Persistent Access, Persistent Threat:
Ensuring Military Mobility Against Malicious Cyber Actors

April 17, 2025
Featuring Annie Fixler, General (Ret.) Mike Minihan, and Rear Admiral (Ret.) Mark Montgomery
Moderated by Bradley Bowman
Introductory remarks by Jiwon Ma

Transcript has been edited for clarity

MA: Welcome, and thank you for joining us for today's event hosted by the Foundation for Defense of Democracies. I'm Jiwon Ma, senior analyst at FDD's Center on Cyber and Technology Innovation. It's Thursday, April 17th, and today's panel will discuss how cybersecurity safeguards U.S. transportation infrastructure essential to military mobility. We're pleased to have you here for this conversation, some in person, some tuning in live and some listening to our podcast.

Recently, CCTI experts published a report titled "Military Mobility Depends on Secure Critical Infrastructure", and the title says it all. In the report, the authors make a compelling case. Our adversaries know the fastest way to slow U.S. military response isn't direct combat; it's by targeting the civilian systems that support them before they even arrive.

Washington must stop treating infrastructure protection as something adjacent to national defense. It is national defense. U.S. adversaries are already prepositioning in our systems today, using cyber as a tool to quietly lay the groundwork for disruption of future conflict. From volt typhoon's infiltration of telecommunications networks, to ransomware attacks on major airports, the warning signs are everywhere. This puts one of our greatest strategic advantages at risk, which is the ability to project power quickly and reliably. And that doesn't just depend on military assistance; it also depends on the digital and physical resilience of ports, rail networks, and airports, most of which are owned and operated by the private sector.

The report outlines the threats and offers a path forward, calling for harmonized regulations, sustained funding for cyber resilience, stronger authorities, and better integration of cybersecurity into military planning. The solutions exist, but time, coordination, and political will are the deciding factors.

To explore these urgent challenges, we are joined by an expert lineup today.

General Mike Minihan served as commander of the Air Mobility Command from 2021 to 2024. The AMC serves as U.S. Transportation Command's air component, executing the air mobility mission in support of the Joint Force, allies and partners with a fleet of nearly a thousand-hundred (sic) aircraft and over 100,000 active-duty, Air National Guard, Air Force Reserve airmen and civilians. Minihan served as deputy commander for U.S. Indo-Pacific Command and as vice commander of the 60th Air Mobility Wing at Travis Air Force Base. He entered the Air Force in April 1990, and retired in 2024.

Rear Admiral Mark Montgomery serves as senior director of FDD's Center on Cyber and Technology Innovation and directs CSC 2.0, an initiative that works to implement the Cyberspace Solarium Commission, where he served as executive director. Previously, he served as policy director for the Senate Armed Services Committee, coordinating policy efforts on national security strategy, capabilities, and requirements and cyber policy. Montgomery served for 32 years in the U.S. Navy as a nuclear-trained surface warfare officer, retiring as a rear admiral in 2017.

Annie Fixler is the director of FDD's Center on Cyber and Technology Innovation, contributing to the Cyber-Enabled Economic Warfare Project and the Transformative Cyber Innovation Lab. As an FDD research fellow, she works on issues related to national security implications of cyberattacks on economic targets and U.S. cyber resilience and contributes to the work of FDD's Center on Economic and Financial Power on offensive and defensive tools of economic coercion. Previously, Fixler worked for the American Israel Public Affairs Committee, AIPAC, as a senior research analyst.

Moderating today's conversation is Bradley Bowman, senior director of FDD's Center on Military and Political Power, where he focuses on U.S. defense strategy and policy. He spent nearly nine years in the U.S. Senate, including six years as the top defense advisor to Senator Kelly Ayotte and senior Republican on the Armed Services Readiness and Management Support Subcommittee. Bowman also served as national security advisor to Senator Todd Young and worked as Council on Foreign Relation's international affairs fellow on the Senate Foreign Relations Committee.

Before we begin, 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 and foreign policy. As a point of pride and principle, we do not accept foreign government funding. For more on our work, please visit our website, FDD.org, follow us on X and Instagram and subscribe to our YouTube channel.

And Bradley, the floor is yours.

BOWMAN: Great. Great. Thank you so much, Jiwon. Really appreciate that introduction.

General, welcome to FDD.

MINIHAN: Thanks for having me.

BOWMAN: Annie and Mark, awesome to have you here, and congratulations on the new report. I wanted to hold it up at least once. I see that many of you have grabbed a copy, and you can get one on the way out if you haven't.

We publish a lot of reports here. This is one that I would say – and Mark didn't ask me to say – this is definitely worth your time. It's kind of the essence of what we try to do here at FDD, and that is understand serious problems, and then just don't admire the problem; come up with real recommendations to get after it and not just admire it. So this is an amazing report that I highly recommend. I'm really looking for to discussing it with all three of you.

Thanks to you – those of you who are here in person and those joining online. I thought we could structure our discussion basically around three big ideas.

First is making sure that everyone understands – and I'll be honest I think most Americans don't understand – the degree to which our national security and the Department of Defense rely on civilian infrastructure to defend us and our interests. So we're trying to sound the alarm on that, and then we're trying to sound the alarm on cyber threats to that infrastructure that are not a theoretical or a future thing; they are a real, current thing. And then, consistent with what I just said, what the heck do we do about it?

So those are the – kind of the three topics that I want to explore with each of you. So without further ado, let's jump right in.

Annie, let me start with you. You're the – you're the lead author on the report, and the title, holding it up one last time, is "Military Mobility Depends on Secure Critical Infrastructure." So that title says a lot, but I really want to make sure that we understand it in practical terms. So why is civilian-owned infrastructure so essential to the Department of Defense's ability to deploy, supply, and sustain U.S. forces?

FIXLER: Sure. Thanks, Brad, and thank you all for joining us.

So I think as – as those of us who have gotten really used to and – and really appreciate next-day shipping, we all understand how efficient the private sector is when it comes to moving goods around the country.

And so while the U.S. military has its – many of its own systems, it doesn't make sense to have complete duplicate systems. So we don't need two separate rail line systems, we need the U.S. military to partner with critical infrastructure owners and operators who operate in the private sector to move men and materiel around the country and then overseas.

Specifically when it comes to the three systems that we took a look at, the Defense Department has various arrangements with private sector partners. So just to, like, shed a little bit of light on that, for ports, the Defense Department has designated 18 strategic seaports.

So those are the 18 privately-owned seaports that the military knows it will need to move ships – to move folks overseas, that it moves materiel in, et cetera. So that's sort of in the maritime domain. It also partners with and contracts with commercially-owned vessels to move equipment abroad, but that's sort of one component of it. So sort of replicated across the different infrastructures.

In aviation, there are civilian airports that the military has partnered with, that the FAA and the DOD have identified, that provide funding for, to make sure that they are available if the military needs to use them. There is a civilian reserve air fleet that are, again, commercial airplanes that the military can use as it needs to. Sort of these kinds of things keep replicating.

So just one last note on rail. The DOD has designated 40,000 miles of rail lines as the strategic rail corridor. Basically, the rail lines that it's going to need to move men and materiel from fort to port, right? How's it going to ship all of its tanks, all of its troops? It's going to go over commercially-owned rail. So that's sort of how it moves.

And so that is sort of the scope of the transportation sector that we looked at specifically in this report. And thank you, Brad, for holding it up and showing it off. And so, our concern is that there's not an appreciation for those systems among policymakers, among sort of the national security community and how integral they are to our ability to mobilize forces and respond to adversarial aggression.

BOWMAN: Great. Thank you. And that's a perfect way to start. General, let me go to you next if I may. Welcome again to FDD.

MINIHAN: Thank you.

BOWMAN: As Jiwon said, you led Air Mobility Command. I'm mindful that not everyone listening knows what that is. So maybe a quick word on what Air Mobility Command is and how it's relevant to what we're discussing today. And then really would love to hear your overview – we'll dive into the details here in a moment – but your kind of overview assessment of how DOD is reliant on the civilian infrastructure.

MINIHAN: Certainly – certainly. Thank you. First, thank you to the foundation for inviting me here today, and then congratulations to the authors of the report. I thought – I think it's really spot-on and worthy of this robust discussion and certainly worthy of robust action after we're done chatting about it.

My name's Mike Minihan. I just retired from the Air Force after almost 35 years of active duty service. You know, one day I woke up and I'm the old guy, and now I'm exploring the bearded part of my life, which it turns out my wife likes. So...

(LAUGHTER)

... pretty cool.

BOWMAN: Yeah.

MINIHAN: I had the opportunity to command Air Mobility Command, 110,000 people, active duty, Guard, and reserve, almost 1,100 airplanes. And you see them in action on a daily basis. So we're the airlift, you know, that hauls cargo. We haul passengers certainly.

We're also the aerial refueling, which is the flying gas tanks that extend America's power and extend America's hope. We are the air medical evacuation, which is the flying hospitals. And then – and we're all of the things on the ground that enable everything in the air. So think about the port facilities that process cargo and people, think about the maintenance that makes all of the airplanes go.

So all of that is a worldwide enterprise. We have fantastic partners with the Civil Reserve Air Fleet, which are America's passenger and cargo carriers that opt in to not only provide lift on a daily basis, but in times of crisis like Desert Shield and Desert Storm, crisis like the Afghanistan withdrawal, they can be activated and help augment the capacity that Air Mobility Command supplies.

I got the job for one reason, and it's because I worked for this guy in the Pacific. 10 years in the Pacific, two tours in Korea, two tours at INDOPACOM, and then a tour at Pacific Air Forces. So I got about 10 years in – and almost all of my general officer time was handling the challenge of China, handling the challenge of North Korea, handling the challenge of the tyranny of distance, and then I say the tyranny of water, too.

So I realize that there's a maritime component that handles water better than the air, but the reality is a lot of theaters suffer from the tyranny of distance, it's just that you've got a 8,000-foot runway every 100 miles that you can land, and that just doesn't exist in the Pacific.

So everything that I do relies on the civilian infrastructure. And, you know, so whether you're doing a withdrawal from Afghanistan, whether you're running supplies to Ukraine on a moment's notice, whether you're running supplies and support to Israel on a moment's notice, whether you're retrograding American forces out of Niger, or whether you're airdropping humanitarian supplies in Gaza, this all is heavily reliant on the civilian infrastructure.

To me, the – the key components of the infrastructure are this – communication, navigation, real infrastructure like runways, ramps, and taxiways, and then also the utilities that make them go. And so, you know, think about utilities not just in terms of electricity but it's the radar, it's the – it's the flight planning, it's the access to the national air system, the – the access to the international air system.

All of those things matter and come away. And so as critical as those partners are to making the mission happen, they're – also add vulnerability to the mission.

So I know we'll get into that later, but that's a broad overview.

BOWMAN: That's superb. Thank you. Mark, let me go to you next. You served as Director of Operations at U.S. Pacific Command and Deputy Director for Plans, Policy, and Strategy in U.S. European Command. So you view this, obviously in addition to your cyber expertise, from the perspective of warfighter, just like the General does.

From a military planning and operational standpoint, Mark, what are your thoughts on DOD's reliance on civilian infrastructure and how it relates to American military readiness and mobility and deterrence?

MONTGOMERY: Well, thanks. And first of all, I just want to say I'm excited to be on the stage with my – the best deputy I ever had. That's Annie. And...

(LAUGHTER)

... and a...

MINIHAN: I knew it.

(CROSS-TALK)

MONTGOMERY: ... I do – you can see I'm height agnostic on my choice of deputies.

(LAUGHTER)

So look, this is a big deal. We are not – our military has chosen for – over the last three administration – and really for 25 years, but a – particularly the last three administrations, from Trump 45, Biden, and Trump 47, to ignore the fact that our – to – to concentrate only on defending our bases.

In other words, I actually do think our bases are little Noah's Arks of critical infrastructure. There's two comm systems, there's two power systems. One of them might be a CATL battery set up – you might want to take a look at that but you know, two water systems, two of everything.

And then that train is loaded on a – that tank is loaded on a train car at Fort Cavazos, former Fort Hood, and starts to make its way to one of the ports. And it enters – you know, as it leaves the base, it enters Mad Max Thunderdome, right? It's on Norfolk Southern, and cybersecurity is just as good as that private sector company can afford when competing with a nation-state actor.

And they've fully accepted it, and DOD's embraced it. DOD says, not my problem, that we'll talk about later on. But they say it's TSA's problem, its U.S. Coast Guard's problem. It's not – it's the private sector's problem. It's not my problem. The problem, of course, is, it is our problem, right? It is the Department of Defense's problem.

When I was at PACOM, or Mini's at PACOM or TRANSCOM, in the components there, we absolutely are reliant on 69 airfields, 17 or 19 ports, depending on how you count them, and 40,000 miles or 40 percent of the rail network of our country.

We have identified, though – ahead of time, we've said, we've put the word "strategic" in front of strategic, 69 strategic airports, 19 strategic seaports, strategic rail. I don't know what STRACNET means, but it's something about strategic and rail, right? So, we acknowledge this is part of our team and yet, are fully committed – at the Department of Defense – to not supporting that team. And that is very unhealthy.

And here's the one thing that makes it worse. Congress goes along with it. Now, Congress doesn't go along with it for the crappy parochial reason of, "I don't want to pay for it." Congress pays for everything – because that's why the Department of Defense doesn't want to pay for it.

They're afraid, if they say, "I value that enough that it needs to be fixed", the next statement is, "You're paying for it because you're moneybags." You know, the DOD is dropping billion dollars out of its pocket, and U.S. Coast Guard doesn't have a, you know, wood nickel to rub together, right?

And so – but the follow on to that is in the House and in the Senate, this is controlled by – what we've mentioned here, those three that what Brad calls "a triad of mobility" are controlled by about five committees in the House and four committees in the Senate. None of which are Armed Services. So it's really hard to get this fixed. And in appropriations, it's three subcommittees of the HAC and three subcommittees of the SAC.

So, we're talking about 14 or 15 subcommittees that have to get their act – and committees – that have to get their act together on this. That is really, really hard to do, and so far, impossible.

If I could put one other tickler on it. Annie and I are starting to think, and I know we're not supposed to talk about the U.S. supporting NATO, you know, but I'm going to talk about the U.S. supporting NATO, since I think we're legally obligated.

We have this – NATO has the same problem. NATO's problem is worse. At least, there's only one federal government screwing up U.S. national security planning; in NATO, you got 32. So, if I went to NATO right now and I said, "Right now, give me your top 32 critical infrastructure projects that you need to get fixed to support military mobility through NATO."

I would get one thing from 32 countries, you know, one each from 32 countries, because that's how NATO looks at priorities. The right answer is five things in the Netherlands, four things in Belgium, seven things in Germany, eight things in Poland, one thing in each of the Baltics, because that happens to be – that is, for those who know the war plan, understand the unclassified TRANSCOM support to that war plan – that's the backbone of U.S. and U.K. forces flowing into Europe, are those five or six countries. We've got to convince NATO to attack this as a SACEUR-NATO problem, not a NATO Secretary General, 32 nation states problem. And so we've got to get on this.

First, they've got to agree, they've got to address it. And then when they address it, they've got to address it right. So, this is exciting. I think this is our third of four papers, probably, five with the NATO paper. You know, we've done the aviation and ports and the chapeau, the military mobility chapeau. We still have to do rail in a couple of months, and then the NATO one in a couple months as well. But we've got to attack all these issues.

BOWMAN: Great. General, did you have something you wanted to add to that or...?

MINIHAN: I think the – having been a part of, you know, I mentioned I got hired for the mobility job because of my experience in the Pacific. You know, I was intimately familiar with the challenges of a North Korea event and a China scenario playing out.

I certainly learned along the way how to do things, big things quickly and, you know, I was told to go faster. And so I've been very consistent on my concern for the mobility capabilities, the reliance on mobility. And I'm saying it from a, you know, from an air component perspective.

And the frustration with the system, you know, my frustration actually centers mostly on my service and what happens inside the building. I've had good resonance on the Hill with understanding the problem. But the only way you get graded on that is if more money comes your way, you know. And therein lies, I think what Admiral Montgomery was pointing out very good.

You know, the resourcing needs to follow here to enable the action. It's time. You know, I think there's enormous consensus on the challenge that lies ahead. There's enormous focus on why that challenge exists. And so now that, you know, there's two questions that a commander has to be able to answer – when did you know and what did you do?

It's time to get after the what did you do part. And I think that resourcing piece is incredibly important. It starts through the service, through the joint staff, DOD building, and then make a concentrated, consistent, passionate effort on the Hill for funding.

BOWMAN: Thank you.

MONTGOMERY: Let me pick one thing up because you made me think of something. Like, I went out to visit Mini when I was at St. Louis. And I was traveling around the Midwest, and I had to land at Columbus Airfield.

I've told Mini this. I don't know our war plans, but I'm going to put money that the Columbus, Ohio Airport is one of our 69 strategic airports because when you go there, there's like 70 gates and only six are being used.

But someone – for some reason, they're maintaining all these gates there. My gut reaction is, that's a good airfield. It's located centrally. It's close to St. Louis – it's close to, reasonably close to where other stuff is flowing to.

Now, why is this important? Because Columbus Airport is run by a local operating authority that is persistently broke. Right? That tax we all pay on our tickets, they're not getting a lot of those tickets, and they've got to maintain the physical and cybersecurity of all that stuff.

So, if I was the Chinese, I'd be looking around at all these airfields that we call strategic air facilities and say, "I'm going to go ahead and put malware, either plan a physical or cyberattack to disrupt movement at these airfields," because what you want to do is make Mini or Mini's successors' jobs harder, remove opportunities.

And I guarantee the TRANSCOM movement of like two or three divisions, or all the munitions we can to either the East, either to the Pacific or to Europe is a beautiful ballet that if I can shoot the lead violinist early on, you know, the music's not going to play right for the ballerina, right?

So, you know, that's the whole idea is I don't have to shoot all the C-17s down. I have to make it so the C-17s don't have the things to take, and I have to disrupt that thing. So, it would be very easy for a planner like me or a planner like Mini if we were on red in China to figure out how to undermine our system.

I think we're extremely vulnerable. We used to not say this out loud. I'm done not saying it out loud. And, you know, so from my perspective, we really need to attack on this.

BOWMAN: I wasn't expecting the orchestra ballerina metaphor.

MONTGOMERY: Yeah.

BOWMAN: But well played. So, just putting a bow on this first of three points. Right? So, I think what we're saying, and you all will help me correct me if I get this wrong, is that if deterrence fails in Europe, the Middle East, or the Indo-Pacific, for example, a large portion, arguably a vast majority of the forces that will ultimately deploy to fight in a major combat operation to defend vital or core American economic and national security interests will come from the United States. And they will not get there without relying on air, maritime and rail infrastructure, which we're incredibly reliant on. And now we're about to talk about how vulnerable it is.

So, did I get that about right in terms of the summary?

MINIHAN: Yeah. I think the exclamation point is the majority of America's power is in the CONUS [Continental United States]. And the same readiness that delivers deterrence also delivers decisive victory.

BOWMAN: Correct.

MINIHAN: So that you get a two for one out of that.

BOWMAN: Yes.

MINIHAN: And you want to create a situation where any potential adversary looks at you and says, I don't want a piece of that.

BOWMAN: And if our adversaries believe they can impede the flow of those forces from the continental United States, it may make them more likely to roll the dice on the aggression.

MINIHAN: That's not deterrence. Yes.

BOWMAN: And that's – and that is undermined deterrence.

MINIHAN: Exactly.

BOWMAN: Yes, Annie?

FIXLER: Yeah, I would just, I mean, I'm going to preempt some of the – like the next set of questions, I'm sure. But this isn't hypothetical.

BOWMAN: Right.

FIXLER: We're – this – this is what we've already seen from China. Volt Typhoon which I'm sure lots of folks in this room are, are familiar with was an, an operation or is still an ongoing operation to pre-position assets in the very infrastructures we're talking about.

They – the – the U.S. government obviously hasn't declassified all of the various places it found Volt Typhoon, but it's, you know, energy, telecommunications and transportation.

So, the Chinese know that those are the systems we need, and so they're pre-positioning assets there. It's no longer hypothetical. I'm not sure it ever was hypothetical, but we know now it's not.

BOWMAN: Perfect segue. Very well done. It's almost like you knew the plan.

Mark, let me – let me – Mark, let me go to you next. So in addition, building on the great start that Annie got us underway there, can you provide an overview of the cyber threats to the system we just described?

MONTGOMERY: That's good. So, I mean, I think Volt Typhoon's a good visual on it. What I try to tell people is, you know, if it's not just, we sometimes say it's putting malware and systems. I think that's a small percentage of Volt Typhoon. A lot of it is just gaining access so that you can come back at a later time.

By the way, that's much harder to detect. If you put malware in systems, most of our reasonable critical infrastructure companies can find it with decent cybersecurity.

Access is harder to find. I mean, it's, it's really you – it's a temporal moment that you see something happening that shouldn't be happening while you're studying it. So, Volt Typhoon was operational preparation of the battlefield. Mini and I practiced that and for 35 years, and Brad for 15 years, in the services. It is a core – I see Will Metts is here, who was actually our guy that would do that for us for INDOPACOM. Good to see you, Admiral Metts.

You know, that – that operational preparation of the battlefield is – is to me significantly different than espionage, intellectual property theft. It's an indication that they know we have this vulnerability and they're going to exploit it. And the fact that we caught them, I don't think it was on purpose. But, you know, I don't think they meant for us to catch them. But, you know, they were willing to take the risk.

So from my perspective, it tells me that, that if they're willing to try to exploit this risk, we've got to figure out how to do it, how to take care of it. And what really concerns me is that in the – I – I think, and this is true across both parties, so this is not a jam on the Biden administration, but while we are frustrated with them doing it, our initial response was almost like an espionage one, a – a tip of the hat to you. That's not what should happen here.

And I've used this analogy before, but I'll say it again. If we found a thousand Chinese backpacks with Semtex in it, strapped to the same critical infrastructures with a sign that said “the courtesy of the PLA” with a big middle finger on it, we would – we would probably be close to war if we had that kind of physical indications of a physical penetration.

But in the cyber world, and this is what you know, I see Jim Lewis is here, a lot of us have dealt with for 10, 15 years. We don't take these kind of cyber actions, they don't drive a concomitant response by the United States. And we've got to figure out what we're going to do here to take this.

I like that, Mike Waltz, pre being National Security Advisor, but while named but not in the position said, I'm going to be more offensive. I think at some point they're going to have to determine what – if they mean offensive like, I'm going to be a mean guy at your party. That's easy. I do that all the time. But if you're going to be more offensive, like I'm going to go, go do something to you and possibly tell you afterwards you know, do self-attribution and say, “hey boys, that was me, in case you're confused. All those transformers didn't blow up. You know, it didn't burn up simultaneously. That was us.”

I think we're going to need to, what'd we call that the other day? Deterrence by...

FIXLER: Demonstration.

MONTGOMERY: Demonstration. You know, I mean, I know I don't want to get into a big discussion of deterrence theory, but I want to say at some point we've got to do something about this.

BOWMAN: I love big discussions about deterrence. But we'll skip it this time.

All right, so let's dive into the mobility triad as we're calling it here. General, let me go to you first on the air leg of the Mobility Triad based on your obvious expertise on that.

Can you dig in a little – help us understand a little bit at an even deeper level the reliance and the vulnerability of our civilian airports and commercial aircraft? And you mentioned the civilian reserve air fleet, or CRAF.

MINIHAN: Right?

BOWMAN: I'm not sure everyone understands what that means. So make us experts in four minutes or less on the air leg of the mobility triad and the cyber vulnerabilities there.

MINIHAN: Certainly. We'll – we'll use Dover Air Force Base, which is in Delaware, on the East coast and we will – we'll use the operational template of support for Ukraine.

There's enough cargo that can go on the gray tails, which are C-5s and C-17s. And then also involve our Civil Reserve Air Fleet, which is a commercial 747, operated by an – an American Airlines. They would go into Dover, be heavily reliant on the utilities that make that airport go. So think about the electricity, think about you know, the things that handle snow and think about the power to the radar stations. Think about the FAA station, think about the tower that needs to approve flight plans and give you clearance into what is initially the U.S. airspace, and then into the international airspace.

Think about all the roads that lead in to that airfield that allow the cargo to be trucked up from, you know, name your depot or location that's providing 155s [artillery ammunition] or, you know, whatever the critical thing that that Ukraine needs is. Think about the rail transfer, the road transfer, the maritime transfer that needs to happen so that this could be packaged up on an airplane and quickly moved into a theater that matters. Think about – think about what happens when Southwest's computer goes down and the turmoil that would cause.

So, think about the vulnerabilities associated with those utilities. Those services are so critical to get it done, and you can very easily imagine that it could come to a standstill in a second if we were contested. The first mover advantage in cyber and space is the most critical first mover advantage that you can have in any conflict. OK?

And you can almost argue, and – and Annie did – tha, it's already being played out. You know, so their intel prep of the battlefield is complete, they've put in the fires that, that they can call well at a moment of their choosing, and they could completely challenge through multiple domains our ability to explode into theater. OK?

At the end of the day, this is about exploding into theater. This is about demonstrating America's readiness. This is about demonstrating her willingness to deter and if necessary, decisively defeat.

And the challengers out there know this. They don't have to shoot down six F-35s. They need to shoot down one tanker and that solves their problems. They don't need to disrupt too much critical infrastructure before they're having an enormous impact on our ability to operate.

The problem is extremely vulnerable with the military and it grows with the civilian sector. So think about the communication redundancy that exists in both dual-use there, think about our ability to navigate our reliance on precision navigational timing that comes from above, think about how easy that is to jam and have electrical interruption that causes problems there.

So their multi-domain way that they approach the problem is very centered on decisively affecting our ability to explode into theater, and if they can do that, then their first move or advantage that occurred in cyber and space will expand to the other domains, and it's hard to play catchup.

Here's what catchup looks like – the battle space in Ukraine right now. You're in an attrition warfare where a supply chain is trying to keep up with the lethality needed to win. It's very challenged to do that.

And if you want the future battle space to look like 1918 in France, then we continue the status quo. If you actually want to maintain an advantage and get after something that's meaningful and will deliver both that deterrence and that decisive victory lens, then we got some things we need to move out on quickly, and it starts with the civilian infrastructure.

(CROSS-TALK)

BOWMAN: Yeah, please.

MONTGOMERY: ... made me think of something there, Mini. In our paper, we aver to – we aver to – we weren't going to talk about it very much today but – cause Mini brought it up – GPS. One of the things that's interesting is that the military is – because of Ukraine and because of a little bit of Israel, Hamas – become much more sensitive to the vulnerabilities of GPS.

Now, I'm going to tell you, there's two types of vulnerabilities to GPS. There's one where our GPS – our current GPS – system, based on the L1 signal, is just old, you know? It's 50-year-old technology on 20-to-30-year-old satellites – or 30-to-40-year-old satellites that were put up 20 to 30 years ago.

The European system, Galileo, the Chinese system, the Russian system, are all newer and therefore slightly better systems. We knew this and we're slowly replacing it at – the only way DOD can do, you know, like execute a five-year plan in 15 years. And they were moving along.

Then we saw the jamming that happened in – because there's a second aspect to it, that not only is the signal weak, it's bad for, like, having a high-quality signal if you're running a John Deere in Montana but also if you're on an aircraft or if you're on a – if you happen to be a JDAM missile looking for a spot – a GPS coordinate. We started to find jamming on that last part, on the weapons systems. And some of our weapons systems performed very poorly in Ukraine.

Additionally, if anyone travels to Israel and you look at your – and you're up near Lebanon, you'll find out that you're at Beirut Airport, and if you're down near Gaza, you're at Cairo Airport, and that's someone – I'm going to assume the Israelis – spoofing the systems because drones will land themselves often, they have software that lands themselves, around airports rather than create a safety problem. So they spoof a lot.

So we have spoofing, jamming, and weakness. So we need to get up into a signal – and here – here's the problem – the military's first thought is “take care of the military.” So the military has all kinds of alternatives – alternative PNTs. They have a system that encrypts and makes their signal a little better, less jammable on the L1 frequency.

But all of infrastructure isn't going to have access to that. They need what's called the L5 signal. It comes from – it – it's a – it's a more accurate, stronger, much harder to jam signal. And Space Force was slow-rolling the launch of these satellites, and this is really hurting our critical infrastructure.

Now, the good news is Space Force got hard-rolled themselves by Congress and is starting to launch them, but we need Raytheon to finish what's called Operational Control System for next-gen GPS. It's like one of those normal systems. It's been one year away from being one year away for four years. Well, now there's solid, it's going to be done this fall, 2025.

Cut – you know, the Air Force, Space Force, and Congress need to hold Raytheon accountable and get that stuff done by this fall, because we need to be up – the satellites are all up there. We're just not using them because the Operational Control System, which should have been done five to seven years ago, is still waiting to get done.

BOWMAN: OK. So – thank you, Mark. So we've talked about air. Now we've got to go to rail and maritime. So Annie, make us experts in three or four minutes on rail. It seems to me – and I think I got this idea from you – that this is one of the least – probably – arguably the least understood components of the mobility triad, but it's fundamental, right, because we know, with my Army bias here, a lot of Army bases, newsflash, are nowhere near a port. So you've got to get those tanks and Bradleys… to the port, and we do that via rail, right? So talk to us about rail.

FIXLER: Yeah. So yeah, I mean, I think in some ways, rail is the simplest but perhaps most overlooked. I think part of that – I don't know. I think many of us don't think about rail on a daily basis, we haven't sort of thought about rail lines since we played with little trains when we were seven, but it's a complex network. Most of us didn't – don't interact with it.

But it is – it – it basically – most of the vast majority of the rail lines are owned by six Class 1 rail companies. They're freight rail companies. They're massive companies. And – but the – I – and I'm sure that they struggle with cybersecurity issues as all companies do, but they are resourced.

Concerns specifically in rail, a lot of it comes down to what are the short line railroads. So they are the interconnects between the large companies, they are the connectors between the rest of the freight rail system and the actual port, and there are a couple hundred. And they are small businesses, often. And so they are less resourced, have less expertise when it comes to cybersecurity issues. But it's across all of those different systems that the military needs to move its equipment.

So the concern is, look, you could disrupt, and that is for – that – that is a concern. You could also slow down. So if you can just back things up across the rail lines, you can't move a train off a rail except in certain interchanges, right? So if you've got a slow-moving train because there's something wrong with the signals, you're backing up the system.

And so that is – that is where – really, what kind of problem, at least if I were an adversary, I would look to create. I don't necessarily need to knock a line off, I need to create enough confusion that I slow down the movement of trains, and then I have cascading impacts across the system.

BOWMAN: Great. Thank you.

All right, let's go to – Mark, let's go to maritime. So you've been at this a while. Obviously, you bring deep knowledge in this area. – I've heard you talk about – in the past about some of the Chinese-manufactured cranes. I'd love for you to talk about that and our technology at our ports, and also talk about the role of the Coast Guard here, if you wouldn't mind.

MONTGOMERY: Yeah, thanks. So we did our port report about 15, 17 months ago. Atlantic Council's done a good one on it as well. And we supported the China Select Committee and then the House Homeland Security Committee as they looked at this.

You know, from my perspective, the ports is more – it – it – we made a mistake. Early on, one of the first bills was about cranes. This isn't about cranes, this is about automated systems in ports. So it's cranes, gantries, the rail systems, just the gates, everything.

When you go watch one of these ports work to load a large container ship with, you know – you know, 800 CR Land Containers, there are humans there as safety monitors, and there's humans there that operate some safety backup straps and things, but the vast majority of its automated. The whole timing is automated.

It is extremely easy to both disrupt, but also to determine what's happening, you know, to have an idea – because everything has to be laid out digitally ahead of time. It's – you know, it's subject to both surveillance and reconnaissance, but also disruption.

From my perspective – I love the idea that we identify the cranes. We have to be careful. I don't – these cranes are, you know, $100 million-plus apiece. I wouldn't be replacing the cranes. They're pieces of metal. I would replace the brains in the cranes, right? Now, if we get down in the $50- to $100 thousand frame.

And the cellular modems that are in the cranes – by the way, cellular modems, think of them like LiDAR, drones, Huawei, an area where China has decided to favor state-owned enterprises or you know, Chinese companies to become – to grab market share and drive U.S. and Europeans out. Cellular modems are the next big kind of drone/LiDAR problem for us.

But in any case, we've got to fix the – we've got to get the Chinese software and the requirement to communicate back to China for maintenance and for administrative things out of the cranes in the 19 strategic sealift ports. We just can't have that – that in there.

So that doesn't mean you need to replace – I know the – you – some U.S. or Japanese crane manufacturers are like, "Oh, we're in." You know, it comes to $20 billion – because we have about 100 of these cranes, you know, and it comes to $10- or $20 billion order. No. The people who should be, you know, excited are the cellular modem people and the people who build the software and the brains for these cranes, and the gantries and everything else.

Now, here's the problem: Coast Guard – the Coast Guard's a fantastic military service. It is a military service, which means if I tell them to do five things and give them four people, they'll do five things. They might be done shitty, but they'll do five things because they're a military organization who was told to do five things with four people.

So they got an executive order from the Biden administration that was brilliant. The executive order explained exactly what to do. Set up these standards. Do these assessments. Empower your captains in the port for cybersecurity. Blah, blah, blah – all this stuff. And it had exactly the amount of money that's attached to every executive order – zero, right? And that's the problem with trying to solve things by executive order, as both the Biden, and now, the Trump administration are figuring out. If you don't have money, eventually, Congress shows up and says, "Let's talk," you know. And so we've got to get this right, and the Coast Guard needs to have money.

Linda Fagan was a fantastic commandant of the Coast Guard 'til she was abruptly fired, and she understood this issue. But she also had no money, and when asked – their Sector Risk Management Agency budget was, you know, a handful of millions of dollars to manage these ports. We've been – we're going to get into recommendations of that, but one of our big recommendations is this shit's not free – this stuff's not free. You have to pay for services, and even when it's a military organization, you have to pay for a service. So you know, we've got to get on that.

FIXLER: Yeah, I'll just jump in on the port, as well just to, you know, remind us that we've seen incidents at ports before. The NotPetya inc- – cyberattack started – this was 2017 – started in Ukraine, spread throughout systems, hit Maersk – major shipping company. What happened as a result – this is – it was a ransomware attack – disguised as ransomware. It encrypted systems. It encrypted I.T. systems. It encrypted the data that indicated what was on what cargo ship that – that the – the gantries, as – as Mark mentioned, sort of needed that information to let various trucks into the port and out of the port. So you had massive backup because there was a cyber attack. This is the kind – you know, I'm sure that China is studying that incident and saying, "How can I replicate those kind of effects? I could do it with a ransomware attack. I could do it with a different kind of malware." But that is the kind of backup that then cascades again through the system. The issue is that all of these transportation networks are interconnected, so you cause a problem in one, you cause a problem in all. And so that is the issue that we need to be focused on.

BOWMAN: That's great. And some of you might be listening and say, OK, I get it. DoD is reliant on the civilian infrastructure. I get that our adversaries are doing things now to try to mess that up and impede it. But you know, hey, you know, we're America. DoD is smart. You know, we'll figure it out a few days, a few weeks later. We'll be fine. But as you two gentlemen know, and Annie you know from all your research, that time is everything once deterrence fails. And if you're talking about a term we use is "*fait accompli*." Right?

If you're talking about a Crimea-style invasion in the Baltics where Russians do something quickly, getting there quickly with sufficient forces matters. If you're talking about the Taiwan Strait, you were talking about first mover advantage in the cyber domain, first mover advantage in the kinetic domain, as you know well, is everything. So time matters. And by the way, a lot of our forces are going via vessels, which already takes a long time. So, if we can simply be delayed by a week or two or three, that could be decisive, have war and peace, life and death consequences in the theater of action. General, you agree with that?

MINIHAN: I do. I've yet to be challenged on this. If I'm going to be challenged, it's going to be from Admiral Montgomery. But I say that the mobility forces are the most relied upon force in the history of warfare. And I don't say that to be arrogant. I don't say that to seek sympathy. But I say that as simply, you know, a very focused statement on exactly what you just said. That in order to get through that tyranny of distance, get through that tyranny of water, and actually deliver a capability that can deter and decisively defeat requires what only Air Mobility Command can do.

Yet at the same time, the force is the most vulnerable, the least connected and least integrated with the joint force. And it's an intentional decision to do that. So, I think we have an opportunity now to really get after that. We are operating the second tanker that this country ever built. So, you know, think late '50s, early '60s technology, and it hasn't changed much. So, we're operating the exact same way our grandparents did in the '50s and the '60s. That doesn't scream explode into theater to me.

And so, there are critical things that we need to do to decrease our vulnerability, increase our capability, and certainly get after that integration, to make us – And this is not enormously expensive stuff to do, but it's an intentional decision. I'm waiting, I'm waiting. You're going to ask me later something about measurement. I'm waiting for an air power advocate or a senior leader to join me in a discussion that talks about effects and systems instead of platforms, and that advocates for joint effects in faraway battle spaces instead of service-centric solutions.

The quicker we can get to an effect- based approach and the quicker we can get to what the joint team needs to be successful in far away tough battlefields, the quicker we can get to the critical infrastructure investments and the reliance and the understanding of how we buy down risk and make best use of the platforms we have.

BOWMAN: I am restraining myself to not give you an amen on that one.

MONTGOMERY: Mini's about 15 seconds from getting thrown out of the retired Air Force General's club. Listen, he's right. This is –the Air Force, look, I think with the extra money we have in reconciliation, as much as we need to pay for shipbuilding, we need to pay – for the Navy – we need to pay to get the Air Force in a healthier place. And if I gave Dave Alvin, the Chief Staff of the Air Force, two or three, who is himself a LIFT guy, if I gave him two, three billion dollars, I'm afraid it would go into F-35s and B-21s, and the truth is it needs to go into C-46s and C-17s or whatever the next follow ons of those are. We need to preserve our LIFT.

What makes us a special military? We all, Will and me and Mini, Brad, we grew up in the military that said three things made us special. You know, we were committed to education and training, we were committed to empowering our enlisted and we were world class logistics. Those are the three things that make the U.S. military different than every other military. And we saw that with Russia, by the way. We thought that they were a world – had a large scale maneuver army. As they proved in the 2 kilometers as they left their bases in Belarus and Russia, they didn't.

But we still do have a world class maneuver military, and it's anchored in Air Mobility Command, Military Sealift Command. And so, that's the extension of our paper which is about the civilian infrastructure in the U.S. Mini setting up a Maneuver Institute. It's not going to be a subset of the Mitchell Institute I'm pretty sure. If anyone knows who they are. But you know, I think we need a lead advocate to discuss the importance of this. This is a – This is, I know it's a – You know, I know you don't like to hear this, it's a boring issue. Mobility and maneuver and logistics. But you cannot win a fight without it. So, I hope you're successful with this Maneuver Institute because we need it.

BOWMAN: Thank you, Mark. If we're going to say that China is the number one threat we confront as a nation, if we're going to say Indo-Pacific is the priority theater, you cannot hear what we're saying and shrug. I mean, this is fundamental. If you're a China hawk, if you're [focused on] the Indo-Pacific, you cannot shrug at what you're hearing today. This requires urgent action. I'm eyeing the clock. We got 10 minutes to get to the aspirin. We can't not do the aspirin. So, very quickly, General. OK?

MINIHAN: 30 seconds. Everybody hears the amateur study tactics, professional study logistics. Victors study maneuver. Maneuver is putting America's critical capabilities in a position of advantage over any potential adversary. So, this maneuver aspect is much broader than just the air piece. So, all the components have a play in it. But it's the maneuver and its – and it's acknowledging from my – from my tribe that we are in support. Everybody's success depends upon us doing our job.

You know, we're the O line of the military. You know when you got an awesome one and you know when you got a bad one, you know, so I want to be the awesome O line. I want everybody else to get the credit. I just want to do the blocking and tackling that makes it – that makes it possible. So, this maneuver, this victory, Victors study of the maneuver is critically important to the conversation. Nine minutes. Back to you, Jiwon.

BOWMAN: All right, thank you. All right, so lightning round. 30 seconds each on the following three things. Then we're going to go to recommendations. So, 30 seconds from Mark on forward posture. 30 seconds from you, General, on capacity. So, even if we fix all these problems you've hit just a little bit more on capacity. Do we or do we not have the air mobility capacity to fight two simultaneous major combat operations and then, Annie, misconceptions? So, Mark, forward posture, capacity and misconception. 30 seconds. Go.

MONTGOMERY: I just want to say, Black Hawk math, three times 30 seconds is nine minutes. All right.

BOWMAN: Hey, nuclear engineer. Here we go.

MONTGOMERY: All right, so look, on forward posture. This feeds into a deeper, longer issue that the United States military has traditionally embraced, but I think might walk back from under the Trump administration. And that's forward stationing forces. You need to be forward. One of the ways of reducing the risk of your critical infrastructure of your inability to flow things, or your critical infrastructure, of weaknesses in Air Mobility Command. I should say Military Sealift Command or MARAD.

Those are the two. There's a Navy Military Sealift Command, part of TRANSCOM [U.S. Transportation Command], MARAD, part part of Department of Transportation. They marry together to give us, in theory, 60 to 70 ships that can move equipment all over the world.

Let's just say that when we test it, we get like 30 ships, you know, like 40%, somewhere around 40% of what we need. And as a quality comment at a hearing, Anne Phillips, a retired admiral, good friend of mine, when pinned down on this, said, well, look, it doesn't really matter if we fix the ships because we also only have 40% of the people we need. And I'm telling Congress, "hey, we suck at this, but we suck at this worse" is actually not how you get out of the – out of the bull's eye. We just suck at both things.

So, to me, forward posture is critical. And I just want to say, Sam Paparo, a couple of days ago, he probably won't be allowed to say this again out loud, so make sure you took notes. He said, for a Patriot battery, it took 67?

MINIHAN: 73

MONTGOMERY: 73 C-17s to get it from Texas to the theater. Let me just tell you how many C-17s it takes to get a THAAD battery or Patriot battery from, you know, Atsugi Airfield to Tokyo. Zero.

If you're forward stationed, if your equipment's there, if your people are there, you lower the pain. And I'm just going to tell you, in a war with China, we don't have time for 73 C-17 lifts for individual batteries. We've got to get as much as we can forward station. We shouldn't be pulling back from these places. We should be keeping the forces that we know we need there so that they're there to fight.

BOWMAN: Thank you. Unpaid advertisement. December 2020, we published a major monograph Defending Forward – foreword in that by Leon Panetta. Five chapters. EUCOM [U.S. European Command], INDOPACOM [U.S. Indo-Pacific Command], CENTCOM [U.S. Central Command]. We made the argument for the value of forward positioned U.S. forces and all of its benefits in terms of signaling to adversaries about our political will to counter aggression. Building partner capacity, thereby reducing the burden on ourselves, and dealing with the tyranny of distance. Isn't one of the great ways to deal with tyranny of distance is travel the distance before the shooting starts? I don't know. Just a thought. OK. Capacity. We fix all these problems, we still have a capacity problem. 30 seconds. What is that capacity problem?

MINIHAN: First of all, capacity and capability are intertwined. It's hard to unpack them. But you know, the, you know, the capability of your team can also affect your capacity. I never had a day in the last three years of my active duty service where I had enough capacity. I came in on the heels of the Afghanistan withdrawal, instantly into Ukraine, instantly into Israel, instantly into Niger, instantly into Gaza, and then did all the things necessary to help the joint team along the way, too.

So, think theater exercises. Think the other combatant commands that have priorities. Think homeland defense. Think the President's going to travel. Think humanitarian operations in Philippines, Nepal, and other things like that. So, there has never been a day that capacity has been an easy thing. So, we need to get after our capacity. If we're going to explode into theater, if we're going to communicate America's will through action and not just words, if we're going to be able to ensure the President understands that he has the ability to decisively defeat anybody on the planet.

And at the end of the day, it's elected officials' opinions and decisions on whether we use that or not. But it can't be because we're not ready, and it can't be because we don't have enough capacity. So, I will take more capability in every one of my job jars that I mentioned at the beginning, but I also need more capacity on that. There's ways to get after it that's not billions and billions of dollars. Excuse me, but what we really need to drive hard on the capacity lane.

BOWMAN: Capacity. Fancy Pentagon word for "we don't have enough." We don't have enough. That's what it means. And the reason we don't have enough is because we're spending near post-World War II lows on defense as a percentage of GDP. Most dangerous geostrategic environment since 1945. Near post World War II low spending on defense as a percentage of GDP. That's called, strategic failure in my book.

MINIHAN: Thanks for giving me 15 seconds back.

BOWMAN: I didn't. But go ahead.

MINIHAN: That's my opinion. Ask the combatant commanders that are charged to win these conflicts what they think. You know, Admiral Paparo is a great example. But every one of them would lob in and say in order for me and my team to be successful in the problems that I've been charged to handle, AMC, TRANSCOM needs more capacity across the board.

Go.

BOWMAN: Very good. He stole your 15 seconds, so on misconceptions, congressional misconceptions.

FIXLER: No, I – I mean, I think there's a misconception among critical infrastructure owners and operators that if they get hit and it's a really bad day, the Cavalry's coming. Someone's coming to rescue them. But the reality's they're going to be called upon to move the Cavalry elsewhere. And so I think there's a real misconception as to the amount that critical infrastructure needs to be able to operate through the crisis so that our warfighters can move.

BOWMAN: Excellent. So we don't just specialize on headaches here; we specialize on aspirin.

Let's go down the line. One or two aspirins that you would recommend as most urgent to getting after these problems.

MONTGOMERY: So...

BOWMAN: Mark?

MONTGOMERY: So one that's not in our report, but since you brought it up...

BOWMAN: Yeah.

MONTGOMERY: ... we're doing another study on a better way for the National Guard to play a role in the defense of our critical infrastructures. I think there's a capacity there. It's not enough. There's work to be done. But I think generally speaking, that's the most likely way that the U.S. government in – any time in the next decade is going to be able to help the private sector.

From our report, the biggest one to me is grants. And look, these aren't – we're not giving, like, grants to, like, you know, Scrooge McDuck and Richie Rich. I'm talking about giving grants to Chicago O'Hare Operating Authority that taxes all of us, like, 10 time – you know, $10 a visit. I'm talking about small airport operating authorities that ma- – that make – made Mini' list of 69 strategic airfields, but don't have a large private sector – private passenger capacity going on right now. They need a grant program to fix some of these cybersecurity problems.

To get – to access the grant, you would have to do a government-approved risk assessment that's not static, but that's penne- – you know, that is – that's penetration testing the – in things that actually get at what your vulnerabilities are and that directly – the grant is to directly address those vulnerabilities, not by, you – you know, upgrade you from Windows 7 or wherever the hell you were, right?

So you know, that's, to me, the grant programs, and we have suggestions. We have 12 recommendations in the report – 12, 13.

FIXLER: Thirteen.

MONTGOMERY: Three of them are grant programs for each of the industries.

BOWMAN: Annie, four pages of recommendations. What's the number one that you would highlight right here?

MONTGOMERY: Oh, wait. Let me just (inaudible).

(LAUGHTER)

MONTGOMERY: All thirt- – not all 13; 11 of the 13 have legislative or appropriations language written by our FDDA, a 501(c)(4) that is pushing them on the Hill right now. So to me, it's critical that they get attacked in – in either the markup amendment phase or the floor amendment phase of this NDAA. Sorry.

FIXLER: Yeah. So what we talked about today is DOD is dependent on all these infrastructures. We're not advocating that DOD be responsible for these infrastructures. There are sectors risk management agencies, as Mark alluded to with Coast Guard, that are responsible for communicating, collaborating, informing the private sector. Those sectors risk management agencies need to be resourced appropriately so that they can engage in public-private collaboration.

There's some specific recommendations around making sure that various times that there are sort of co-sector risk management agencies that they are collaborating effectively so that they're not sort of – that – that they are the single point of contact, even though there's two of them, and that they are sort of working together. But we need to make sure that is resourced effectively, that that is communicating effectively with the private sector actors so the private sector can make the investments it needs to make and that they understand why and how they need to make them.

BOWMAN: Thank you.

General, one key recommendation from you?

MINIHAN: I'd take the two DOD recommendations. I think they're fantastic when it comes to review and accounting for all of the – the equities, especially when it comes to the civilian infrastructure. I'd take the recommendation right underneath that one that comes to the exercises. I'd combine those into a call that I've been making for years now, which is to get the entire joint team in a basement for six months and plan around the worst-case scenario that three administrations have identified in a row now and treat it like it's going to happen tomorrow, and remove caveats and assumptions and turn them into facts, and really define what our true joint punching power is, identify clearly where the gaps are, and then fund the things that close those gaps rapidly so we can do exactly what this nation needs to do: act like our peace, prosperity, and prestige is at stake here, because it is. And then deliver the president a force that's ready to go, where he or – he understands exactly where the risk is and what the capabilities are, and let them make the best decision possible. But it starts with knowing yourself, and I would take those two recommendations and form it into a six-month planning with no distractions.

BOWMAN: Amazing. As we all learned as junior officers, if it matters, you'd better establish milestones and you'd better measure it. If it matters to you and you're not measuring it, it doesn't matter to you.

MINIHAN: Amen.

BOWMAN: OK, great. Let's go to questions. Please wait for the microphone, identify yourself and ask a question in the form of a question.

Please?

FRIEDMAN: Hi. Sara Friedman, *Inside Cybersecurity*. With the Trump administration, they're looking for – trying to find efficiencies and more cuts to different services. Made a lot of recommendations, but of course, you need to have money for that. How do you see working with what the Trump administration is trying to do and protecting critical infrastructure, protecting services that – the triad that you focus us on?

MONTGOMERY: I'll go first on that. The – so first, Sara, thanks for the question. The – look, the – the Trump administration – I guess we could take some of the money they took from those cuts. You know I'm not a fan of those cuts, but we could repurpose them to these things. So it's not like the amount of money went away; just where they're spending it.

But look, I – I've spoken – I am disappointed they got rid of Dave Pekoske. I just want to say – Vice Admiral Pekoske was a fantastic leader, director of the Transportation Security Agency appointed by both President Trump 45, and President Biden.

Look, I'm not saying I like getting manhandled at TSA, but when TSA did its job as the rail and air cybersecurity advisor, I think he did a good job, but he didn't have enough money. So I – I think he would say as an SRMA, he didn't have enough money. He didn't have the grant programs.

But I'm hoping – I know Sean Plankey pretty well. I've met and I know Sean Cairncross pretty well. These are the incoming CISA director and national cyber director. I think they understand this issue. I think the Coast Guard understands it from the executive order. So I feel like the administration has a great opportunity here to get some wins and the – and do well at this. So I'm not – I have not given up. I am frustrated at some of the losses of public/private collaboration that happened over the last 30 to 45 days, but I understand that they care about this kind of military mobility. I believe the Trump 47 administration will tackle this issue. I just hope they can do it in a timely manner, and you know, they need to stop kind of breaking things and start building things, and this would be one of the things I'd build very carefully.

The good news is I think that Congress is in a much better position to help. There's a much greater understanding at ENC. These are House committees – ENC, TNI, Homeland. Representative Green gets this. Representative Pfluger gets it. Representative Crawford gets it. These are people who understand this. Like, Representative Swalwell gets it in the – on the Democratic side of the House. So they get this. I believe that Representative Houlihan and Luttrell get it in the House Armed Services Committee as a Democrat and Republican on the cyber side. And most importantly, Representative Don Bacon gets it, who's the chairman of the subcommittee.

So there's opportunity here, so if the administration is supportive and Congress funds these recommendations, I think we'll be in good shape.

MINIHAN: I agree. I think from the almost 35 years with, you know, the last third of that being in senior leadership positions, I think the – the time now is perfectly aligned for this administration. You know, there's certainly a different tact after getting things, but when it comes to the disruptive nature that needs to happen, when it comes to the advanced technologies that need to be embedded in, when it comes to, you know, significant collaboration that normally is hard to get to, I think we have an opportunity now, not just for the question you asked, but also for the planning effort that I've been driving for a while now.

I think that, you know, it's time to use this opportunity and take full advantage of it. I'm not certain that it will ever come around again.

BOWMAN: Thank you. Other questions, please?

WATERMAN: Shaun Waterman, freelance reporter for Air & Space Forces Magazine, among other publications. A couple of questions.

First of all, General Minahan, what you said about that, you know, the need to lock everyone in a basement for six months suggests that the current, you know, war gaming and simulation and planning process is not adequate in your view. Could you say a little bit more about that?

MINIHAN: I'm shocked that you asked me that question. Go ahead.

WATERMAN: And then my other question will be, you know, where – you mentioned Ohio, Admiral Montgomery, where else? I mean, San Diego, where can you sort of, you know, identify a couple of key geographic locations where, you know, multimodal nexi, I guess.

And talk a little bit about, you know, whether there's a way to – obviously, it has to be a systemic approach but, you know, is there a way to sort of harden particular vital nodes in these systems?

And then finally, sorry, could you just say a little bit more about how you envisage the relationship between DOD and these sector risk management agencies unfolding? Because, you know, there is a danger, isn't there, that this is seen as the sort of, you know, big DOD coming in to kind of, you know, boss everyone around.

MINIHAN: OK, I got C-130s out of pilot training. You're pushing the limits of my short and long-term memory here. So, I'll – I don't think I've ever met the exercise that I'm satisfied with.

It's a culture thing we need to get back to where we design exercises to fail. And we do our best to eliminate, you know, what we call "white carding" or "fairy dusting" or making it easier on ourselves than it really needs to be. That betrays the true task at hand.

So, I had the opportunity in 2023 to do an exercise called Mobility Guardian. That exercise normally occurred over the mainland of the United States. And we put it into the Pacific so we could specifically test our ability to explode into theater, test our ability on our reliance on civilian infrastructure.

Not white card fuel, not white card munitions, not put people in theater two weeks before the exercise starts so they could adjust their clocks, have them explode into theater and have to fly a mission the second they landed with max endurance operations.

And so all these things come back in the most wonderful, painful way that show you where your true gaps lie. I've got gaps in command relationships and understanding who's working for what. I've got gaps in connectivity. Does my team know where blue is? Does my team know where red is? Does my team have the latest intel? Does my team know who needs the gas, has the highest priority to get the gas?

You know, those things all emerge when you exercise at the right level. I fear that because we think occasionally that we do a TTX, a tabletop exercise, or have a poorly constructed exercise that we're drawing conclusions instead of gaining insights.

You know, we really – we really gain insights from these type of things where we shouldn't draw conclusions. And the sophistication of your exercise program is directly proportional to the insights and the conclusions you can look into. And I don't at all think that we're getting after it to the level that we need to get after it, but we can.

BOWMAN: Train like you're going to fight. Train like you're going to fight. And I'm aware that the Air Force F-15 unit that was shooting down Iranian cruise missiles and drones on April 13th may have been in location about one to two days before they started to do that. And they had to improvise. And if they weren't such trained, patriotic professionals, there would have been American deaths.

MINIHAN: Yeah.

BOWMAN: Question, to what degree is our training reflecting that reality so that they don't have to improvise so much next time? Answer, I don't like the answers I'm hearing. Anyway, so key locations, Mark, and then SRMAs, I think were the other two parts.

MONTGOMERY: Yeah. So, key locations, look, I hesitate to say this because the worst thing we can do is solve 10 percent of the problems because then DOD goes, "got it." Because, you know, where would I go? I mean, Charleston, California, and St. Louis, and then for the Air Force. And then for the maritime, Oakland, and Charleston.

I mean, but if you only solve, by the way, DOD does work on those. Those are places where they sneak their nose over the base fence and go, we better make sure that stuff's OK. What they don't do is all the stuff leading up to it. And if the rail network doesn't – how much of the 40,000 miles of the rail network needs to be secure? Forty thousand freaking miles, you know.

You cannot – this is not – TRANSCOM didn't make these numbers up. I'll give TRANSCOM credit for something. They're really good at numbers, right? You know, they got this – these plans are complex, and they're well understood by the Chinese. So, I would not allow that to happen.

Do you want to answer on DOD SRMAs?

FIXLER: Yeah, I'll hit that. First, I want to mention, just on exercises for a moment since we brought it up. So, a bunch of our colleagues last summer traveled to Taiwan, did a tabletop exercise, a TTX.

What we found in that TTX, the scenario that my colleagues looked at was not the most damaging, the most concerning, the dangerous – thank you, most dangerous scenario, cross-strait invasion blockade. It was the most likely, the cyber-enabled economic warfare campaign by China against Taiwan. That is not a kind of exercise that DOD often runs. It should, because that's the most likely scenario.

So, it's – our exercises may also be sort of geared in the wrong direction in certain cases where we need to gear them in the most likely scenario, which is cyber and economic. Our adversaries aren't jumping straight to military because we've got a vulnerable underbelly in the cyber domain. So, that's the first thing I would mention.

When, with regard to DOD and the SRMAs. So, the SRMAs have a lot of sector-specific expertise. That's their job. Look, a lot of them are underfunded, but there are good people in those SRMAs that have the expertise of what makes their sector uniquely valuable, uniquely vulnerable.

And DOD needs to come to them a little hat in hand and say, help us better understand your sector so that we can help you then inform them on what they need to do. So, a little bit of humility at a DOD, I think will be helpful. And the SRMAs, you know, come to the plate and being resourced to come to the plate and play a role.

BOWMAN: General, Annie, Mark, thank you so much. I feel like we could do a second hour and I would thoroughly enjoy it, but you've given us a lot to think about and to, more importantly, act on and really respect your service to our country. Annie, and congratulations, Mark, on this amazing report.

Thanks to everyone in the room for coming, taking the time to come. I hope you found it useful. Thanks, everyone, joining online.

For more information on FDD and the latest analysis on these and other issues, we encourage you to go visit FDD.org. We hope to see you again soon. Thank you very much.

(APPLAUSE)

END