Transcript

National Guard Bureau Public Affairs
Press Desk (703) 601-6767
ng.ncr.ngb-arng.mesg.ngb-media-desk-owner@army.mil
www.nationalguard.mil

NATIONAL GUARD ON-THE-RECORD ZOOM MEDIA ROUNDTABLE
Tuesday, June 6, 2023

TOPIC	SUBJECT MATTER EXPERTS
National Guard Cyber Shield Exercise 2023	• Army Brig. Gen. Teri D. Williams, exercise director and vice director of operations (CYBER), National Guard Bureau • Army Col. Jeffrey Fleming (ILARNG), exercise officer in charge • Air Force Lt. Col. Jenny Naylor (WVANG), exercise staff judge advocate • Maj. Marcin Barszcz, cyber analyst, Polish Cyber Command • OR-6 Staff Sgt. Selim Jashari, cyber defense unit, Kosovo Security Forces

Introduction:

Our nation, states, communities, corporations and institutions are under attack each and every day; but rather than bombs and bullets our adversaries are using binary ones and zeros. And, just as it has for more than 380 years, the National Guard is playing a key role our defense.

The National Guard is conducting its annual unclassified Cyber Shield exercise June 4-16 at the Army National Guard Professional Education Center on Camp Joseph T. Robinson Maneuver Training Center, North Little Rock, Arkansas. This annual exercise began in 2007 and involves more than 900 National Guard Soldiers and Airmen along with U.S. Navy Sailors from throughout the United States and its territories as well as partners from other government agencies and the private sector.

The exercise is a result of the National Guard's commitment to responding to attacks on U.S. critical infrastructure. It is conducted in an unclassified environment to allow for more involvement from partners outside the Department of Defense. The mission of Cyber Shield is to develop, train and exercise cyber forces in the areas of computer network internal defensive measures and cyber incident response. These capabilities facilitate National Guard Cyber Teams' abilities to conduct missions to coordinate, train and assist federal, state and industry network owners that are threatened by cyberattack.

Transcript

National Guard Bureau Public Affairs
Press Desk (703) 601-6767
ng.ncr.ngb-arng.mesg.ngb-media-desk-owner@army.mil
www.nationalguard.mil

The focus of this year's exercise is on the National Guard's role in responding to an attack on U.S. Transportation Systems Sector critical infrastructure. In addition to assisting outside agencies, the civilian-acquired skills that many cyber–National Guard members possess also strengthens the military's resolve to support and defend the nation against all enemies foreign and domestic. Freight Rail consists of seven major carriers, hundreds of smaller railroads, over 138,000 miles of active railroad, over 1.33 million freight cars, and approximately 20,000 locomotives. An estimated 12,000 trains operate daily. The Department of Defense has designated 30,000 miles of track and structure as critical to mobilization and resupply of U.S. forces.

This year marks a significant milestone as members from five State Partnership Programs join forces with National Guard Cyber Teams for the very first time during the exercise. The collaborative efforts will bring together Poland and Illinois, Kosovo and Iowa, Armenia and Kansas, as well as Moldova and North Carolina.

Opening Statement:

Welcome to this media roundtable on the National Guard Cyber Shield 2023. I'm Nahaku McFadden, and I'm going to be moderating today. We are here with Army Brigadier General Teri Williams, who is the exercise director and vice director of operations, cyber, for the National Guard Bureau. We also have Army Colonel Jeffrey Fleming from the Illinois Army National Guard, and he is the exercise officer in charge; as well as Air Force Lieutenant Colonel Jenny Naylor from the West Virginia Army National Guard. She is the exercise staff judge advocate. We have Major Marcin Barszcz, cyber analyst, Polish Cyber Command, and we also have OR-6 Staff Sergeant Selim Jashari, cyber defense unit, Kosovo Security Forces. So what we are here today to do is to discuss the National Guard's Cyber Shield 2023 effort, and we appreciate if you would focus your questions accordingly. Brigadier General Williams will start with an opening statement and then we will open up for questions. And to ensure we allow for everyone to to participate, please ask one question and a follow up, and if there's time at the end, we can open it up again. Reminder to keep your phones mute when you are not speaking. I do have a list of the media and I will call on you by name. And with that, Brigadier General Williams.

Brig. Gen. Williams: [00:02:52] Hey, good morning, everyone. Thank you for being here and thank you for this opportunity. I really want to focus most of this on the stars of the show, which are the folks that you see seated at the table while they are there who have done the yeomen's, you know, yeomen's work in terms of pulling this exercise off. But again, you know, really an unclassified cyber defense exercise that we use uniting the top talent across the nation and across the world, as you see with our partners here, to really get after capability, capacity, competence

and and quite frankly, will. So you're going to get to hear a lot of great things about the things that they're doing. Both this week and next weekend and excited to share that with you guys today. Thank you.

Dialogue:

[Name]: [QUESTION/RESPONSE]

Nahaku McFadden: [00:03:41] Thank you, ma'am. We are going to be dropping your bio in the chat. So, for any of the media, if you don't have that, it will be available as well as the list of our panelists here on Cyber Shield. If each of you, starting with Colonel Fleming, would introduce yourself and your title, that would be great so everyone knows who is who.

Col. Fleming: [00:04:06] Colonel Jeff Fleming with the Illinois Army National Guard. In Illinois I am the G6 and here at Cyber Shield on the officer in charge.

Lt. Col. Naylor: [00:04:15] And I am Lieutenant Colonel Jenny Naylor. I'm actually with the West Virginia Air National Guard and not the Army National Guard. I am the staff judge advocate for the 167th Airlift Wing, out of. Martinsburg, West Virginia. And what that means is just the military general counsel.

Maj. Barszcz: [00:04:40] Good morning, everybody. I'm Marcin Barszcz from Polish Cyber Command. I play a role as a incident responder in the Computer Incident Response Team, Polish, MOD. And here in the exercise I am a cyber analyst in Blue Team Illinois, No.13.

Staff Sgt. Jashari: [00:05:02] Thank you. Good morning, everyone. I'm Staff Sergeant Jashari, from Kosovo Security Force Cyber Defense Unit. I work there as a cyber analyst. Here in Cyber Shield, I'm attending one of the courses provided here and also will be participating in the exercise.

Nahaku McFadden: [00:05:21] Thank you and welcome to everyone. So we're going to go ahead and open up the floor for questions. And so, please, if we can, one question and a follow up, and then we'll open it up if we have time. So let's start with the Liz Friden from FOX News. Liz, are you here?

Liz Friden: [00:05:42] Hey, thanks. I'm here. I guess what's the main difference between this exercise and past exercises? Do you guys plan on doing anything differently? Will it be bigger? Just can you elaborate a little bit?

Col. Fleming: [00:06:00] Yeah, certainly so a couple of the big differences this year is obviously the first one you see sitting on the panel here. It's the first time in a long time since we've had our international partners sitting on blue teams with their respective state partners. And so that was a big focus. And then the other significant change is this year we brought operational technology into the mix and we're getting back towards that and which is different from information technology. And so we're looking at several

response to a critical infrastructure involving operational technology, compromise and things of that nature. So evolving as the threats evolve.

Lt. Col. Naylor: [00:06:41] And from the legal perspective, I think this is the first maybe the first time that we're strictly operating under the Title 32 statutory authority. And I'm not sure if that means anything to the audience out there, but it's actually a great deal for the National Guard because as some of you may know, the National Guard Guardsmen, we occupy a very different mission space under different title authorities. And that title authority or duty status, this actually drives our authority under the state or federal statutory regulatory policy sources. And this year we have a record number of judge advocates attending the exercise. And because of that critical mass of attorneys here, we're also going to test and stress various different legal principles and doctrines that haven't really been thought through or operated on the ground. So I'm also looking forward to see what our attorneys can come up with.

Nahaku McFadden: [00:07:41] Excellent. And any of our State Partnership Program. Do you have anything to add as far as what this means for you participating in this exercise, as well? Major Barszcz or Staff Sergeant Jashari?

Maj. Barszcz: [00:08:01] Thank you on behalf of Poland and Polish Cyber Command. Firstly, I would like to thank you for the invitation through cyber issued exercise and express our hearty thanks to you all for your hospitality assistance in each step taken here, as well as the whole effort that has been put into this exercise. I would like to highlight also the importance of the State Partnership Program, especially on cyber related field. This bilateral collaboration is beneficial to both sides, I believe, and strengthen our relations, which are crucial in the cybersecurity effort and struggles we have on a daily basis. We are excited to death to have this subject of the exercise for the first time. As you know, the ICS technology and integration with IT networks on this field, the security concerns arise. So this is important for us to practice review this matters. Thank you.

Staff Sgt. Jashari: I would also like to express my gratitude to all the efforts that have been done to bring us here. So we will having a partnership for several years with our National Guard. But this is our first time in Cyber Shield. And I want to express my gratitude to all who made it possible for us to be here and to gain skills and expertise and experience. And thank you very much.

Nahaku McFadden: [00:09:49] Thank you. Liz, do you have a follow on?

Liz Friden: [00:09:54] No, that's it. Thank you. Thank you very much, everyone. Thank you.

Brig. Gen. Williams: [00:09:58] If you don't mind, I'll just jump in. I'm sorry. I'll just jump in and kind of just summarize it in terms of I would just say really and trying to capture what each one of them said. It's really about integrated deterrence, right? Like, that's really kind of the next step, whether it's operational technology, working in close collaboration with our allies, but basically to ensure that potential foes in cyber understand the folly of aggression.

Nahaku McFadden: [00:10:26] Thank you, ma'am. Next, we're going to Breaking Defense Jaspreet Gill.

Jaspreet Gill: [00:10:31] Hi, thank you for doing this. I'm curious if you've taken any lessons are not of Ukraine and applied it to this exercise this year?

Col. Fleming: [00:10:43] Yeah, so specifically to the Ukraine. So cyber is cyber. So what they're using there is is kind of global stuff. And so what we did early on as we had some partnerships with the FBI and Homeland Security and the private sector, as well as a few of our research universities across the DOD and across the world. So we had my staff at the small level. We have two planning conferences early on where we sit down and start to frame out what is the exercise look like. And so in we take in at the top levels of classified stuff and use that based upon what they're seeing, what their threat is, what folks think is going to be coming in the near future. We have some very elite folks on our, that play our exercise bad guys and gals that do the advanced threat research for their full time jobs as traditional Guardsmen. And so we kind of take the holistic look at that and figure out what is the best scenario that we should focus on based upon what's currently going on, and more importantly, what the forecast looks like. So it potentially includes some of the things from the Ukraine, but that's not we're not limiting in scope one single engagement that we have going on.

Nahaku McFadden: [00:11:59] General Williams, do you have anything else to add?

Brig. Gen. Williams: [00:12:03] No, I totally agree with Jeff, of course. And I would just say timing resiliency is one thing that we tried to throw in as kind of an ancillary piece. Again, important to cyber, but also has other ramifications. So we tried to squeeze that into the scenario for some of the things that the teams are are rehearsing and preparing for.

Nahaku McFadden: [00:12:31] Jaspreet, do you have a follow on question?

Jaspreet Gill: [00:12:33] Yeah. I was wondering if you can give an example of a specific scenario that you guys are preparing for.

Col. Fleming: [00:12:43] So I would love to talk some of the exercise specifics, but with the foreign partners here who are sitting on the blue teams, they don't necessarily know what's coming out yet next week. So I can't go too far into it. But it's it's common things. So it's going to be the average and not the average, but the common way the attack chains play out. So it's, it's a very sequential effort and very deliberate. We do run multiple capabilities of, of bad actors beginning at script kiddies all the way up to advanced persistent threats. So they'll face several different levels of the bad groups in the network utilizing the advanced tactics for whatever skill set or whatever operational campaign for the exercise that those bad actors have been selected to carry out.

Nahaku McFadden: [00:13:31] And Colonel Naylor, I know you mentioned a little bit about bringing in some of the a different aspect to this. Is there anything that you could add to that?

Lt. Col. Naylor: [00:13:41] Well, along the same line, we're also partnering with our counterpart attorneys from FBI and CISA to give us sort of an overview of whether the legal authorities, when legal authority of the FBI, and CISA and interacting with our private partners with state, territorial, tribal and local governments. And I think through that coordination with FBI and CISA on the on the legal side, we can definitely sort of train our attorneys to move quickly and to know a wider diversity of law and also to ensure that our cyber activities are conducted in accordance with domestic and international law. So I think one of the lesson that we're hoping that our attorneys will take away from this is that, you know, the demand for a legal counsel and advice, advice and counsel is no longer reactive, but we're proactively seeking and enabling our commanders and cyber operators, but then continue to promote that rule of law here at home and abroad.

Nahaku McFadden: [00:14:43] Thank you. Okay. So we're going to go to Chris Adams, Reserve and National Guard Magazine. Hello, Chris. Well, we can't hear you yet. I think. Are you trying to unmute? We'll come back to you then, Chris. Just hang in there. Next, we are going to go to Joe Belford from Arizona State.

Joe Belford: [00:15:31] Yes. Good morning, everybody. I'm a student at Arizona State University. I'm studying for a master's degree in global cybersecurity. I appreciate the invite, No. 1, thank you very much. My question is about if there was a successful cyber attack launched against, say, a public utility or co-op, I was wondering how the National Guard would initially be deployed, Who would who would make the call and who would be the initial contact to the utility if in such a scenario?

Col. Fleming: [00:16:09] You know it. It depends.

Nahaku McFadden: [00:16:14] General Williams, okay. Sorry. Go ahead.

Col. Fleming: [00:16:17] So I'll say it depends. A lot of it in cyber, especially at the National Guard level, is relationship based. So, depending on how that critical infrastructure provider has also decided to align their response. We have some of the states, including, you know, from the 36 represented here, where the first call is to the governor or the National Guard. Some will make their first call to their private incident responder on retainer. Others may reach out to Homeland Security, FBI, just depending on the level of the attack. So that would be their first entrance into the response ecosystem, on a call, or the response framework. And then depending on who they tap first and the level to which it escalates will determine which agency ultimately ends up running the investigation. Does it touch ... is that critical infrastructure provider, does it touch multiple states? Is it, does it touch multiple utilities because it's a or multiple critical infrastructure pieces, because it's a common or a common system that they have between multiple ones and kind of scales up from there. So I can talk vaguely or as an example of the exercise we're looking at here, without giving too much away for these folks. This year we're looking at force projection in a contested homeland and how do we defend the rail networks to support the movement of military goods, equipment, personnel and commercial stocks across the country? So in that instance, you have a railroad that stretches from coast to coast. So if they get into a rail network, it's definitely going to

cross several geographic lines. And at that point, what I'm told from the law side is this DHS/CISA owns the lead federal agency response for that type of effort. And so they would take over in the lead federal perspective and then call on other federal and state partners to come up under their umbrella of command and hand out assignments accordingly. Some of those could be Guard forces, some could be DHS as a forces or whatever forces they have to bear that are partner with them.

Nahaku McFadden: [00:18:23] General Williams, will you like to add a little more? I'm sorry. Go ahead.

Lt. Col. Naylor: [00:18:26] So I thought Joe asked a very interesting question that he used the terminology cyber attack. And I think a lot of time from the attorney's perspective, we also are always looking for more facts on the ground to develop before we can actually characterize a cyber incident. Because the word that we use carries a lot of weight. And calling something "attacks" necessarily has certain legal implications. So I think the National Guard could be called upon to respond to a wide range of incidents from maybe a nuisance to a criminal vandalism to maybe at the highest end an actual attacks. So I think, you know, I think the words that we use really matters.

Nahaku McFadden: [00:19:12] Thank you for sharing. From the bureau level, ma'am, do you have anything to add?

Brig. Gen. Williams: [00:19:23] No, I mean, like. Like everything. It depends. Right? And so Jeff talked about the state response. There's also obviously a federal response. And he kind of touched on it in there. But, you know, you have you have CISA, but you also have processes in place in order to to get assistance from the Department of Defense. Doesn't mean it's going to be the National Guard per se. But we do have processes in place for that sort of thing. So the best mechanism for those partners in the critical infrastructure space to really start is build those relationships with your National Guard units, with your CISA cybersecurity advisors that are that are resident to the state. And then those folks can help you kind of move through escalation if that's necessary.

Nahaku McFadden: [00:20:14] Thank you. Joe, do you have a follow on?

Joe Belford: [00:20:19] Yeah, actually, I do. I was wondering. The interaction between all the governmental agencies. I know you know, DHS, CISA, you know, Easterly truly says that cybersecurity supposed to be a team sport. But how are the lines drawn? You know what? The Department of Defense, what Homeland Security, with the FBI, it seems like there's a lot of blur between who does what. You know, is there any way that, you know, one agency specifically is in charge of like an initial cyber incident, for instance?

Brig. Gen. Williams: [00:21:06] Yeah. So what I would tell you is there are absolutely lines and I think we all have our own roles and responsibilities and internally I think we understand those well. Maybe they're not projected well, you know, to the public. But ultimately, I think where what you're getting after is this nexus that you have with the National Guard, right? We have a federal mission and we have a state

mission. And then and we have an immense amount of talent that we bring to, you know, to the cyber arena. So essentially, Cyber Command, you know, they not only have the responsibility for the DOD networks, but they're looking kind of out, you know, and protecting the nation from adversaries from afar. You have essentially DHS/CISA who is more inward facing, as well as NORTHCOM, kind of inward facing in terms of the protection of the, you know, of the nation and the homeland defense arena. And then you have the National Guard that, again, can kind of wear whatever hat you need us to do. We can we go on missions for Cyber Command and we do the federal missions for them. But we can also, if needed by the governor, can be activated to, you know, assist with incidents within the state or even I'm not going to even say I don't like playing the game to lose. Right. Like, I don't like to say that it's all going to be reactive. You've heard members of the panel talk about the proactive piece and how important it is, and that's really what it's about. It's about relationships matter and and building those relationships, the unity of effort. I think the director Easterly is spot on. It is absolutely a team sport. We each have a part to play and if we're all going on full cylinders, you know it's a beautiful world. The problem is, is when one of us starts to kind of get, you know, a little out of sync. But ultimately, we you know, there is hope for the you know, for the win on the defensive side ultimately.

Nahaku McFadden: [00:23:18] Thank you. Thank you, ma'am.

Joe Belford: [00:23:20] Yes. Thank you very much. Thanks.

Nahaku McFadden: [00:23:24] Back to Chris Adams, Reserve and National Guard Magazine. Hello, Chris.

Chris Adams: [00:23:28] Can you hear me? Yes.

Nahaku McFadden: [00:23:30] We can.

Chris Adams: [00:23:31] Okay. I had a mic. Actually, you guys, this is a follow up ask you with infrastructure, because I know that's a focus, but are any of the exercises specifically targeting the cyber shielding efforts maybe in regard to the border infrastructure? Obviously, it's economically significant, among other things. But that's just my question. I don't know if you can explain what those are. To whatever extent it's possible.

Col. Fleming: [00:23:58] I'm sorry. You were a little muffled, to what type of infrastructure?

Chris Adams: [00:24:02] The infrastructure along the border infrastructure? You know, it's commercial, obviously, significance and and other areas of interest, too. But I'm just wondering if any of the exercises throughout the 12 days are specifically targeting cyber shield efforts in pertaining to border infrastructure.

Col. Fleming: [00:24:30] To the, the scenario itself this year is focused on all railroads. Oh, it's a scenario focused on the railroads. Now, the scenario you know, I've always said going in is more of a it's a it's a briefing topic. So it's hey, this is what we're covering this year, but especially even with our

international partners here this year, you know, we're looking at its basic cyber tenants, cyber hygiene, cyber incident response. And those are the tenants of all that. And the basics behind it apply to whatever piece of information technology or operational technology will hit on. So it's not to say we're the experience that they're going to get here is not going to be applicable to any response. We go on. It's just this year, the top level brief happens to be, you know, we're looking at railroad specific.

Chris Adams: [00:25:12] Okay. Thank you.

Nahaku McFadden: [00:25:15] You have a following question, Chris?

Chris Adams: [00:25:17] No, no, I don't. Thank you. Thanks.

Nahaku McFadden: [00:25:21] Okay. And now we're going to KATV Channel seven with Kristin Ballou. Kristin, are you here? Hold on, Kirsten. Okay. If. If you can hear us, just drop something into the chat. Otherwise, we are open to anyone who may have a follow on question. Does anyone like Jaspreet or David or anybody have a follow on? David, you just unmuted yourself. Go ahead.

David Strom: [00:26:05] Hi, everybody, and thanks for the opportunity. I participated as an observer two years ago in Utah and just found it a fascinating event. Could you give us a little bit more details on the logistics? How many Guard's teams from across the country are involved? Are you all going to be in Little Rock this time around? How many state and state separate countries, representatives besides the two guys you have here are and you said they're all on the blue teams, So maybe a little bit of rationale for that.

Col. Fleming: [00:26:39] Yeah. So. So this year we're going to bring, once the exercise is at full capacity and everybody's on ground, we'll have approximately 800 of the world's best cyber professionals here doing Cyber Shield. So as of now, that includes over 36 states that are represented here and teams. We were going to have the territory of Guam join us, but unfortunately with the typhoon, they had to stay home and take care of business there. So that's what we do in the Guard. In addition, the two gentlemen you see here next to me, we have three other foreign partners with us. So a total of five of our closest SPP's are here to, to participate in and sit alongside the blue team. So rationale for the blue team was the experience that behind the state partnership is that partnership and collaborating with your respective states to build that collective an integrated defense that Joe Williams talked about. So keeping them with their blue teams talking, they can get the work together, sit side by side as opposed to potentially go into some of our other work groups where they may not have that, you know, may not be working with their partners depending on those alliance, that's why we wanted to keep them together. And especially this being very first year in recent memory where we're we got them here and are able to actually get them on on keyboard next to us, you know, building towards that unity of partnership to get here as well. So logistically, we got everybody here. So far so good. We're in addition to the military folks, as I mentioned a little bit earlier, we have had close collaboration on partners on ground from the FBI, Homeland Security. FEMA is going to be here a little bit later this week. Our research institutions, Idaho National Labs and Johns Hopkins University, the FBI brought us the operational technology expertise of Siemens.

They were critical in helping us make sure we get the operational technology network right as it really functions and operates so our defenders can get on there and have a real replica of what it looks like when they go to support that. And then from some of our state and local partners, we have folks from the West Virginia State Fusion Center and Ohio Cyber Reserve participating alongside us as well. So it is definitely a teamwork opportunity for everybody here to get together and prepare.

Nahaku McFadden: [00:29:03] Major Barszcz, would you like to add a little bit about what it means for the Polish Cyber Command to participate in your participation?

Maj. Barszcz: [00:29:16] Yes. Thank you. This is the first time we are here. This is our first step in our future collaboration on this field. As for the National Guard, of course, as I mentioned before, this is important for us that the subject of this exercise, our personal technology, industrial control systems. There are now significant risks for ICS that were never a consideration before. So to name a few, worms, various viruses, unauthorized remote accesses, so whole arsenal of toys and tools that adversaries uses. And for us, this is a great opportunity to take a look on your way of thinking how to defend against them. And what is the whole effort that you take to try to stop this kind of struggles or jeopardy? So definitely, this is important to participate for us to take our experience here and apply accordingly when we go home. Thank you.

Nahaku McFadden: [00:30:52] Thank you. And Staff Sergeant Jashari. How about from you in Kosovo Security Forces?

Staff Sgt. Jashari: [00:31:00] Thank you also for Kosovo Security Forces this is of huge importance. I mean, being here and getting all these experiences and let me just mention like 2014, when they started cooperating in this realm of cybersecurity, we were so ignorant of cyber frontier that is exists. But now we have a cyber defense unit and also all the capacities in human capacities and indeed in technology. And with all this culminating with us being here, which is a great thing and hopefully this is not the last time we are here. And guys, this is great.

Nahaku McFadden: [00:31:40] Thank you. David, do you have a follow on?

David Strom: **[**00:31:46] No, I'm good, thanks.

Nahaku McFadden: [00:31:48] Great. Thank you. Kristen, are you, do you have a question? Are you there? TV Channel seven? Okay. Nothing heard. Does anyone else have a follow on question that they would like to ask? Either. Joe?

Joe Belford: [00:32:17] I have a question about Cyber Shield itself. I know it's a fairly long time frame as far as the exercise. Is there any physical component to the Cyber Shield as far as you know? I see everybody in fatigues and stuff, did everybody get up and run five miles this morning? Is there anything at all or is it all just specifically cyber related?

Col. Fleming: [00:32:43] So from a traditional Army exercise standpoint, it's it's it's cyber. Now, we do have access to some outstanding facilities. I know different folks. You know, we stress that cyber is overwhelming. It is a stressful two weeks that we put folks through here. So we do give them a little bit of off time at night so they can do some mental refresh. So there's not a, you know, a traditional brigade run, you know, with flags and lots of cadence calling. But folks do get out and exercise are some good mountains in the areas and various gym classes and things of that nature that they do. But no, there's no whole of exercise, you know, forced physical activity events. And we're not dragging our computers through the trees to crawl into position to type.

Lt. Col. Naylor: [00:33:26] So and unfortunately providing legal advice and counsel is actually not a contact sport.

Nahaku McFadden: [00:33:33] Okay. Thank you, everybody. Do we have anyone else who would like to ask the final question? General Williams, do you have anything that you would like to leave everyone with regarding this Cybershield?

Brig. Gen. Williams: [00:33:59] Absolutely. Always. Yeah. So first and foremost, I'll just say what what you didn't hear from the folks sitting at the table today is just all the effort and and and the immense amount of kind of public servitude that it takes to put on this exercise so that the cyber shield staff, they have a special place in my heart. Not only do you have to be this amazing person that has two jobs, right? Like they have a civilian life, they have a guard life, and then probably a third one. So really, probably three them trying to raise a family. But you throw in another kind of extracurricular activity and that is planning and executing this exercise with an all volunteer staff. Right. And that's really there's a lot of blood, sweat and tears that go into doing something this big and and this great. Right. It really is a phenomenal exercise. So I'll tell you that just my hat's off to the team for all the work and all the and the effort that's gone on to this. I can't thank our our allies and our partners, industry partners and our allies in terms of their participation and their contribution. It's really cultivating ideas from a broad range of experiences and backgrounds that really makes this exercise what it is. And then finally, I'll tell you, no, I can't be a general officer without talking about the speed of trust. Right. And that's a term that we love to throw out there. And I'll tell you that a functional exercise like Cyber Shield is the best way to really build that trust. Resolve is tested, but it's tested in a safe environment that we can really get after things and rehearse, you know, for one of our worst days. So I just want to thank the team. I won't be there with them until this weekend, so I just want to thank them for all the work that they've done up to this point as well as, you know, the massive amount of work that they'll do in executing it. And thank you guys all for listening to our story.

Nahaku McFadden: [00:36:05] Thank you so much, ma'am. Thank you as well. To Colonel Fleming, Lieutenant Colonel Naylor, Major Barszcz , as well as Staff Sergeant Jashari for being here and sharing all about the great things that Cybershield is doing. So thank you. If anyone has any follow on questions, please send that to the National Guard Bureau, Public Affairs media operations team, and we will get back with you as soon as possible with an answer. Thank you. And this concludes our media roundtable on Cyber Shield 2023.