FDD Media Call: Findings of the Commission on Cyber Force Generation

June 1, 2026
Featuring RADM (Ret.) Mark Montgomery, LTG (Ret.) Edward Cardon, Joshua Stiefel and Lauryn Williams
Moderated by Joe Dougherty

DOUGHERTY: Good morning, and thank you for joining us for today's media call as experts walk you through the summary findings of the Commission on Cyber Force Generation, a joint 10-month effort from the Center for Strategic and International Studies and the Foundation for Defense of Democracies.

My name is Joe Dougherty. I'm Senior Director of Communications at FDD. Joining us this morning to walk through the commission's findings:

Lieutenant General (retired) Edward Cardon served as co-chair of the Commission on Cyber Force Generation. General Cardon, of course, as part of his distinguished 36-year U.S. Army service, served as former director of the US Army Office of Business Transformation and served as former head of the Army Cyber Command.

Joshua Stiefel also served as co-chair of the commission. He is currently vice president for government relations at Second Front, and served as former professional staff member for the House Armed Services Committee, where he was responsible for the oversight, legislation, and policy for DOD's cyber warfare, cybersecurity, and information technology activities.

Rear Admiral (retired) Mark Montgomery served 32 years in the U.S. Navy. He is an FDD senior fellow and senior director of FDD's Center on Cyber and Technology Innovation (CCTI), director of CSC 2.0, and is former director of the Cyberspace Solarium Commission (CSC).

Lauryn Williams is deputy director and senior fellow in CSIS' Strategic Technologies Program. Lauryn is former chief of staff to the assistant secretary of defense for industrial base policy, and former director for strategy in the White House Office of the National Cyber Director.

This conversation is on the record, and we will provide a video and transcript after the call.

Mark, we'll start with you: Prior to the launch of the commission, at FDD we published two monographs exploring the need for a Cyber Force. This commission purposely did not rehash the debate about the need for a Cyber Force but instead focused on vision, mission, and implementation plan. Before I ask Lauryn, Ed and Joshua to talk about the findings of the report, set the stage for us. How did we get there?

MONTGOMERY: I understand it's 12 years of force generation struggle and there've been a lot of legislative interventions. Josh [Stiefel] can get into that, but dozens to help. For the first three to six years, you can forgive things. It's a startup in the government. It's hard, and we're seeing that with Space Force. So as Cyber Command stood up and you're trying to figure out how does force generation get right, you can forgive things.

But the last six to 12 years, I would say that the performance of the services has been an obstruction to success. And that's a tough thing to say because services don't want to be an obstruction. They are services, they want to do the right thing. But our ability to recruit, train, maintain, and retain a cyber force has struggled. Our recruiting has never focused on... none of the services' recruiting efforts focus on, can you code Python?

And they focus on, can you do 75 pushups, 50 sit-ups and run a six-, seven-minute mile, depending on the service. And if there was a technical requirement, it's because the services need it for something else. So the Navy has a need for nuclear engineers. And I promise you, every kid who hits that ASVAB for a home run, the academic testing we do, the AQT, if they hit that for a home run, we immediately begin to bribe them into joining nuclear power.

So the recruiting's not right. The training's not right. We're not producing what are called masters. I incorrectly had said out loud for the last couple of years, we don't have enough people. Someone from NSA came in and said, "It's not that they don't have enough people. They're closer than you imply." But when they don't have enough people is when you look at the spread between apprentice, journeyman and master, we just don't have enough masters.

We don't have enough of the people with the right level of training, particularly Title X and Title 50 combined. And then in the maintain, our pay is crazy. Most sailors, soldiers, airman, Marines can live with their pay. What they can't live with is the guy next to them or the woman next to them from another service with the same credentials or less, making more money than them. And there's this vast inconsistency as we throw money at solving an individual retention problem in a service. We don't have any consistency there. And I know they're working on that, but services will buck that to save their own skin on their... Because this applies to broader than just your offensive cyber operators.

And then finally, retention. Look, NSA picks off the top people, I get that. The private sector takes a lot of people. But when Josh provided us with interviews of the scores of people, I'm sure he'll talk to that a little bit, money is not the driving factor. It's a factor. It's not the driving factor. It's a sense of frustration with how the government is organized. And you don't hear that too often in outgoing interviews. I never heard in the Navy, "I'm really frustrated with how surface warfare is handling this issue." Usually it was a specific leadership problem or a specific financial issue, things like that. That wasn't there.

So when Eric and I wrote these two reports in 2024 and 2025, we were trying to figure out why cyber force and how cyber force. I think this report you're going to see is a detailed explanation of how to do cyber force. And I think that's a necessary implement because at some point there's going to be a go order, and there's a lot of things that can drive that go order, a national crisis, a president getting motivated about it, Congress getting motivated about it, any series of things can do it.

And when that go order comes, we have to be better prepared than we were for Space Force. If you talk to Space Force veterans and we did, their feedback to us was, I think [first Chief of Space Operations of the US Space Force] General Raymond said, "I was Space Force employee number one and not for just a day, but for several weeks," while he tried to get things organized. And he had number two, and that was another couple. That's not how you start this up. You need to be ready to go.

And so this report is going to be an important part of that ligature of how you get ready to go and how you don't dork this up, because this is going to be hard and there will be antibodies to it from... even when the president says "do it," there'll be antibodies to how to do it. And so we've got to layout the best possible course. So I leave it to my three co-panelists here to really lay out the details of that. But Joe, that's the why this report is happening, front page.

DOUGHERTY: Thanks, Mark. Very much appreciated. Lauryn, let's move over to you. So, FDD was pleased to partner with CSIS in this terrific effort and it was quite an undertaking, of course. The report is born of in-depth discussions and debates. Can you walk us through the process in organizing assumptions of the commission?

WILLIAMS: Absolutely. Thanks, Joe, and thanks to the FDD team for hosting this conversation and for the group of reporters that we see online here. So, if FDD was glad to partner with us, we were absolutely grateful on the other side to build on the work that Mark just talked about that he and Dr. Erica Lonergan have been putting out into the world for years now as well as to partner specifically with the Cyber Solarium Commission 2.0 on this project.

So from the CSIS perspective and the joint management of this project, it really was, as you mentioned, Joe, a really extensive undertaking. So if, as Mark noted, the core premise was not to re-litigate some of the conversations that have already taken place over years, not to re-litigate the question of whether there should be a cyber force, which other commissions, other congressionally-mandated commissions are taking up, it was to really look at what should happen the day after a presidential decision or a legislative movement on this issue.

And so really what the report looks to do is to lay out an implementation plan, essentially, to hand over to decision makers, again, the day after, to be able to stand up a cyber force. So that's really the key starting assumption that we want to make clear is the premise for this report. Stepping back a little bit, this was a 10-month effort, let's call the commission a 10-month effort, obviously, years and years of work as I mentioned, that it built on.

A 10-month effort to bring together, I think, close to 20 incredibly experienced former military officials representing each one of the existing cyber component commands of the existing military services, as well as a range of operators whose experiences we drew from industry leaders who are driving the face of change in the cyber industry today. So you can head to the CSIS landing page for this commission and see a real breadth in depth of experience among the commissioners. And then of course, the co-chairs who we have online today, who were really driving, this morning, in that report.

And then from the CSIS perspective, Matt Pearl, our director, Taylar Rajic, our associate fellow, were driving from our side of things on the day-to-day. And the day-to-day really was a team effort. Over 10 months, the commission met for upwards of six hours to really deliberate through all of the issues that you see laid out in a really impressive amount of detail in the report. And so there were certain issues that the commission was able to drive to consensus on over those 10 months.

And then there were others that essentially were points of discussion that we also tried to faithfully lay out in the report, and maybe specifically not to jump into the conclusions before Josh and Ed dive into those, but specifically issues and questions such as where a cyber force should live, where it should be institutionally aligned within the Department of Defense, were issues that were extensively discussed among this incredible group of experts. And there were good reasons and good rationales for both sides of a conversation around where the cyber force should sit. So just one example of our attempt to faithfully lay out where there was consensus among this group and where there were questions that were raised.

And I think maybe lastly, I'll just note that what we really tried to do at a high level was to explicitly lay out the man, train and equip functions that a future cyber force would take on from the current array of cyber forces across the existing services. What would a consolidated cyber force be responsible for? What would its authorities be? And I think if there's nothing else that you take away from this report, it's how we thought systematically about what a cyber force would do and how it would take on those force generation capabilities from day one. So I think I'll stop there.

DOUGHERTY: Very good, Lauryn. Thank you for your leadership on the research here. We'll turn it now over to Ed and to Joshua as co-chairs of the commission. Gentlemen, thank you both for your leadership and terrific work on this effort. Ed, we're going to start with you after all the setup from Lauren and from Mark. What did the commission conclude? How should cyber force be stood up? How should it be implemented?

CARDON: Yeah, thanks, Joe. And maybe first start with thanks to CSIS and FDD for the support and all the commissioners for their time and thoughts and hard work that went into this. So normally the way the departments organize -- the services handle force generation and the combatant commands handle force employment. That's not really the way it's set up for cyber, meaning that each service is responsible for standing up forces to present to cyber command.

So instead of having one service, you have four services. But before we get into that part, it's what mission set are they responsible for? And the department normally defines the mission sets as offensive cyberspace operations. That seems very logical. Defensive cyberspace operations, that also seems very logical. Department of Defense or Department of War Information Networks or DODIN, as it's often called, that gets a little bit more problematic because service networks are often designed for that service.

And so, one of our conclusions is that it primarily covers offensive cyberspace and defensive cyberspace operations. That's the first piece. The second piece is on the people. And I already mentioned that each service which has a responsibility for its own domain is recruiting for another domain so it's not on the top. Admiral Gilday made this very clear as a former chief of Naval operations in the kickoff that recruiting cyberspace operators is important for the Navy, but not as number one priority. It's to create, as Mark said, the Naval force.

So if you have a [cyber force] service, now you can have a more common path. So for example, get the missions right as was already discussed, but now you could have a service that is made up of all commissioned officers. You could have a service that has different pay programs. It's very common inside the services that create the manning side in a way that's conducive to that service.

The second part is I just want to go back to what Lauryn was saying. So what's driving this, Lauryn and Mark both in the last six years, it's artificial intelligence and the growth of what's going on in the cyber world. And former CYBERCOM commanders who said the force we have today is not the force we need for the future, but how are we going to create a force for the future when we're still using the same principles we use for the force for today?

Now in fairness, Cybercom 2.0 took a big swing at this. A lot of hard work went into this. It's clearly a pathway that at the end, if you follow it to its logical conclusion, you have to ask yourself, should the CYBERCOM commander also be the cyber force generation, should also be the director of NSA? That would be three huge jobs on one person. And I'll stop there and let Josh talk a little bit about some of the others.

DOUGHERTY: Thank you, Ed, for that. Josh, Congress has been raising concerns about how the US military is organized to prevail in cyberspace and particularly the question of force generation, manning, training, and equipping for cyber operations. So what makes this moment different? Why do you think this commission's findings come at such a timely moment?

STIEFEL: So what's interesting is that as someone who was in the legislative process for almost seven years, we tried, I tried, my colleagues tried everything and it seems as if we've reached that breaking point where there isn't any more authority to give to address this problem that doesn't start to begin to chip away or take away from the service chiefs. And that dilemma means we're at this precipice. That's how I know we're at this precipice.

It's not like, well, we need to wait for some institutional maturation before we can allow cyber command to get this next authority that will then improve it. We've reached this breaking point. So for example, CYBERCOM and the commander has had the authority since 2017 to oversee the incentive pay and assignment cycles for personnel to the cyber mission force. They have been unable to exercise that because of a very important clause in that provision which says "in coordination with the military service chiefs."

And so unless you remove that, which then impedes the service chief's ability to organize, train, and equip as they are statutorily responsible for, there's no more authority you can give to the CYBERCOM commander.

And so that manifests itself in a host of different ways and it really speaks to Congress has tried to jam this square peg through a round hole and we just have to recognize it's proven out that this is a situation that we're not unfamiliar with. This mirrors very closely the issues that befell aviation when it fell to the Army to oversee that through the '20s and '30s before the establishment of the Air Force. It mirrors similarly how space was mismanaged by the Air Force in the 90s and early 2000s before the establishment of the Space Force. Except the difference here is, as my colleague said, you have four services trying to do this and four services manifesting these issues instead of just one in those historical antecedents.

MONTGOMERY: Hey, Joe, can I pick up on one thing there? I'm glad Josh mentioned that one of the biggest problems we have on the Hill is a congressman or senator will go, "But Mark, Cyber Command's doing such a good job." And first of all, whether we think that's true or not, we'll set it aside. This isn't about force employment, it's about force generation. And the biggest arguers against this are former Cyber Command commanders and deputies who I think take this as a jam on them. This is about the force generation to support them. This isn't about past performance by Cyber Command. It's about future performance by Cyber Command and other entities like the other COCOMs that might employ cyber force. And if we don't fix this force generation problem, we're not going to be able to keep up with the Joneses. And the Joneses is a euphemism for the Chinese MSS and their military services, who by most estimates have about 10 times as many offensive cyber operators as US cyber force employees.

That doesn't make them 10 times better. But over time, quantity will have a quality, and when they're fielding tools like Ed mentioned with AI, things like that that are going to make individual operators more effective, we're going to have a problem. So again, this is not about cyber force. It's not about Cyber Command. It's not about Cyber Command. It's not about Cyber Command. It's about the force generation to support Cyber Command. And we are not criticizing Cyber Command when we say that Cyber Command needs better force generation. There are criticisms of Cyber Command in the report, but it's not about the force generation since that's not their responsibility. It's the services. And we are critical of the services. And as Ed mentioned, the former service chiefs who I won't say get religion, but get a little bit of hindsight, look back and say, look, it's impossible to prioritize cyber as a top one, two, or three priority when I have undersea warfare, air warfare, power projection, sea control, all these other missions.

I'll promise you when a cyber force commander wakes up in the morning, his or her number one priority is going to be cyber, which you cannot say for any other force generator. And by the way, we've seen this in Space Force already where we're really getting better bang for our buck having created a space force. Sorry I intervened there, but Josh reminds me that we've been through this rodeo before.

DOUGHERTY: Lauryn, I saw you nodding your head there, Josh as well. Anything you'd like to add there to Mark's comments?

STIEFEL: I would just say our system has been well established. We've had a construct in place since 1986 with the Goldwater-Nichols reforms. Services organize, train and equip, and combatant commands operate. And the organizing principle of the US military is that we build military services aligned to war fighting domains. There are five domains and we have built services to cover four out of those five. I don't see how this domain is any less deserving of a service when it is where we literally have troops in contact with the adversary on a daily basis.

WILLIAMS: Sure. And not too much to add on top of, I'll just draw on a couple of points that Mark made and Ed, to Josh's as well, and to zoom out a little bit as has already been alluded to, which is the cyber threat landscape that we're having these conversations in. Which I think is an incredibly important backdrop to inform the need for prioritization of cyber forces, as Josh mentioned, to make sure that we are covering and adequately prioritizing the fifth designated war fighting domains. So all of that to say the developments that we continue to see in the headlines are related to the cyber threat from the PRC [People's Republic of China]. As Ed mentioned, the fast moving evolution of AI-enabled offensive and defensive cyber threats. We could go on and on, but all of those things really do speak to the need for more prioritization, cohesion when it comes to cyber forces within the Department of Defense.

CARDON: I think an important point here also is on capability development. So in November of 2025, Anthropic released the report on the Chinese using agentic AI for cyber operations. And of course, recently you have Mythos that was released. It's this idea of speed. So think about capability development and speed. Right now, a lot of the services still have capability development that's being consolidated now under Cyber Command to a degree, but it's all about speed. Can you imagine creating a... Well, let me back up. So some people point to SOCOM, Special Operations Command and say, look, they're very effective at this, but they have what's called Major Force Program 11 funds, which are for soft unique items. Imagine what you're going to need based on those two incidents I just reported for cyber. And so the whole capabilities development side, the partnerships they are going to have with industry, the partnerships they have with the labs, the train that they're going to need to do it themselves to have the speed that's needed, that's very different than most areas that we have today inside the Department of Defense.

As a former division commander, I'm given capabilities by the Army. Here, you might actually have to develop capabilities, which means you need an entire skillset of development. And then how do we manage that and then how do you keep them in? And this means you need a different pathway, which is like some of the big tech companies, you can rise up all the way up to the top as an engineer, but that's not the way the services are organized. We put a premier emphasis on leadership. Well, here premier emphasis might be on technical ability in certain areas. So it's the ability to have the flexibility to pull these levers for what's needed at the time to generate the force that Cyber Command needs.

DOUGHERTY: Thank you for that. I know a few reporters did join us a little bit late. Just a quick reminder that we are recording this conversation. It is on the record and we'll share the transcript and recording with you later today. In the meantime, just before we go over to the Q&A portion of the call, just a reminder, you can use the raised hand feature to ask your question or you can submit your question in the chat. I do have one final question I wanted to run by Josh before we move to the Q&A. Josh, again, the timing of the report is no coincidence. The House and Senate Armed Services are marking up the annual defense authorization bills this week. And next, what comes next from this report?

STIEFEL: So it'll be interesting to see what comes in the markup if this raises to the level of attention that it's debated. I'm excited to see what comes out of both chambers, but this is something where it feels like a conversation where the volume continues to rise. And so I think we're going to see that this issue is not going to go away because as impressive as what the department has put together with the intent and vision for Cyber Command 2.0, it still leaves some issues that will be unaddressed. One issue that we talk about in the report is a foundational intelligence center. That's a gap that is not addressed in 2.0, but something that the force and the commanders have said repeatedly over the years that they require.

And so I think that we're going to continue to be talking about this issue because the issues that are causing them to raise tensions are not going away and further reinforcing a lot of gaps that services deal with for themselves that we've never been able to create unique solutions to address in this domain. So I think we're facing an inevitability. I'd just rather we pull this trigger and do it sooner rather than later. It's typically better to prepare for war in advance of conflict rather than after the fact.

DOUGHERTY: Very good. Thank you, Josh. We do have some questions in the queue, so we will get that started. Let us begin with Mark Pomerleau. Mark, thank you for joining us this morning and over to you for your question.

MARK POMERLEAU: Hey, good morning. Can you hear me?

DOUGHERTY: We can, Mark. Thank you.

MARK POMERLEAU: Super. Thanks for doing this. Just I know that there's been some discussion about the roadmap that you guys have laid out and how a potential cyber force would look a lot different in terms of the makeup of a historical force like the Army or the Air Force. Is there anything or is there any light that you can shed on what some of those differences would look like and maybe how you guys are thinking about scoping what an actual separate service focused on cyber operations would look like?

CARDON: Mark, I think that... Go ahead. Go ahead.

MONTGOMERY: Yeah, no, go ahead, Ed. You go first and I'll go second.

CARDON: So Mark, first, if a cyber force is created, it has to have the ability to interface with the department and the other services and the combatant command. So that part has to look normal. We've already learned this lesson. In other words, every service has a 3, a G3, an N3, an A3. There will have to be a C3 in this case. So that's one part. But what that looks like underneath, that could be completely different. And I think that's much like the Army did when they created a branch. They could have a lot of different rules because now it can have its own setup.

And so underneath that, we divided it up much like we said in terms of for the big muscle movements, man, train and equip, but there's also this idea of cyber law. There's this idea of cyber intelligence. There's this idea that now these things could be created because you could mass all the expertise in one place and grow that and then have the right partnerships that are going to be necessary with both industry and academia. In this case, there's law firms like Venable working on this in a big way. I'll stop there, Mark, over to you.

MONTGOMERY: Thanks. Yeah. So thank you, Ed. And then Mark, I'll say I think there's a big difference in the civil... To get it exactly what Ed was talking about, there'll be a difference in the mix of civil and military personnel than say a traditional operational unit. If I wanted a Navy operational unit to ship a squadron, a sub, the civil-military mix within that operational unit would be 98 to 2. Air Force quadrants might be like 96 to 4. Army battalion might be 100 to 0. I mean, there's a handful of civilians that usually are contractors, but sometimes government civilians who are long for the technical expertise. But the reality is we don't have a lot of civilians in operation units. Already within Cyber Command units that are made up of people from services there's a stronger mix of civilians. I can imagine a world where it's fifty-fifty.

I can imagine a world where a lot of our cyber force personnel are civilians who don't fit well in a military uniform, who possibly have haircuts that are non-standard, whose face tattoos might seem offensive, whose previous weed usage would bum us out normally. But in a cyber force that's made of this mix, that's great. And by the way, those people don't need to go do career development tours and recruitment or in a training command. They don't need to get to different leadership. NCO leadership, well, we won't have NCOs in the same way, but training leadership courses and they can just do what they want to be kick-ass good at, design tools for breaking into open source software, whatever their specialty is within the program. And I just think that kind of focus is going to help us a lot. In other words, when you do this to a service, they have to account for it.

Even as we have different branches in the Navy, Army and Air Force, we try to have some kind of stability across them, not necessary. They'll be stable within themselves. And if I could mention one other thing, the guard currently, the National Guard has cyber elements, but very few National Guard chiefs say cyber is my number one priority. It's infantry, aviation, disaster response, civil engineering. Cyber's in there, but not in the top five. If you had a cyber guard, again, when the cyber guard, the Maryland Cyber Guard general wakes up in the morning, his or her number one priority is going to be cyber and we're just going to have that focus. And we have inconsistency in our current guard units where we have guard units like Maryland and Virginia that are just massively kick-ass good. And then you have other states where they have three people and it gets some inconsistencies that you can make up with agreements between states, but it's not the same.

So we got to figure out how to get that right. And I think a cyber guard, which is recommended in the report, it would be an important element of this. And trying to fix the guard, by the way, if you think fixing a service is hard, the guard is like fixing a service except you got 150 congressmen saying, "Do whatever the guard commander says." You know what I mean? It's a much harder thing to fix the guard. So you want to get it set up as a cyber guard where your congressmen are helping you, not hindering you from getting this fixed. I say that because the guard is easily the most political of the services in terms of congressional relationships. I just want to add those two things, Joe. Thanks.

DOUGHERTY: Thank you. Mark Pomerleau, Breaking Defense, that was a great question. Thank you for that. We're going to turn over now to a longtime cyber reporter, Shaun Waterman. Shaun, you've got your hand up, over to you for your question. Thank you.

SHAUN WATERMAN: Can you hear me okay?

DOUGHERTY: We can, Shaun. Thank you.

SHAUN WATERMAN: Okay. So two questions, little one and a larger one. Can someone explain the difference between defensive cyber operations and the DODIN, like defending the DODIN or the DOWIN or whatever they're calling it now? That's the first question.

Secondly, much bigger question, this is going to be a force that really doesn't look like any of the others, does it? I mean, it's not going to have enlisted ranks. I mean, you can talk about the medical service or whatever I think was mentioned in the report, but I mean, being real, isn't that going to create a huge challenge culture wise? Especially one might add, in the Department of the Army, which is a service which has regard for its enlisted force. I mean, second to none really. So could you address those two for me? Thank you.

STIEFEL: I'm happy to take that, Joe. Shaun, thank you for that. So the difference between DCO and DODIN or DOWIN operations, Hunt Forward is a prime example of DCO, that is active defense when invited by a partner ally to go hunt for the adversary inside their network. DODIN operations is defined as the care, feed, secure and operate of DODIN, DOW, DOD assets.

So that'd be your system administrators, your CSSP functions, which is separate and distinct from DCO, which can, like I said, Hunt Forward, DCORA, response actions. So there is a line between the build and securely operate, versus the active defense that we talk about with DCO. That's not our definition or delineation, that's in DOD policy and doctrine.

On your second question about it looking differently, I would say that the reason why we came out to this conclusion and I think it's been misunderstood is that it is not that we don't value the enlisted cadre. In fact, the opposite. We value the enlisted cadre so much that we believe that if they can make it through the cyber pipeline more than have earned the credibility, the merit to wear a warrant officer's collar device.

This is what you would see also if you went to, speaking of the Army, 160th Special Operations Aviation Regiment, where your aviators are a mix of commissioned officers and warrant officers operating at the absolute highest level for their discipline. That's what you're going to see there is technical experts and managers who are also able to operate.

So that parallel, that exists not only in the military, also in the private sector. If you go to Google, you can rise up through a managerial track, you can rise up through a technical track. That's the parallel we create by having a commissioned officer track, i.e. a managerial track, or a warrant officer track, more of a technical expert track.

What we're seeing with the Space Force where you have a one to 1.04 officer to enlisted ratio is it is generating some issues. We believe that this is a mechanism which addresses that and especially for a force that's so small, it really has to be able to punch above its weight. When an individual shows up, they don't have to rely on their corridor file. They are going to be able to say, "Hey, I'm CW02." Everyone's going to say, "Wow, okay, this guy must know what he's talking about if he's wearing a CW02 collar device."

DOUGHERTY: Lauryn, anything to add there?

WILLIAMS: No, not much on top of what Josh just noted. I think to the first point, one point we really did try to hammer home throughout the report is the expected scope of a potential cyber force, which as we've dug into already, the distinction between the scope being defensive cyber operations and offensive cyber operations as opposed to a much broader scope that would encompass DODIN operations. So I think that's certainly one key point to emphasize in terms of how we lay out what a cyber force might be and what it is not intended to be for the purposes of the commission's discussions.

Then finally, absolutely, I think a big takeaway from this report, as Josh has already dug into is the recommendations that the commission, over the course of deliberations, really spend a lot of time digging into and listening to and hearing from perspectives from other services, including the Space Force, to inform that recommendation around the composition of the force. So you'll see quite a bit of discussion around that in the report.

CARDON: So, Shaun, if I could just go back a little bit on the defensive cyberspace. So if you look at the commercial side, you have a CIO and most organizations have a CISO. Now the CISO responsibility is a little bit bigger because it also covers physical security in a lot of cases, but it is differentiated and there's a reason because if you want to have security, you got to have somebody that thinks about it all the time. So it's the same sort of thing here for defensive cyberspace operations.

I would argue this is one of the areas where AI is going to really have an impact. I mean, we're already having troubles. It's very widely known about Volt Typhoon, Salt Typhoon. It's not just a defense problem, it's a national problem. So how do we deal with this? Those operations would be defensive cyberspace operations, [inaudible] the operations of a unit's networks or a ship's networks or the air networks.

DOUGHERTY: Very good. Shaun, thank you for those questions, very much appreciated. We do have a couple of questions in the Q&A portion. First, we're going to go to David Roza over at Task and Purpose. He asks, "The report calls for cyber force to not commit to any single unit structure and instead adopt an agile approach to unit structures. Would this mean there would be no battalions, squadrons, or companies? If so, what would it look like?"

CARDON: So most ... Having been the initial commander of Task Force ARES, which at the time was a top secret offensive cyber task force against ISIS, you need a lot of flexibility in organizational structure. So you see the widespread use of task forces. Now you're going to have to have some sort of organizing principle, but the way that they're presented does not have to be a 40-person team. It might be a three-person team.

It has to have the kind of fungibility that the cyber force is well-used to. They're very used to, we just need the people we need to accomplish this mission. We might need somebody that's a specialist in UNIX. We need somebody who's a specialist in Brook Switch. We need someone that's a specialist in this language. We need someone ... Here, that's the team. Oh, then this problem over here, that's a different group.

We need people that are really good in cloud engineering. Well, this group we need over here, we need somebody that understands these large language models, or we need somebody over here that understands crypto. So you can't just form a unit for every one of these. You're going to have this expertise that will be organized and presented to the combatant command going forward. So there will be some organizing construct. We didn't fall down on exactly what that is, more on leave it open and let it organize much like we did in Task Force ARES.

DOUGHERTY: Mark Montgomery, anything to add to that before we move on?

MONTGOMERY: No. So what I would say is that one of the things we're trying to do is allow the cyber force by laying out the ... By trying to determine what the mission sets are, we'd allow the first cyber force commanders to really organize that. This is one of those things where we don't want to be overly prescriptive, but we want to give the mission task set so they can set up underneath.

I suspect that organizationally, since almost all their forces are going to be passed through, how they're organized in their training commands and in their initial administrative commands will be pretty traditional and basic. That will not be what's governed them. Almost all these people ... The beauty of this, if we do it right, is 80% of our operators are in operations.

Maybe 10% are in training, getting their own training, and then 10% are providing training or doing recruiting. I mean, there's breakdowns on these numbers to get them right, but the beauty of this is they will be in employed status from the very get go.

DOUGHERTY: Thank you, Mark. Thank you, Ed. Next question is from David DiMolfetta. He's with FCW, Nextgov. "Given how this force structure would get the attention of multiple congressional committees, intelligence, armed services, et cetera, what do we know about the appetite for this effort in terms of congressional leadership?" Josh, how about if we start with you on that one?

STIEFEL: So not knowing exactly what is in the language that was reportedly associated with Senator Gillibrand, it's hard to answer that, but what we said is, look, we're going to build this commission. We're going to build this product like a Title 10 mission. There have been talk in the past about service that blends Coast Guard authorities and DHS authorities and military, and we didn't go down that path.

Our golden assumption, our ironclad assumption at the outset was the president orders the establishment of a cyber force within the Department of War. So with that in mind, that's how we wrote this or that's how we wrote our paper, how the Senator has shaped her language is unknown to us at this time. When it comes to, let's say, the intelligence center idea, that's not a question of should there be a cyber force intelligence center or should there be an intelligence center for cyber because that's been deliberated. That's actually been adjudicated that was included in the FY25 NDAA.

The question is, there's a cyber force, should a cyber force have an intelligence center? I think that the answer to those questions are very different. I think it's unabashedly yes in the latter. So I'm not really concerned.

I think when the members see what this is and should there be a determination by the president and by the committees to do this, everyone wants to see it be successful. So they'll empower it and rally behind it. As Mark was saying, having a Cyber National Guard, having 50 governors, territorial leaders getting on board and supporting a Cyber National Guard in their respective states has a lot of political heft behind it. So I'm really excited about how this is received.

DOUGHERTY: Thanks, Josh. We do have a question from Tabitha Reeves and then we'll go over to Lauren Williams in a moment. Tabitha is from National Defense Magazine and she asks, "You estimate in the report about $10 to $11 billion to stand up the cyber force. Could you talk about that figure, how you reached it, how it compares to past estimates, and how feasible it would be to get the funding in full?"

STIEFEL: Yeah. So in the FY27 budget, there's $7.7 billion allocated for cyberspace operations. Of that, about 4.5 I believe goes to Cyber Command. The remainder goes to the services. So what we're saying is this is money that's already in the budget for this purpose, whether it goes to Cyber Command, whether it goes to services, that's what the Congress is allocating and appropriating this funds for. So that would be an easy thing that a cyber force could take on to then be doled out to Cyber Command, et cetera. That's for later. That money exists in the budget today.

The remainder of, which is military personnel costs, again, that's money that exists today in the budget, just fractured or fragmented across the four services today. For 20,000 active duty uniformed for 5,000 guard, and 5,000 civilians, that military personnel budget, at least for the uniform side, that's a, let's call it an educated estimate based on how the various services fund and pay for their individuals.

So this is really not new money we're talking about. This is actually money that exists in the budget today. It's just fragmented across four services. So by unifying that, by consolidating and in centralizing it, our proposition is you're going to get a lot better return on your investment.

MONTGOMERY: I'll tell you, this is one of these areas that... why we put numbers out there so you can manage this right. If you watch a Space Force budget recently, it went down 5% one year, then up 77% the next year. This is what happens when you don't think it out ahead of time. In fairness to them, it was dropped on them. There were fights between Republicans and Democrats on Alabama and Colorado. Don't want to get into all of it, but the challenges of Space Force, one of the things you have to do is learn from them. And one of our recommendations there is to learn from them and we did. And I would say hearing former Space Force senior leadership talk about those challenges is important. Josh and I have done a lot of congressional appropriating in our times, authorizing and appropriating. The way it works is you bring a workforce on as you transfer units. The first year you may say that our overall personnel budget is $4.7 billion, knowing that $2.3 billion is all that will be used that year because you only own the people for six months of the year.

But then the next year... We want to say up front what we think it's going to be, low ball the number and then later on go, "Oh, well, that's the growth that we mentioned." So we're putting the straight-up numbers in there, but the bottom line is this is being paid for. Our problem is, again, Cyber Command's doing okay. The problem is there's not a path to growth and it's a declining okay in a more aggressive adversary environment. So we are trying to be ready for the future. We can either have a calamity cause this or we can intentionally cause it through thoughtful, deliberate programming. What Ed and Josh and Lauryn and I are advocating for is thoughtful, deliberative programming to get to the eventual end state of a cyber force generating forces for an increasingly effective Cyber Command.

DOUGHERTY: Next question in from Lauren Williams of Defense One. Lauren, you have your hand up. Over to you please.

LAUREN C. WILLIAMS: Hi, thank you so much for doing this. I want to, I guess, build on Mark's answer there. My question is really about how your recommendations get after or maybe preempt some of the challenges that DoD had with standing up the Space Force and the Air Force as Joshua mentioned since those are the closest comparisons there.

MONTGOMERY: I'll pick it up and then I think Lauryn with a "y" is required to answer Lauren with the "e." Okay. First, like I said, the idea is that you lay out a predicate of what you think it'll look like and what forces need to be transferred, recognizing it'll go year over year. Space Force was unusual. Space Force came 88 to 92% depending on what capability you're talking about from one service. I want to say almost every original OG general was Air Force. They all came from the Air Force and then there's this 5 or 6% from the Army, 2 or 3% from the Navy, 1% for the Marine Corps kind of thing.

The Space Force was created because there was a perception, fair or not, that space was not getting due prioritization within the Air Force. Cyber Force is being stood up because there's a perception, which we think is right, that it's not getting due diligence from all the services. So it's going to be coming from all the services. So this is going to be a really interesting challenge. And look, it's going to be harder in some respects because when we say, "That 1.3% of the Army's recruiting budget needs to come over..." These will be challenging things. But if you lay it out ahead of time and say, "These are the functions. These are the lines of effort. These are the tasks to do that. These are the functions to do those tasks. We now need to take the appropriations for those functions and align them here," you can do it.

The good news is what we're talking about is in the Armed Services budget and both HASC and HAC-D and SASC and SAC-D. Intel's involved because the commander of Cyber Force is dual-hatted as NSA, as Ed mentioned, and there is a natural affinity between Cyber Command and the NSA, and the NSA are thieves who steal the really high-quality cyber operators. So they're involved in this, but they're not directly... Their appropriations, their authorization is not involved in this. So this is a HASC, HAC-D, SASC, SAC-D problem that we'll get our hands around that I believe if people follow this report, they can get their hands around it properly and get it done. Lauryn?

WILLIAMS: Yeah, so I'll jump in here. Lauren, I think we've met each other, including when I was at the Pentagon, so good to have you on. So some of the parallels just to add on related to the Space Force in particular that I think I and the commissioners, through our discussions, found really relevant and Mark already hit on one of them, which is around the shift in perception even in the last decade toward the 2019, 2020 period when we saw the standup and creation of... and restand up essentially, of new military space war fighting components, including the service as well as the reinvigoration of US Space Command, which are the kind of change in conversation, change in discussion around space as a war fighting domain. So I think that's a key element to keep in mind and drawing back to some of the comments that everyone on the call, Ed in particular, have already made around the changing cyber threat environment. So I think you can draw some parallels there in terms of the need for a force dedicated to the fifth war fighting domain, cyber in particular.

And then another key element to draw out that the report really hits on and calls to the need for a service, which is a conversation in a lot of several sections around service culture and doctrine... Culture and doctrine, which are essentially key elements that only a service has the responsibility to dictate. And so drawing to some of what Mark has already said, when we saw the standup of the Space Force, obviously a lot of the culture and doctrine was drawn directly from the Air Force, not least because that's where the personnel were drawn from. One key element of the report that Dr. Erica Lonergan really drew out is the similar need for a lot of deliberation and discussion around what a cyber force culture and doctrine should look like, not least because it would be drawing personnel from every other military service, so would be a mishmash of cultures maybe to start.

Therefore, there would need to be that true service development of its own culture and doctrine, which again, only a service can do within its fourth generation responsibilities. So I think that's another key element to point out, and we can only have that sort of discussion in the context of standing up a separate cyber service.

LAUREN C. WILLIAMS: Awesome. Thank you.

DOUGHERTY: Thank you to both Lauryns there. Very much appreciated. We do have one final question in from Drew Lawrence with DefenseScoop. Drew asks, "You mentioned competition with the private sector at the beginning of the call as well as with other government agencies such as the NSA. Can you expound on compensation for specialized cyber skills and how you expect funding for those skills to be sustained over time? I understand compensation isn't the only driving factor for cyber service, but I imagine it may be a decisive one, especially throughout the adoption of AI for cyber and historic legislative uncertainty for funding priorities." There's a lot there. I'll open the floor.

STIEFEL: So I could start this and then Ed, I'll call you in. But if you go to the 82nd Airborne and you receive jump pay because you're on a status that requires that sort of thing, no one talks about taking jump pay away from the 82nd Airborne. So once you have a service that plans and programs and budgets for these things, then they start to build in the rule sets and the institutional designs around compensation. And so whereas there has been variability with cyber pay and some missteps and two steps forward, one step back over the history of this. When you have a cyber force and your service is the one actually designing your budget, programming for incentive pays and assignment cycles and all that kind of stuff, that's what a service can institutionalize in a way that the existing services who don't have this as a first, second, third, tenth priority, are able or willing to do. And the history sort of bears that out.

CARDON: My experience of [Army] Secretary McHugh and [Army Chief of Staff] General Odierno standing up the cyber branch in the Army, once that branch was stood up, the amount of people that volunteered to come into it was stunning and it allowed us to put it in an assessment program to make sure we're getting the right people. I think that'll happen... We talked a lot about what the people will come in for mission, then they'll want to leave and we talked about we can do this with our personnel rules and we have some of this now, permeability, go out and work somewhere else, then come back because you can do things with the government that you can't do on the outside. You would like-minded people, as long as you're reasonably well compensated, the compensation is not going to be the driver. It's going to be, "What am I working on?" Because that's the culture of this area is more about, "What am I known for? What's my reputation? What have I done?" That is what drives this.

And you can see that in spades at Black Hat and DEFCON. In spades. So it's no different in the military. It just a lot of it happens to be behind closed doors. But you can see even recently to the point about, "Is CYBERCOM doing great work?" I think that's been in the papers. This is all about, "Can we continue to generate a force to do that?" And I think that a lot of our initiatives in play, and I want to build on Lauryn's comment, this idea of having a culture, that is so powerful, because if you think about it, there are other areas in the government, that they can make a lot more on the outside, but they don't because they love the culture and they love what they're doing. And so it's a higher purpose. So appreciate the question. Thank you.

DOUGHERTY: Lauryn and Mark, I see you both also nodding your heads as Ed was speaking.

WILLIAMS: I have nothing else to add, just agreeing.

MONTGOMERY: Oh, that was a great summary.

DOUGHERTY: Terrific. Well, that is excellent timing as we are coming to the conclusion of today's call. First, let me thank Josh, Ed, Mark, Lauryn for providing your expertise to the journalists on today's call. It is very much appreciated. To the reporters on today's call, thank you for taking the time to join us. We know you had multiple things you could have been doing and you joined us instead. You do have the embargoed report in your inbox. We will send you the link as well as the timing of the lifting of the embargo for Wednesday morning. We'll get that to you later today. If you would like to speak to one of the panelists separately today, reach me at press@fdd.org and I will be happy to make that connection. Special thank you to the team at the FDD Comms shop for the great work in the background for making this go smoothly. So this does conclude today's call. Thank you for joining us.