you know, Volt Typhoon, for example you know, knowing how our adversaries are thinking about employing force in and through cyberspace, not just in the gray zone sort of below the level of warfare, but also as part of, you know, the reality of modern high end conventional conflict. Cyber will be a part of that fight. We all know it. Our adversaries know it. And so are we optimally organized, you know, on our side of the house to succeed in that fight.

GALLAGHER: So obviously, not everyone agrees with you two about the need for a new military service. Your paper actually addresses some of those other proposals. I think it's another strength of the paper. You go in depth into the counter proposals. So that includes moving further towards the SOCOM model that Mark talked about or just tasking Cyber Command with force generation.

Erica, walk me through these other proposals and where you think they fall short.

LONERGAN: Yeah. So Mark sort of, you know, touched on the SOCOM model issue. But let me get into that a little bit and then I'll talk about the idea of sort of just tasking Cyber Command with force generation responsibilities outright. You know, special operations command is a force employer, but it is unique compared to other combatant commands in that it does have some service like authorities when it comes, especially when it comes to acquisitions. And a lot of experts have drawn explicit links between the Cyber Command model and the Special Operations Command model, and have advocated for making CYBERCOM look more and more like SOCOM.

And there have been, you know, recent efforts over the years to grant Cyber Command, as Mark mentioned, greater purview over acquisitions because of challenges with the acquisitions models across the services. I think most – great recent example of this is the 2022 National Defense Authorization Act where Congress granted Cyber Command enhanced budgetary control, which essentially, you know, would allow Cyber Command to control resources for equipping the Cyber Mission Force rather than have the services control the resources.

And so that's just the latest example of what has been an incremental, you know, increasingly greater and greater service like responsibilities for acquisitions that have been granted to Cyber Command. And so this is bringing Cyber Command more in line with the SOCOM model. But, you know, from our perspective, the comparison between cyberspace and special operations falls short in a critical way. And Mark alluded to this already in his reflections.

In a SOCOM model, each of the services is still providing the personnel to SOCOM to be employed. And those individuals are all trained in their unique domain specific warfighting competencies. So Mark gave the example of, you know, what we would want a Navy SEAL to be doing, given their sort of unique competencies in the same vein, you know, an Army Ranger, for instance, is trained specifically for special operations on the land domain. And there's no other service that can provide that particular training and skill set.

But cyberspace isn't like that. To Mark's point, there are no domain specific functions that only a particular service is able to provide. And so this is a critical flaw, I think, and that weakens the case for, you know, the comparison between the SOCOM model and the CYBERCOM model.

And the other sort of I think major proposal that's an alternative to establishing an independent uniform service is to simply, you know, give Cyber Commands force generation authorities. The problem with that is that that's basically creating all but a service in name, right? And I think that's equally, if not more problematic than the SOCOM model.

For one, and, you know, Mark mentioned this, you know, this runs counter to you the Goldwater-Nichols Act, right, and how we think about roles and responsibilities for the services to do forced generation and the combatant commands to do forced employment. I think it raises some serious concerns about the burden that that would place on the commander of U.S. Cyber Command, who is currently dual-hatted as the director of the National Security Agency.

This would essentially add yet another hat to that role. And it would give that commander less time to focus on their, you know, key core missions and priorities of being director of the NSA and the primary force employer for the US military in and through cyberspace. And in fact, the arguments that – some of the arguments that have been made in various circles against continuing the dual-hat structure is precisely that even just being, you know, commander – I wouldn't say just, right, these are two significant responsibilities being commander of Cyber Command and the director of the NSA – is too much for one person.

And so if we add another hat on top of that, I think that not only adds a significant burden, but also reenergizes the case for splitting the dual-hat, which I personally, you know, my position would be against that.

And then finally, Mark made this point getting back to Goldwater Nichols about civilian oversight. Creating a Cyber Force is the mechanism, is what – the way that we've established and organized our military and the relationship between civilian leaders and uniformed military personnel is through having a service that is accountable to obviously, of course, to Congress, but also to a civilian secretary.

And if you simply, you know, provide the commander of U.S. Cyber Command with, you know, the full scope of responsibilities and authorities for force generation you don't have a comparable mechanism for civilian oversight. And I do think that's problematic in terms of how we traditionally think about civilian control. And so while I respect –certainly respect the experts and the arguments of those who are making alternative proposals. And it was important to us in this report to really take those into account in considering sort of viable paths forward. And also would note that everyone agrees – all of those alternatives reflect either implicitly or explicitly a recognition that the current state is not tenable and something has to change.

But I personally disagree with making incremental changes that don't get at the root of the problem, given the threat environment that we're in. And that also create unnecessary challenges and problems in their own right. So, you know, that's sort of our perspective on the alternatives. But, you know, looking forward to – to this debate continuing in the public sphere going forward.

GALLAGHER: Mark, any other thoughts on the alternative proposals that you wanted to offer?

MONTGOMERY: Yeah. One quick thing is, you know, we had General Dunford study the split – you know, the NSA/Cyber Command dual-hat arrangement, and he came back with, “hey, they’re – Cyber Command isn't ready.” And the reason they weren't ready were things that the force would generate for the services we're supposed to generate for them, which is the kind of the infrastructure and the tools to operate independently from NSA. And I respect General Dunford's feeling on that.

I think we ended up – I mean, this is an official, but I think we're probably in a five-year, you know, observe and report each year for the next five years, and then make another decision on this. And General Dunford was right. The services aren't doing what they need to be doing. And so I would want to get it like this.

You know, in the end, our report is not enough. Our report – you know, I think in the end, I'm passing it back to you as a sitting congressman, is that, you know, we need some kind of, you know, direction to the Department of Defense to do an independent report. You've asked them to do lots of reports on readiness and on the feasibility of the current model. And I would say gently that they have not treated those with the seriousness required and getting the data back to you that you as members need, you know?

And Chairman Rogers a few years ago made the very – you know, made an aggressive push, you know, a compelling argument for a Space Force. And I think almost every element he saw, plus additional ones, exist now in the Cyber Force. So I would hope, you know, because he had that kind of vision and creativity, you know, six – five, six years ago, General [Chairman, sic] Rogers, when he looks at this, will see the same – will recognize the same challenges facing us in the cyberspace domain and join on board, and getting some kind of independent study to look at this.

GALLAGHER: Well, as you look back not only in the process for this report but both of your experiences and working with the Cyberspace Solarium Commission, I mean, how do you – just put this in the context of – one thing that's clear in our final report for the Cyberspace Solarium Commission is that there are a lot of threats in cyber, but in my opinion, I'm biased as Chairman of the Select Committee on China, China is the pacing threat, right? Did you learn anything about how our adversaries approach their organization and how they develop their human talent? Because ultimately, it's all about the humans, right? Are our humans better than theirs? It's a bit of an oddball question, but Mark, maybe you can start with that.

MONTGOMERY: Yeah. I like how you asked that. So each of our adversaries is different, particularly Russia and China. The Chinese model is about a quantity, a number, you know, they're cranking through cyber development – office of cyber operators. It's really hard to pin down an exact number, but I would say somewhere in the 50,000 to 100,000 range as compared to our kind of, as we mentioned earlier, 6,200. Not all of which are even on mission all the time.

Now, our quality does have a value all its own. And so I don't say that they're 50,000 to 100,000 yet exceeds our offensive capability, but it's interesting. So that's one model. The Russian model is much different where they spin people off into, you know, between the intel – their intel and military, you know, it's very hard to see the difference. And their contractors, you know, Prigozhin, through Wagner, was running one of the largest, you know, cyber, you know, hacker kind of contract facilities, which included a good chunk of the world's ransomware as a service provision, right?

I mean – so I mean ...

GALLAGHER: So they should – they do like cyber letters of marque and reprisal thing?

MONTGOMERY: They do. They've got Decatur and Bainbridge out there looking for prizes, right, you know? So, you know, from my point of view, they each generate separately. I will say this. They are growing. You know, we see this one – and if you took at our closest partner who's good at this, the Israelis with Unit 8,200, they don't mess around with different services doing this, right?

GALLAGHER: Yeah, yeah.

MONTGOMERY: They got the Army doing this. They've got this down. And by the way, it feeds their whole GDP developing, you know, cybersecurity entrepreneurial thing. So I would say, you know, if we get the Cyber Force right, it's going to help the military, it's going to help the intelligence community who, by the way, poaches are very best operators frequently, particularly when we have these pain disparity issues going on that we see between the services. And it's going to help our private sector.

I mean, this could – if we get this right now – that's why Erica is right. Don't fiddle-fuddle around with interim like tweaks on the margin, see if we can get there. Get this fixed right, get going. The good news is we have the Cyber Mission Force right now in place. It will not fall apart as you rename it. You'll be fine. It'll be very clear. So from my point of view, we have a path forward on this. Our adversary – it's not our adversary's path, it's our path.

GALLAGHER: Erica, we're running out of time. Any other thoughts on that question of where we are versus our adversaries?

LONERGAN: Yeah. I mean, I agree with everything that Mark said. Thinking about China in particular, China made a series of significant reforms almost a decade ago in, you know, integrating its forces and creating the Strategic Support Forces. And, you know, not that we want to – you know, I would caution against, like, mirror imaging what our adversaries do. But obviously, it's important to take into account how they're not just thinking about strategy and doctrine, right, but how they're organizing their forces to fight in cyberspace.

And so clearly China recognized over a year ago that you need, you know, one integrated entity that's responsible for, you know, for developing forces in cyberspace. And I do think – I was going to mention the 8200 example, Mark, so I'm glad that you mentioned it. I think one thing that, you know, obviously that, you know, compares – comparing to our allies and partners also, you know, creates challenges because the U.S. is organized differently. A key difference between us and Israel, of course, is that we don't have universal conscription.

But I think something that 8200 prioritizes that is worth emphasizing here is the focus on quality over quantity and really just, you know, honing in on, you know, they have a rigorous process starting all the way in elementary school for identifying, you know, like, high, you know, the potential for, you know, high skill and technical competency and then really cultivating and refining that through service.

And so I think a prospective U.S. Cyber Force in the United States should similarly focus on that quality over quantity and that, you know, technical knowledge and training, which is – which can't be static, right? It has to be dynamic given the nature of the cyber domain.

MONTGOMERY: Hey, I don't want to piss the ACLU off and get them on us, Mike, so I just want to say right away, we're not for the 8200 model, except for the quality, but not the, like, checking out elementary school grades. And so...

LONERGAN: No, no, no, I was not suggesting.

GALLAGHER: It's like a – you know, like an Ender's Game model, you know?

(LAUGHTER)

MONTGOMERY: There we go, yeah.

GALLAGHER: Yeah. Well, thank you both. This is great. Your paper is a remarkable piece of work. I recommend it to all my colleagues. You have to read more than the executive summary, read the whole thing. And it seems to me we have a clear next step here, which is that Congress needs to have the Department of Defense commissioned an independent assessment of the force generation challenges to include some recommended ways forward. I think we need the Department to have an outside assessor replicate the study, but at an even deeper level.

They recently had a commitment to create a vision for Cyber Command 2.0, which is kind of a tacit recognition that the status quo in force generation is not working, but I worry that it might not be an honest, independent assessment of how we fix readiness. And I worry that – General Nakasone had a statement that all solutions are on the table except the status quo – that in fact the straightforward solution that Mark and Erica have laid out may not be on the table if DOD looks at this internally.

And what I admire about FDD is that you don't just sit around and, you know, admire the problem, but you actually put in the hard work to figure out solutions and put forward clear recommendations to take on our biggest national security challenges. So thank you for your research, your analysis. I'm disappointed that we didn't get the provision for a more fulsome study across the finish line in last year's NDAA, but I hope we can in this NDAA. And that brings us to the end of today's discussion.

I don't have my Chairman's gavel to adjourn this event in my usual way, but just want to say thank you to our speakers for shedding critical light on the shortcomings of the U.S. military cyber readiness and proposing a concrete solution.

Thank you all for tuning into this discussion. There's a lot more work to be done in securing our nation in cyberspace. And I look forward to getting it done. Thank you very much.

END