Transcript

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

NATIONAL GUARD ON-THE-RECORD TELEPHONIC MEDIA ROUNDTABLE

JUNE 29, 2021

TOPIC	SUBJECT MATTER EXPERTS
Cyber Shield 2021	▪ Army Gen. Daniel R. Hokanson, Chief, National Guard Bureau ▪ Air Force Maj. Gen. Richard Neely, Adjutant General of Illinois and Master Cyber Space Officer. ▪ Mr. George Battistelli, Exercise Director and Chief of Information Technology Security, Compliance and Readiness Division, G-6, Army National Guard ▪ Army LTC Brad Rhodes, exercise Officer in Charge and Incoming Chief Information Officer for the 76th Operational Response Command, U.S. Army Reserve ▪ Army Chief Warrant Officer 3, Dionysus Griffith, Information Systems Technician, G-6 Cyber Security Response Force, North Carolina Army National Guard ▪ Army Sgt. Tucker Huff, Senior Host Analyst, 175th Cyber Protection Team, 91st Cyber Brigade, Kentucky National Guard

Introduction:

Army General Daniel R. Hokanson, Chief of the National Guard Bureau:

Good morning, everyone, and thank you for the opportunity to talk about the upcoming National Guard Cyber Shield 21 exercise. Cyber incidents are ongoing and substantial threat in 2021 alone, America's power plants, food supply, water supply, health care, law enforcement and defense sectors have all come under attack. These cyber threats extend our adversaries reach across borders and time zones, it could have a devastating consequences. Just last week, Secretary Austin and General Milley testified about the need to add more cybersecurity resources to counter Russian cyber hostilities. That's why exercises like Cyber Shield are so important. The National Guard plays a critical role in the DOD's cyber enterprise. We've also emerged as a trusted and valuable resource in helping our local, state and federal partners defend and mitigate against cyber attacks. Today, there are nearly four-thousand National Guard cyber operators across 40 states during the last presidential election, more than 12 hundred guardsmen and women from 18 states provided IT support, vulnerability assessments, risk mitigation and network monitoring. In addition, we've also seen National Guard cyber partnerships grow in many of our states. For many years, the state of Washington's National Guard has worked with public utility companies to identify gaps in their security. They also worked with the Washington Secretary of State's office to ensure the 2016 and 2020 general elections were secure. As another example, over the past two-years, Louisiana reported 90 attacks on each of their 64 parishes that required cyber support from the Louisiana National Guard. These are just two examples of real world events that benefited from lessons learned, at previous cyber shield exercises. In this cyber shield exercise, the National Guard cyber operators will train to Army and joining for standards, they will test their knowledge of network defenses, forensic analysis, reporting and mitigation and incident response. When our National Guard cyber warriors are called to deter, disrupt and defeat malicious cyber activity, we will be ready. Before I go, I'd like to introduce some of our guard's finest cyber operators, first Major General, Richard Neely, the Illinois Adjutant General, Head of Cyberspace officer. Mr. George Battistelli, the Cyber Shield Exercise director and the Army National Guard's chief of I.T. Security, Compliance and Readiness Division. The Colorado Army National Guard Lt Col Brad Rhodes, exercise officer in charge, and cyber operators Chief Warrant Officer 3, Dionysus Griffith of the North Carolina National Guard, and Sgt. Tucker Huff of the Kentucky National Guard. With that, I'll turn it over to Major General Rich Neely.

Opening Statement:

Major General Richard Neely, Adjutant General of Illinois and Commander of the Illinois National Guard and a Master Cyber Space Officer:

Good morning and thank you all for joining us today. General Hokanson mentioned a few states that been attacked through cyberspace recently. Either state-sponsored or independent cyber criminals have attacked or attempted to attack critical infrastructure in every state.
If I look at my own state of Illinois, just this month the St. Clair County government was attacked by ransomware. In April, the Illinois Attorney General’s computer networks were attacked. And, as you all know, the Illinois Board of Election’s networks were hacked in 2016 and the Illinois National Guard has been working with the Board of Elections in cyber defense since. You may not be aware of most of these event, but you are all aware of the very significant cyberattacks on this countries critical infrastructure that occurred in the last 60 days. The first was the Colonial Pipeline attack that shutdown 45% of the East Coast fuel supply in May. The second attack was on JBS, which supplies 1/5th of our country’s meat. Both attacks threaten our countries wellbeing. Not all attacks require a National Guard response, but as with other domestic emergencies, it is incumbent on the National Guard to be ready in the event that

civilian resources are exhausted. As with other emergencies, it is best not to be trading business cards in the middle of a crises. It is all about planning and training together.

Cyber Shield is special because it integrates all levels of government and utilities, high-tech industry, law enforcement and other partners. It has been described as kind of like a pick-up basketball game where the teams choose their best players, both in the military and outside the military, and brings them along. These military cyber warriors have a significant advantage over their active duty counterparts, as they bring their civilian acquired skills and experience, in addition to their military cyber training. This year's exercise has 14 State Governments, plus Guam involved. It has municipal and county governments, including the City of Tacoma, Washington. It has the Southern Company, the 2nd largest energy utility in the United States. It has the SouthWest Water Company, which operates in six different states. It has The Citadel and Cal Polytech, Microsoft and Dell are involved. While the SANS Institute will be providing training. For the first time ever, 15 of the National Guard's State Partnership countries will get a glimpse into how we train in cyber defensive operations. This includes the Illinois National Guard's partner, Poland. All these organizations did not participate because Mr. Battistelli or Lt. Col. Rhodes – or even General Hokanson - called them up. They came to the table because some of the cyber warriors from the individual states asked them to participate. That gets to the strength of the National Guard as a community-based organization – how we can be the connective tissue between the Department of Defense and, for example, Pleasant Prairie, Wisconsin. This village of about 20,000 people on the Wisconsin/Illinois border doesn't participate in a lot of military exercises, but a representative from this community is participating in Cyber Shield. That happened through local connections between that state's cyber response team and their National Guard cyber warriors, who connected a cyber security expert that works for the village with this national-level military exercise.

In some cases, some of our National Guard cyber warriors work for the organization that is now participating. In the other cases, we are taking advantage of the relationships we've built in states and communities, like Pleasant Prairie. It's said that no problems are solved top down – that the best solutions come from those with hands on and then are implemented across organizations. That is very true of Cyber Shield. The exercise started several years ago with a few cyber warriors getting together to try and fill in some training gaps and it has evolved into the largest unclassified cyber training exercise in the military, with more than 750 participants.

And it continues to evolve each year as the threat evolves.

With that, I'll turn it back to Mr. Wayne Hall, and again, thank you for joining us today.

Wayne Hall [00:10:56] Thank you, sir. We'll move on to Mr. Botticelli, who is the exercise director, sir.

George Battistelli [00:11:04]

Yeah, good morning, everybody, thank you for for joining us. My name is George Battistini. This is my third cyber shield as the exercise director. I've also run the defense of cyber operations for the Army National Guard at the Enterprise. So we inspect all the traffic at the point of entry in the point of demarcation for all the 54 states and territories. And we have the Defense of Cyber Operations mission. One of the unique things that I got to do this year is, as I'm sure everyone is aware of the solar winds supply chain attack that happened. So I was the incident commander and the task force lead for the Army National Guard response to the solar winds incident. And one of the things that that helped us do is we took those lessons learned and injected some realism into cyber shield this year. So the exercise has has continued to evolve based on what is going on in the in the public sector, things that you see in the news. And we continue to make sure that we're evolving and training our defense cyber operation elements so that they're able to respond, whether it be on a state active duty mission or a mission on the Department of Defense Information Network, that they have the same tool sets, that they have standardized training. And that's really the goodness of cyber shield because the states get to coordinate, communicate, meet and greet with their their fellow DCEOs, defensive cyber operation elements, incident responders from the other states. They get to continue to build that network. Last year, we were a little bit handicapped by the covid-19 pandemic because we had to go fully virtual. We pivoted three different times and then we figured out that we could do a virtual exercise. Now, with the virtual exercise, you do lose some of that goodness of the in-person. But we're starting to now get better from from covid. People are getting vaccinated. We're starting to get back together this year. We have a hybrid event. We look forward to next year being a fully in-person event. But I think we have a really good exercise plan. We're getting after some significant mission, essential tasks. And I really appreciate everyone being here today. And I look forward to answer any questions you might have about the exercise or our Solar Winds incident response. And with that, I'll pass it over to Lieutenant Colonel Brad Rhodes, the OIC for Cyber Shield 21.

Lt Col Rhodes [00:13:23]

Awesome, thanks, George. Good morning, everyone. It's nice to be here and see all of all of you today. So Cyber Shield is an amazing exercise. I've been in the Colorado Guard in the Army for about twenty four years. I'm a cyber warfare officer, which makes it interesting. And, you know, multiple combat deployments, the whole nine yards. It is probably the most fun that I have had in the military is the opportunity to lead Cyber Shield. Cyber Shield brings together a volunteer staff of 50 plus folks from across the fifty four states and territories. Truly a national effort to put this exercise together. They spend time outside of the normal drills, normal annual training that we do. They spend a lot of their own time developing the construct of the scenario that we're going to deliver this year. Really, really amazing, amazing stuff. Cyber Shield is about training as we fight. And so that's an old adage in the military. If you don't train as you fight, you don't know how you're going to actually perform in a fight. And so what we do at Cyber Shield that is really unique is we bring an absolutely world class opposing force. So a red team that is actually actively engaging our blue teams on the persistent cyber training environment. That's our record. That's the program of record of range for the for the military that we're operating on this year. Obviously, as George mentioned, we like to bring in the realism, we call it sort of ripped from the headlines when we designed this exercise. We look at what's happening out there right now in cyberspace, in the world, and we say, what can we bring to the exercise that will get our soldiers, airmen, the joint forces that participate in cyber shield every year and our mission partners? That's really important. How do we give them a realistic event that helps them to understand what's directly in front of them right now? So Cyber Shield provides that touching on the fact that cyber shield is unclassified. We could not bring the large amount of mission partners from across state, local, local tribal, territorial governments, academia, industry partners, critical infrastructure providers. As Major General Neely mentioned, we couldn't do that if this exercise is not unclassified. So that gives us a huge advantage to be able to interact with those partners and help in terms of getting their understanding and building those relationships. What I like to say is left of boom, left of that incident, because you don't want to be trying to figure out who's in the room left of incident back in 2018, I was part of the Colorado Department of Transportation incident response where we addressed the Sam Sam ransomware attack on that organization. And because of the exercises that we did in the guard with those mission, with many of those mission partners that were in the room with this from the Office of Information Technology in Colorado to Sedot to some of the academic partners that help with that response. We knew everybody walking in the door. And so that instant trust there that you engender with being a guardsman, living and working in the local community, in many cases working for the organizations that we were helping, really helped us to get a feel for that response and to address those issues faster than if we had been walking into a cold. So really great opportunity there at Cyber Shield. And last I'll touch on before I pass it back over to Wayne is the integration of the state partner programs countries? That is amazing. We're doing that for the first time this year at kind of a good scale. We're doing it virtually, which is going to be interesting, but are as part of the support that we do from the DOD perspective to our foreign partners and our foreign allies, this is absolutely essential. Our foreign partners and allies are facing the exact same threats that we see in the United States. And in some cases, they're much closer to the threats than we are. And so helping them to understand how to build one of these training events and how to actually train and interact with their own mission partners is really essential to what we're doing here at Cyber Shield. So, Wayne, I'll pass it back over to you.

Wayne Hall [00:17:37] Thank you very much for that great introduction. I'm going to pass it on to Chief Warrant Officer 3 Dionysus Griffith. Hope I didn't mess it up. Chief, are you there?

Lt Col Rhodes [00:17:59] I think he might have dropped off I'll ping him.

Wayne Hall [00:18:01] OK, so I will pass on to Sergeant Tucker Huff.

Sgt Tucker Huff [00:18:09] Thank you, Mr. Hall. Good morning, everyone. I am Sergeant Tucker Huff of the Kentucky Army National Guard. I've been a guard member for roughly eight years. I am the senior host analyst for the 175 cyber protection team and the 91st Cyber Brigade. And I'll pass it back to you, Mr. Hall.

Wayne Hall [00:18:26]

OK, thank you. We'll catch up. Chief Warrant Officer Griffith, if he is able to rejoin us. All right. To the members of the media joined to thank you for joining us today. I'd like to ask that all members of the media, when you when you ask a question, please state your name affiliation for clarity for the group. Be respectful, being respectful of time. We will start off with allowing reporters to ask a question and a follow up. If we have more time, we'll circle back. I will go through the list as best I can. If you have a question I haven't called on you, please feel free to put a note in the chatroom. So you have a question. And if you were not able to answer a question on the round table, we'll do our best to try to get back to you with an answer. With that, I'd like to start with Courtney Kube from NBC. Are you with us? And you have a question?

Courtney Kube NBC [00:19:17]

I am here. Thank you. I'm sorry. I think it was the maybe the second person I dialed in a minute or two late who was involved in the solar WINPAC. Is it Mr. Mr. Battistelli? Yes, that is. Sorry. I'm wondering if you could just tell us a little bit more about your involvement in that. And and specifically, I'm interested in how you said that you're trying to take some real world examples like how are you applying what you saw and learned from solar winds to this exercise and then to larger cybersecurity?

George Battistelli [00:19:54]

Yeah, absolutely, I can take that one, Courtney. So I think what you were asking for is the lessons learned that we got from the solar winds compromise, right. So well-known in the news that it was a supply chain compromise where a certain version of the software was compromised. But one of the things that we use that for specifically as we relate to the cyber shield exercise, is that it helps us in our training when we have one of these events. Right. So you start to understand where you have gaps in your data analysis. You start to understand where you have gaps in your tool sets. Right. So as we send our teams on what happens if they're unable to to see the health of the network, when they get on the network, they have to have secondary courses of action as to what tools they can use to begin to determine what the health of the network is. From a National Guard Bureau perspective, we had to determine which troops we had to task, who we could pull to support those efforts from a national level. And then we had to determine what kind of skill set that they had. And so Cyber Shield really now has given us the ability to make sure that everybody is standardized on their toolset so that if I call out to the brigade or I call out to a state to activate their defensive cyber operation element, we understand that they all are trained to the same level and then standardizing the tool sets in the tool access. Right. So during the Cyber Shield excuse me, during the solar winds event, we realized that we did not have the right accesses for the right people at the right time. So those are some of the lessons learned that we took from the solar winds incident. Right. And we mapped it to Cyber Shield because at the end of the day, solar winds showed us that we can't rely on a single tool to monitor the health of our network devices. And so we've started to to implement alternate courses of action so we don't have all of our eggs in one basket and we're making sure that we train the force in that way also over.

Wayne Hall [00:21:57]

Thank you. Sorry, go ahead. You have heard of Courtney.

Courtney Kube NBC [00:22:01]

Just a very quick one, can you just explain what you mean when you said that making sure everyone had the accesses what was the breakdown there that you uncovered?

George Battistelli [00:22:13]

Yeah, absolutely. So from the the Army National Guard enterprise perspective, we run an enterprise network. And when you have incident responders, they may not work with the security tool sets that we're working with at the Enterprise every day. And so when we bring in extra help, we need to make sure that we're giving them access to the right tool sets and the right level of access to those tool sets. So if I bring on somebody, for example, from the state and they don't have the ability to to look at the security events that are coming across, then they can't be helpful and they can't be fully engaged in the mission. They're not fully mission capable until we get them the right access to the right tool sets so that they can use those tool sets and get the right information over.

Courtney Kube NBC [00:22:57]

Thank you. Thanks, Wayne.

Wayne Hall [00:22:58]

Thanks, Courtney. OK, so let's go to Ellie. Eleanor Watson from CBS News. Ellie are you with us?

Eleanor Watson CBS [00:23:08]

I'm here to thank you guys for doing this. Just a quick one. I am trying to get a handle on how often the guard is being called on to respond to these things because we don't learn about all of them. Do you have an estimate of how many times maybe in a month the National Guard has to respond to? These types of security incidents.

Wayne Hall [00:23:32]

General Neely, I'll let you see if you can take a crack at that.

Maj Gen Neely [00:23:38]

Well, I will take a crack at it, I do not have the data in front of me and what we can do is circle back with our one of our team members at National Guard Bureau to come up with that data. But, I would estimate across the country a couple of times a month we're getting responses. You know, I spoke to in my opening comments about both our attorney general before, as well as our secretary as well as our one of our counties that had an issue. And what we found is that most of those cases, the guard was advised and what we talk about, those partnerships were very locked into at the local level with the incident response team and the National Guard's advise. And sometimes we may be consulted for questions in that. And then if the events significant enough will actually roll out and support that particular event, either over the shoulder or virtually. But it really depends. I think what we've all seen across the last six months, Mr. Battistelli talked about the solar winds hacked, which happened in December, followed by a major attack on the Microsoft Exchange in January that was well publicized. I talked about two major critical infrastructure attacks. So these attacks and particularly ransomware are increasing very significantly over a month, over month. And so what we're starting to see is more, I think, issues arising across our country, particularly as ransomware becomes more prevalent. And Lt. Col. Rhodes spoke to that a little bit in his comments when he was talking about responding to a ransomware event. So I don't know if we Lt.Col. Rhodes had anything additional or if that answers your question.

Lt Col Rhodes [00:25:41]

No, I can add a couple of things here. So, you know, one of the unique pieces of our union is that we're 54 states and territories. And so each of the states utilizes the guard a little bit differently. In Colorado, for example, we tend to be very proactive. We're out there. We do annual exercises with mission partners to build those relationships left of boom so that we have an opportunity if something does arise, that we can do that over the last every single election cycle. For the last five, six years now, we've been in the room with our secretary of state, helping to monitor, helping to advise, helping to look at that. Thankfully, we didn't see anything like that this year. So that was that was definitely positive. But part of that part of what it is, is, again, every state is a little different. Every state utilizes the guard a little differently. But I will tell you that every single state and territory is plumbed with cyber operators to go out there and actually support when needed. And I think that's very, very important. And part of what we do at Cyber Shield is a level set that training. We bring all of these teams in, we assess them, we provide them pointers as they walk out the door, says here's things you need to work on to continue to improve so that over time we get to a solid 100 percent readiness across the board for the 54 states and territories.

Wayne Hall [00:27:03]

Sir, thank you. I'd like to pass this over to Chief Griffith, who's operator assignment operator out of North Carolina at his perspective a little bit on what a response in his state looks like and then see if there's anything that certain can add up to that.

Chief Griffith, can you please introduce yourself to the group and then please try to talk about how a response unfolds to North Carolina.

CW3 Dionysus Griffith [00:27:28]

Good afternoon, everyone. Chief Griffith with North Carolina National Guard G6 Security response force for a response that's our side deals with a lot of the civilian agencies, contacting the liaison in our state we are tied in with and we go through several challenges. So initially sending out a couple of personnel maybe to see a team lead to get a response person to see what exactly happened, maybe tracked down how it happened. And depending on how serious the incident is, the additional personnel to do some training or a small triage and then of responses, how do we move forward and building and better securing their network infrastructure.

Wayne Hall [00:28:18]

Thank you, Sgt. Huff, can you provide anything from the Kentucky perspective?

Sgt Tucker Huff [00:28:23]

So Kentucky is beginning their relationships with the local state governments and our mission partners. So we are in that first stages of how we can be integrated or embedded to assist those people that need those training or whether the validation exercises or whatever they may need. Back to you, Mr. Hall.

Wayne Hall [00:28:43]

Thank you. Ellie, did you have a follow up or are you OK?

Eleanor Watson CBS [00:28:47]

I'm good. That was great. Thank you.

Wayne Hall [00:28:49]

Thank you, Steve Beynon, are you on the phone?

Steve Beynon, Military.com [00:28:53] Yeah. Hey, yeah. Can you hear me?

Wayne Hall [00:28:55] Yes.

Steve Beynon, Military.com [00:28:56] Awesome. Thanks. Real real quick. I don't know if this might be a question for Colonel Rhodes or anyone else can join in. If you can kind of paint me a picture of what this is in the big picture, is this sort of the cyber equivalent of NTC? And then if you can kind of go into a little bit about what the OP floor is actually doing, maybe specific scenarios, things that they're actually going to be training on.

Lt Col Rhodes [00:29:21] Sure, Steve. Happy to do that. So cyber is akin to NTC. So that's a really good analogy. These teams train all year. We actually provide them with pre training events that they can do. So they should they have the time again, a lot of it. Again, 54 states and territories, they build their own training plans. They do that stuff. But we do provide them the opportunity to get on range and do some of that free training. And then they come to NTC, if you will, cyber shield, and they go through a standardized set of training. So we provide during our training week, we provide them 85 sets of DOD8570-8140. That's the regulation that says what professional certifications and training soldiers had and the joint services have to have to operate on Dotan. So we provide some of that. We provide some technical training. But if they've completed those tasks, there's a lot of things we do in joint-training. During exercise week we bring in both our defensive cyber operations elements. So that's what exists in each of the 54 states and territories. Those are eight to ten person elements. And then we also have our cyber protection teams that are all up in our 91 cyber brigade. And so they come along as well. And so our DCOE's are in a scenario where they are doing an advise and assist mission to an area of critical infrastructure. This year our scenario is focused on in a civilian company that is polluting water in a town and they that pollution is being caused by a cyber attack against my OP floor. And so they come in there. The OP floor has been in that network. They are in that network and they're continuing to attack in that work and give and give the blue teams are so our maneuver elements, our defensive cyber ops elements and CBTs things to find artifacts to discover, try to stop them in the sense of the attack. Right. Working with those mission partners. And that's really key here. Just because our maneuver elements actually catch the OP floor guys in the act, it doesn't mean that they can just stop something. They have to work with that mission partner who owns that network to say, hey, here's what we found, here's some recommended changes. How do we do that and continue to operate and do the production environment? Do not break a bunch of stuff, but our OP floor will do Web based attacks. They will do network based attacks. They'll do host based attacks that we give them. We give the OP floor carte blanche to do whatever they need to to get that point across to deliver those in line cyber effects so that our maneuver elements can actually see the attacks and then learn what those look like. So when they go back to not only their National Guard jobs, but to their civilian jobs, they're actually much better trained than they were when they got to us at Cyber Shield. That answers your question.

Steve Beynon, Military.com [00:32:06]

Yeah, I've seen it.

Steve Beynon, Military.com [00:32:07]

This is almost equivalent to a platoon like Live Fire or something like that. What's a general time a whole scenario would take?

Lt Col Rhodes [00:32:17]

Absolutely. So, yeah, it is. It's kind of like platoon live fire. That's a good analogy. So that's the scenario. The exercise week runs for a week and it builds on itself. So the team walks in the door. They figure out the lay of the land. They work with the mission partner. They figure out how broken the network is. At the same time, the OP forces in the background doing their stuff. And then we have a number of, well we dont want to give way too much because I'm sure they'll be some some of my operators out there in the maneuver, elements that are going to look at for clues. Right. The answers to the questions for the scenario. And so they get the opportunity to see a number of very advanced attacks by the OP floor and to try to catch them and then ultimately try to figure out how would they stop set attacks from happening. The OP floor is going to have multiple vectors into the broken network. In the case of what we're talking about for the scenario. And so it's going to be very hard to get them out. And that's the whole goal, because once attackers get into these networks today, they hang out. They persist as long as they possibly can. And that's what my OP floor does.

Steve Beynon, Military.com [00:33:19]

Great. Just a clarification. I think someone said it was 750 troops involved. Is that a combination of army and air?

Lt. Col. Rhodes [00:33:25]

So that is a good question. So that's actually we're very joint this year. We have a combination of Army Guard, Air Guard, Coast Guard, Navy, some active component folks and obviously our civilian mission partners. So it's a large, very, very joint flavor of the exercise this year.

George Battistelli [00:33:45]

Hey, Brad, really, really quick. I can just give one comment on that, too, so when we talk about the realism, this is the realism, right? So a defensive cyber operation element responding to a state active duty or a mission on the Department of Defense Information Network if they're responding, the expectation is that the adversary, our peer near peer, has already compromised that. And they're walking into a compromised situation. And that's where we inject the realism because they are walking into an environment that is, you know, potentially compromised, known, compromised, and they need to work backwards from there.

Wayne Hall [00:34:23]

All right, very good. Thank you. So Bianca from Reserve and National Guard magazine or you online, you have a question?

Bianca Strzalkowski, Reserve & National Guard Magazine [00:34:33]

Yes, I am. What challenges exist in moving this exercise virtually?

Wayne Hall [00:34:42]

I think Mr. Botticelli, I think you mentioned students having experienced last year in this.

George Battistelli [00:34:49]

Yeah, I can I can start and then Lieutenant Colonel Rhodes can certainly shore up any cracks that I miss. But I appreciate that question. So certainly last year, a lot of uncertainty right. In the early stages of covid, I think we pivoted three different times. We were going to be at Camp Williams, Utah, and then we pivoted to Camp Atterbury and then we pivoted to San Luis Obispo and then finally online. And each time was a little bit different.

Right, because we were trying to get to the point where can we do 100 percent? Can we do 80 percent? Can we do 50 percent? We went to the Microsoft team's commercial virtual remote environment, the CVR environment this year. The CVR, as everybody knows, went away on June 15th. So that helped us even more in our planning because we started off on a version of Microsoft teams that any of the soldiers or the traditional soldiers could get on their phone. And so now we've moved to the A365 environment where, you know, they have to have a GFE or a CAC. And so it's made it a little bit more difficult. And so we've had some some significant challenges there. As a matter of fact, we are still using a team's environment, but a a hybrid environment for the exercise because we're actually doing our DVD on Cisco WebEx. So it's not a a one size fits all solution, but we really are trying to to get to the point where we can all get back together because virtual works. But you don't get that that person working together. So with that being said, I'll pass it to to Colonel Brad Rhoades now.

Lt. Col. Rhodes [00:36:28]

Thanks, George. No, the virtual environment is challenging. You know, it's in the room, right? Whether you're in the room together, I can look around the room and see who's reacting to certain things and that kind of thing. And depending on where soldiers participate from and we've done our entire planning of this event virtual. The first time that we're going to actually get back together with at least a portion of the staff to execute the exercise is, is when we go out to Utah next week to start getting things set up to actually go. And so it's going to be great to see everybody, but it's definitely challenging because, again, you don't necessarily get the interaction and the feedback that nonverbal communications that you see elsewhere. Right. The good news is, we have a pretty close and tight knit group of planners here and guard cyber that have put this thing together that once we pivoted from, you know, to virtual last year and then we pretty much got told you're going to conduct your entire planning cycle for this exercise virtual. We all sort of got used to it. I literally conducted because of covid-19. I literally did every single planning conference from the comfort of my home offices, which where I'm sitting at today. So that was that was kind of nice. And, you know, folks like to see my cats when they come to visit. They've been booted out for this discussion. But I'd actually like to ask Deon to jump in on this, because Deon's one of my planners on the forensic side of the House. And Deum, what was your experience with the virtual thing? Was it good? Was it bad? You know, are you excited to get back in person next year? What do you thinking.

CW3 Dionysus Griffith [00:37:59] I would definitely good about being able to work from home and still be able to accomplish things, but I look forward to going out and actually being around in relationships with other states and other partners.

Lt. Col. Rhodes [00:38:11] Awesome. Wayne, back to you.

Wayne Hall [00:38:13] Thank you, did you have a follow up or are you good Bianca?

Bianca Strzalkowski, Reserve & National Guard Magazine [00:38:18]
My only other follow up, in addition to cyber operators, what other sort of billets are involved in this?

George Battistelli [00:38:26]

There's there's a lot Bianca, I'll turn that one to to Brad Rhodes, because Brad will be able to tell you better. But I mean, we've got IO, we've we've got the entire gamut because, again, this is the largest unclassified cyber exercise in the Department of Defense. And it doesn't take place without... Let me foot stop really quick, an all volunteer workforce. Right. So everybody is doing this in addition to whatever position they're currently doing the M-Day soldiers. But there's a lot, Brad, if you want to go through some of them.

Lt. Col. Rhodes [00:38:59]

Absolutely, George. I mean, we have an entire what we call a joint staff. So we have personnel, intel, operations, logistics, all of that. We have we have an entire training cell which is put together an awesome training plan for this week or for this coming two weeks from now. We have a white cell so akin to NTC, right. We have a white cell that has done the bulk of the exercise planning scenario, the range development and builds. We have a legal team. We have our opposing force. We have our assessments team. We have awesome help desk team that's going to help everybody that has issues. We obviously have our maneuver elements spread across. So we've got 30 plus blue teams out there doing amazing work across the 54 states and territories. And then the one thing that George touched on that I do want to highlight is the fact that we do bring in information operations to this. So, on range, we actually have social media platforms and we allow our information operations folks to come in, developed personas and interact and provide that what we like, what I like call the the cyber of the fog of cyber war. When we get out into the actual operational environment, we've seen a lot of things when it comes to disinformation and misinformation and influence operations conducted by actors outside of the United States and in the United States. And so we actually simulate and deliver that so that confusion, if you will, as to who's them, who you who you should be paying attention to as a voice out in cyberspace versus who you shouldn't. We provide that to the blue teams that adds that sort of multi domain operations flavor to the operation. And next year, we're looking to bring in some of the electronic warfare capabilities. So we have a lot of moving pieces and parts that George mentioned within the exercise.

George Battistelli [00:40:41] I'd also add on to that really quick is that we also have legal on staff with us as well, because as you get into cyber right and whether it's a response or an activity, we've got to make sure that we're staying within the authorities and we're doing everything legally. And it gives the legal personnel the ability to practice and to vet and to really sharpen their skills as well. And so we bring everybody together so that when we have this next solar winds or next cyber event that everybody has read it and everybody knows what we're supposed to do. And I think that's very important.

Wayne Hall [00:41:21] All right. Thank you both. So. Sophia from Bloomberg, are you online, do you have a question?

Sophia Cai, Bloomberg News [00:41:33] Can you guys hear me?

Wayne Hall [00:41:34] Yes, we're here. We're hear you just fine.

Sophia Cai, Bloomberg News [00:41:40] I was wondering, I mean, I guess this is another question for Mr. Battistini. And it's not directly related to the training, but I wonder if you have any insight into whether any tax data at the IRS might have been access and if we will ever know what was taken because of the lack of logging?

George Battistelli [00:42:11]

So that would not be something that I would have specific purview on at the Army National Guard because I do not monitor the tax networks, so that would be something that, you know, would be monitored by another entity. So everything that I have under my purview are the Army National Guard networks, portion of the Department of Defense Information Network. And so I don't have the answer to that question over.

Wayne Hall [00:42:38]

Yes, Sophie, we we're solely focused here on the guard networks, the DOD network that the guard monitors and manages maintains. So that question is probably best addressed to DHS or the IRS themselves. Do you have anything specifically related to Cyber Shield?

Sophia Cai, Bloomberg News [00:42:58]

Yes, could you just repeat, and I think the first someone from the NBC asked this question, but what your specific role was in the Solarwinds response?

George Battistelli [00:43:17]

Yeah, for sure. So my role in the solar wind's response as I was the task force incident commander, so I quarterbacked the Army National Guard response to the solar winds event. And so it was trying to determine whether we had a compromise across all the 54 states and territories, trying to determine what version of solar winds that the states were on. Because if you remember back, there was only certain versions of the Orion software that was thought to be compromised or known to be compromised, and then making sure that we had those devices offline, sending forensics if needed. And I will say that the Army National Guard did not experience a single compromise from the solar winds event. So we had no compromises associated with it. But it did help us to standardize our data sets. Right. What we are capturing, what data we should be capturing, which tools we should be using, standardize our training. And a lot of that has gone into cyber shield this year. So when solar winds number two happens, we'll we'll be ready and we'll be there over.

Sophia Cai, Bloomberg News [00:44:42]

Thank you. Wayne, I think you're still muted.

Wayne Hall [00:44:45]

Sorry about that. We will move on to Dave Dahl from WTX radio, understand you have a question Sir. Are you there, Mr. Dahl? OK, moving on, MSgt. Erich Smith, I understand you have a question.

MSgt Erich Smith [00:45:10]

Master Sergeant Erich Smith, National Guard Bureau, Public Affairs. This question is for Sergeant Huff. Sorry, Sergeant. If we're going to put you on the spot here, I reviewed your background, obviously very impressive, but still, even given your background and all the amazing things you've done on the civilian side and of course, with the Army Guard, is there anything that you hope to take away from this exercise in particular?

Sgt Tucker Huff [00:45:38]

Yes, MSgt. Smith, I hope to keep building on my skills, I always when you start to develop your SOPs or your battle drills, you cant always use the same steps with each event or each incident. You always have to adapt and overcome. We are also placed on different teams with different individuals, probably from different states. And they also do not have the same steps that we take. So learning how to integrate well with their mission partners, other National Guard units, local, state authorities, it's more of a learning experience. Always keep your toes and it bonds my experience level so I could offer more to the table with each passing year.

Gen. Hokanson [00:46:19]

Thank you very much. And, of course, the civilian media, SOPs: standard operating procedures. Thank you,

Sgt Tucker Huff [00:46:27]

Thank you, MSgt.

Wayne Hall [00:46:28]

Thank you. I think Mr. Dahl had a problem coming off mute, so I'll ask his question on his behalf. Mr. Dahl with WTX Radio in Springfield, Illinois. His question is for General Neely. It seems as if the bad guys and the good guys are neck and neck in this constantly with one step ahead of the other. Is that right? And will this ever change or end? Sir, would you like to address that?

Maj Gen Neely [00:46:53]

No, absolutely love to. Thanks, Dave, for the question and thanks for joining us today, as we talked earlier about all the support that has to occur with Cyber Shield. I think one good example is our public affairs. And Col. Brad Layten's here with me helps over the last five or six years support cyber shield. So it's really a team effort to really appreciate all the supporters of the operators. Today's question, yes. You know, cyber continues to leapfrog each other. And look we've talked a lot today about even Sergeant Huff just referred to changing the standard operating procedures. We cannot rely on the procedures that we had even six or eight months ago and their processes and take those for granted that that's going to keep the bad guys out. And what we saw with the solar winds attack and really even going back to 2016 when we saw the attacks on the election system, at that point, many people would say, why would why would anybody attack an election system that way or why are we really concerned? It was even considered piece of critical infrastructure when it was initially attacked. And today it is because we had to change our processes and procedures. And as technology changes, we these cyber very loosely, but as technology changes and we see things like artificial intelligence, quantum computing and many of these 5G and all these other new autonomous vehicles, all these new things are going to open up the aperture for additional attacks. We live in an IP based society, which means we have a lot of conveniences with things like refrigerators, with cameras in it, and Wi-Fi enabled everything. But those products also bring vulnerabilities because of cybersecurity issues. And so we'll constantly be, I think, working through this as we continue to look for the better way to build the mousetrap and protect, protect our country. And that's a great thing about Cyber Shield, is we'll bring in new techniques and new approaches to deal with these issues, much like we did, much like the lessons learned from the smaller ones attack that Mr Beazley spoke of. Hope that helps.

Wayne Hall [00:49:14]

All right, sir, thank you. Want to go next to Ryan Morgan from American Military News. Are you online? Do you have a question?

Ryan Morgan, American Military News [00:49:29]

No question at this time, I appreciate it.

Wayne Hall [00:49:32]

All right, thank you, Sir. David Strom from CSO. Are you online and do you have a question? Nothing heard will go to NBC five Chicago, are you online, do you have a question? Nothing heard Josh Norwood, are you online and do you have a question?

Josh Norwood [00:50:02]

I am on the line, but no questions.

Wayne Hall [00:50:05]

All right, thank you. All right. Is there anybody in the group that we that has a question for the panel?

MSgt Erich Smith [00:50:13]

I have one more question, Mr. Hall. That's OK,.

Wayne Hall [00:50:15]

That's fine.

MSgt Erich Smith [00:50:18]

Again, this is MSgt Erich Smith here NGB public affairs. So obviously, Sergeant, you're more embedded in the cyber trenches, if you will, and you have a greater pulse on all of this being, what, next year, battle buddies and so forth. So I'm just kind of curious, what is it besides having the aptitude for this? What is it about cyberspace that you really find engrossing? And what is some of your battle buddies tell you what they find interesting about cyberspace as well.

Sgt Tucker Huff [00:50:56]

Yes, Master Sergeant, this is Sergeant Tucker Huff. It's always the learning that you have like everything you think you always know everything about everything or you want to know. And it's always changing, wanting to be the tools, whether it be developing their own tools, the networking, the experiences, being able to feel like I'm going above and beyond my call of duty where I first came in and I was during the 9/11 attacks, then I was like, well, I'm here to defend my country, but here I am.

I'm helping defend the domestic front, even when it comes to other local state authorities or even other civilian companies. I'm going above and beyond. I'm doing what I'm doing, a more personable effect where, you know, they get to interface with me directly. I get to travel more of the United States. I get to see different teams. I get to learn how they think. It's just. Different from just being in a regular unit. I come from a signal unit and most people don't know your name when you're going out on a mission. And here I get to be able to showcase what I know and I get to gain more from others.

MSgt Erich Smith [00:52:11]

Thank you.

Wayne Hall [00:52:13]

Thank you. I actually Ryan Morgan just put a message in the group text. I think we've addressed this, but he may have missed it earlier. This is probably for Colonel Rhodes, or Mr. Botticelli, he's asking about the scenario for cyber shield, how we describe the scenario and it will be something similar to the pipeline attack. Can you can you reiterate on that, sir?

Lt Col Rhodes [00:52:42]

Absolutely. So, yes. So the scenario this year is we have our elements. So that's our defensive cyber operations elements. There's one of those in each of the 54 states and territories. And we also have along for the ride the Navy, Coast Guard teams. Those are cyber protection teams. We also have National Guard and Air National Guard cyber protection teams in the mix. And so the scenario that's going to be in front of them is they are going to be responding to a civilian organization. So truly a commercial organization, an entity that is causing pollution to a water system, to the water system, waterways in a town. They believe that is being caused by a cyber actor. In fact, it is. And so and that cyber actor is alive and in the network when the teams arrive. And what they're going to discover is that the network is is very, very broken. We are doing a traditional incident response. And so previous years in Cyber Shield, we've created a we'll call it a discovery learning opportunity for the teams this year. There's less discovery learning. It's we're telling them when they walk in the door, the network is broken. You've got to figure out what happened to the network, how it got broken and do that traditional, like I said, incident response and walk all of those steps that we do. It is, as Mr. Botticelli mentioned, we are bringing in elements of solar winds. So part of that is access to the logging and understanding and being able to hunt through and look at the logs to discover what happened. So that's part of it. And then not directly related to Colonial Pipeline, but again, a large chunk of this network is what we saw with Colonial Pipeline, which was the administrative network. That was where the incursion occurred, at least from the reporting that I've seen. And then everything else was then shut down out of an abundance of caution to make sure that the actors had not moved laterally or pivoted across the network into the industrial control systems. So we have a very similar setup in our network for the blue teams. This is typically what we do every year. We introduced Skata and Industrial Control Systems about four years ago now because that is a huge part of what we see out there. We see that you see Skata industrial control system integration across not only the critical infrastructure areas as specified by DHS, but you see it in building systems, the whole nine yards all across the board, we see this intersection of Skada, ICS, Internet of Things, and we have to understand what that looks like. And so that is truly a part of what we do at Cyber Shield is very similar to that construct. Hopefully that answers your question.

Wayne Hall [00:55:20]

Thank you, sir. Briefly, I'd like to be following up on Sergeant Smith's last question, like the pitch back to chief. The Chief Griffith, and ask if you could offer some of your personal perspectives as a cyber operator, what operating and what doing this job in the guard really means to you and how it shaped you, your military career?

CW3 Dionysus Griffith [00:55:47]

This is Chief Griffith. So for me, it's kind of something that's more than just on a day to day life in the country is more local to your state and with people that you see everyday in your community, helping protect them on the IT front. That's really it, just make sure everybody's safe domestic side here and to our states, the individual states.

Wayne Hall [00:56:18]

All right, thank you, sir. All right, I believe that's just about all the time we have, unless there's one last question from anybody, give a minute to see if anybody has one last question. All right, nothing heard. So before we leave, I'd like to I'd like to ask General Neeley, do you have anything else you'd like to provide with a little leave the group with today?

Maj Gen Neely [00:56:48]

But just again, thank everybody for taking the time to join us. This is a very important exercise and I think based on the questions that came today, I think all of you understand the significance of cyber and cyber cyberspace in our in our society today. We continue to watch the evolution. And I speak on this topic on a regular basis. And I like to sometimes talk about Pearl Harbor and what that meant to us and the development of the Space Force and what that development meant to space and how that changes in. And we're seeing an evolution in cyber right now that we're living in some days that are very unique. And most of society doesn't understand it because they may not live in this technology realm. But what we're doing is we're seeing an acceleration of risk and attacks that are coming forward. And so it's it's very important for us to exercise and train plan, as we talked about across our nation, because these attacks wont occur in big places. They will occur in small places across the nation, and it'll be small places that will affect larger and larger ways of our lives. So it's this is another example of where the National Guard, again, is community based. We're working closely with our employers, bringing unique skill sets together that we bring from industry, from people like Lieutenant Colonel Rhodes, who is a tech expert from industry that brings his special capabilities back to the military and helps lead events like this is a great example of of our citizen soldiers and airmen and what the great things they are doing. So, again, appreciate everybody's participation today. And we look forward to talking more during the exercise and there'll be more updates coming along. So thank you.

Wayne Hall [00:58:45]

Thank you, sir. I appreciate it. Just got a note, Mr. Battistelli would like to add something as well.

George Battistelli [00:58:53]

Yeah, I appreciate it first. I appreciate everybody being on, but I just want to reiterate the thing that is different about the Army National Guard, specifically when we have the cyber shield effort really and a lot of these things, the rank is inconsequential because we bring people in. I think we have a staff sergeant running our our red team. And frankly, it's because he's amazing. Right. And so you have very, very talented soldiers. And then we have the whole dual status. Right. So when we had the solar winds task force and I brought in Lieutenant Colonel Brad Rhodes, Brad Rhodes was feeding us information and then I was feeding him information. But guess what? He was still working also in his civilian capacity. So when he went back to a civilian capacity, he had information that he could share back and forth, obviously from an unclassified opportunity. But that is the goodness of the guard when we bring in those subject matter experts that have the ability to work back and forth every single day between industry and military, and they really bridge those relationships. So that's what we get from Cyber Shield that's different from any other event, because we have a collective of some of the sharpest minds in the Army National Guard where rank is inconsequential, skill is the defining factor, over.

Wayne Hall [01:00:11]

Thank you, sir. And with that, ladies and gentlemen, I'd like to remind everybody had placed in the chat. Lieutenant Colonel Bradley is the public affairs officer for Cyber Shield. His contact information is in the box. It's the cell is 217-725-2265, and he can be reached by email at Bradford.E.Leighton.mil@mail.mil. He'll be very happy to accommodate any requests that he can for as far as coverage of the actual exercise or assist with additional questions related to the exercise. If you have any other questions for us, you can reach us by email as well. Thank you all for your time and your your your effort to help us communicate the significance of Cyber Shield 2021.

[End of Audio]

Duration: 1-hour 00-minutes

For information regarding this transcript, please send an email to the National Guard Bureau Media Operations desk at ng.ncr.ngb-arng.mesg.ngb-media-desk-owner@mail.mil.

-30-