Ep. 33: It's a big cyber world out there

Welcome to Sword and Shield, the official podcast of the 960th Cyberspace Wing. Join us for insight, knowledge, mentorship and some fun, as we discuss relevant topics in and around our wing. Please understand that the views expressed in this podcast are not necessarily the views of the U. S. Air Force, nor the Air Force Reserve, and no endorsement of any particular person or business is ever intended. (Light music)

Welcome back to the "Sword and Shield" podcast. I'm Colonel Rick Erredge, 960th Cyberspace Wing Commander. Today, I'm joined with... - Chief Master Sergeant Chris Howard, 960th Cyberspace Operations Group Superintendent. - Welcome back, Chief. - Thank you, Sir. I appreciate you taking the time and let me sit down and talk with you today. - Yeah, so I think today's going to be an interesting discussion, lotta stuff going on in our world right now, that's timely. We just had the changeover in administrations, Corona virus is still impacting us everywhere in the world. I know that the new administration is finding ways to deal with Corona virus. And I think we're going to see a lot of movement and some different things that they're going to try to help us. But also in the news, and hopefully it doesn't get buried, is obviously the news in the cyber world is about SolarWinds. - Oh yeah, no. When you start to really peel back that onion in our arena, right? When we talk about cyber, cyber defense and the breach with SolarWinds, it definitely makes you take a moment to pause and think about what the ramifications are of that particular breach. But it also helps us start to think about what is our role as a reservist when it comes to cyber defensive operations, right? I guess the question I would have for you, Sir, is what's the first thing that makes you think of as the Wing Commander of the Reserves on the Cyber Wing? - Yeah, so the first thing to think about is where can we help? Are we postured in the right places in order to provide capacity to our partners and how to solve this thing, but not only the SolarWinds issue, but I think broader about what other things could there be out there, right? Surely we don't know where all our adversaries are. They don't know where we are, and when we're doing our business, so I think we need to make the assumption that they've used this opportunity and possibly others that we just haven't found yet. And that kinda keeps me up at night. - No, I agree, I know whenever I'm able to talk to our airmen in this arena, one of the things I like to highlight is the importance of defensive cyber operations, right? It's not as simplistic as one might think, when we look at what they're really defending, we look at the importance of them being the centuries on each one of these fence lines. The problem is that when we look at cyber, it's not like a traditional base where I can scope it down to one or two entries, right? And then have a focus and then have some perimeters. We're talking about a very porous environment. I think the analogy that you brought up when we were talking in the past was a chain link fence, right? The problem is that each one of those gaps in that chain link fence is an opening for someone to come into and how do we monitor that? - Yeah, and think about that, and then put it on the top of that

chain link fence is constantly moving. In all spaces, from if you put it in 3D, it's moving everywhere. And so, it's a moving target all the time too. So, not only are you trying to find somebody what they're doing, trying to find what techniques they're using, what tactics, and then this constantly shifting and moving, where do you even start? And so, I think as a reservist, the best thing we can do is kind of always be ready. And I know that's not super tight and finite, but we just need to make sure that our folks are trained to the best we can, that we're the ready and enable when called upon, and making sure that we wanna leverage our reservists, civilian occupations and capabilities to bring to the fight, to have us think differently when we work with our mission partners, maybe we're bringing something different than they are. - Definitely, Sir, and it brings up two thoughts for me. And the first one that really comes in the challenge that I put forth to our airmen is a geekin' out, right? When we look at keeping ready, when we look at how this environment's always changing, and the tactics are changing, if you're not consistently geeking out, digging through the information outside of just reserve duty, if you're not reading the stories of what's being found out in the community, what some of the new techniques in the community are, what some of the new software is, what other individuals are identifying as threats, and really starting to hone your knowledge, become that subject matter expert when it comes to the greater sphere of cyber and cyber operations. - Yeah, I find that really hard for me, just maybe it's 'cause my age and the way I grew up and how I consume information, I can get overwhelmed with the amount of information out there, but I see my kids deal with, they're kind of used to having all the noise in front and they can kinda, they're better equipped to sort through that, and then try to find what they really need. And so, I've trusted our airmen that are really excited about this mission we're in and the business of cyber that they're able to kinda sort through that chaff and figure out really what's important to them based on their specialty and where it's important, they know where to go, they know where the sources are, the trusted sources to continue to learn, and hopefully push people around 'em, and their teammates, and their mission partners to explore those different things. I know every day I'm learning something else. Somebody's sending me something to read, and I'm trying to consume it, and I'm reading it. And I'm like, wow, I never thought of that. Every day my mind's blown in this business. And I think that's what makes it exciting for me and wanting me to keep coming back to work every day. - Oh, definitely, right? And I do try to stay away from a lot of the noise, because there's a lot of theories and there's a lot of conjecture, but actually digging into some of the meat and potatoes, going into some of the actual large corporations where they're putting out publications of things that they're finding, manufacturing references of what the next iteration is, what they're looking at. There's a number of different outlets through the DOD, right? CNET is another one I was looking at recently. I think there was an article about the potential incoming Secretary of Defense and informational warfare and information ops, and some of their perspective in reading into that. So, things that are just kinda guiding us in what kind of directions that we may be headed towards, right? And that drives me to my second piece of this conversation drives my thought process to is that the great power competition, right? What does that really mean? It's a term that's getting coined more and more, it's getting to be

use more often. And when we look at the national defense strategy and some of the other doctrine out there, its referenced a few times. I just wonder if you can give me your perspective on that. - Yeah, that's great, that's a great segue to talk about the great power competition. What's that really mean? We talk about it, the strategy lays out the specific adversaries or countries that we're worried about. And I don't see that change in the next administration. I think we are going to get a new national defense strategy maybe in a year, that the Biden Administration is going to work through that, what they want to focus on. And what I heard yesterday on the news, just kind of flipping stations that here was going on in Migration day, there were some discussion about there's gonna be probably a more focused approach to cyber from this administration, so I find that interesting. I don't know really what that means, and hopefully the authorities stay where they are, 'cause we worked really hard to get those authorities. I think at least DOD has done a great job with using those in the right way and not abusing some of the opportunities we have. And then, certainly those authorities, we have to look back at the elections, and I think we're pretty confident in saying that there was no foreign influence in elections and that was largely part due to the authorities we had from a cyber perspective. So, I think the great power competition next is, again, I still think it's China and Russia for the most part. And that's the great piece. They both want to be great powers along with us. And I think each country, including us, has a different approach on how are we going to do that. - Right, no, I do feel like cyber is predominantly agnostic, really when we look at it, when it comes to any of the political peace, or religious, or anything like that, right? It's really about the power of knowledge, right? And the power, and why is it agnostic from our perspective is the fact that the barrier of entry is very low, right? So, a 15-year-old with a $500 laptop, and a little bit of free software is now a player. Kinda goes back to SolarWinds. Granted, we don't know exactly who or what, but that doesn't take that person or somebody like that out of a key player potentially, right? - Yeah, a very small group presumably was able to do very large espionage campaign, using this tool, and we really don't know how big it is yet. And it could be worse, and I think that's the interesting part is that the door to the great power competition maybe is open past the whole nation state discussion. - And when we talk about the great, the larger nations, right, they have a lot more resources. They're able to put a lot more capability to it, and make them much more powerful as far as a potential threat and the potential breaches. It's just amazing when you start peeling back all these things, the differences, and going back to that a chain-link fence, what could breach that, right? - Yeah, and the other piece of this tool is that great power used to be, in the '50s and '60s, large standing armies and militaries, right? And that took a significant investment in order to get there. Cyber is not that way, and you mentioned the cost to entry is extremely low and some of it's free tools that are available, and there's people willing to sell those or provide those at such a low cost that it's gonna be really hard for us to really focus, you can't focus on all of 'em. So, we've got to come up with some sort of policy and a strategy that's gonna allow us to use cyber to deter, and I think there's a big discussion in the academic circles right now about what that means and what does cyber deterrence look like, and when you pair it with kinetic type deterrence, maybe there's a good policy, a way forward there. And I think the administration's going to think about

that, and then what that means. But I think still we gotta be focused on the big giants on the block, and that's probably China and Russia, not just from cyber, but from their capabilities, what their goals are, and their approaches. And so, this great power competition could be different for us based on who that actor is. - Right, no, and the reason I bring up that low cost of entry, it's really easy when we look at the craftsmanship of this arena, how easy it is to look like one thing, or look like another, how it only helps keep a fog over this type of business of what's really happening, what's not really happening, and it makes the ability to hold people accountable for it a lot harder, right? And then of course, when we talk about that threshold, as you pointed out, that threshold of armed conflict, where do we really get into that? Are we going to attribute this to an individual or to a group? Then, how do we hold them accountable without getting into that threshold of armed conflict? What is really considered an act of war when it talks about cyber? Cyber laws are a big thing that's coming out, right? A lot more caseloads going out there about what is considered illegal, what is considered a violation of a nation's rights, and so forth. - Yeah, there's a big discussion right now with SolarWinds is that is an act of war or is it espionage? And I think that's still, I think it's worthy of debate, what the intent is, 'cause it's so hard in cyber to understand what the intent is. And so, the "Tallinn Manual" kinda talks about it from a legal perspective, what the international community has defined as what's an act of war or act and aggression. And then, what are the approved methods to respond to that? And so, I think that's way above our heads, and certainly a lot of conjecture, and we can talk about that all the time. But I think what we need to focus on is doing our job, and we do our job well. It does impose greater costs on whoever that adversary is. And just makes it harder for them. And the more we can impose costs on them, the harder it is. And then, a lotta times in cyber, right, they're going to look for the easiest way in. And if you make it just a little bit harder, then maybe they go after somebody else. - Right, I think this key piece right, Sir, or when we talk, rolling it back to the reservist individual acts or individual acts at the unit level in defensive cyber operations is every time we can actually just stop or deter an enemy from coming across that barrier is a win, right? And then, how many wins can we get in a day, and just keep on racking those numbers up of, did I find this hole, was I able to patch it? Am I identifying what is and what is not a flag? Am I making sure that I'm using the tools that are available so that I'm keeping up on each one of these new TTPs every time that something is coming out? Am I making myself aware in my practice and against that and making sure that there's no reason for the enemy to know or think that this whole area in this parameter is free reign? And we have a pump rush for that, right? - Yeah, and I think that applies not to just when you're here on duty doing your military job, but it's in our personal lives, right? We need to harden our own cyber hygiene, and not turn our computers into bots, not keep 'em connected to the network all the time, do reboots, pull patches down. Just doing' good practices that you would normally do, like with your house, you don't leave your door open all the time, you lock your car when you go places. Same kinda things we need to do with our cyber practices that makes us a hard target, and maybe they'll go after somebody else. I think the other thing I think about too is I think I'm starting to see a shift is the whole struggle and in our community and the Intel community about

what do we wanna attribute, or what do we don't, and for what purposes? And our civilian businesses, especially big corporations, have been somewhat unwilling to voluntarily disclose that they've had an impact. And I think the government's pushed really hard to get them to cooperate and help. And I think we're starting to see maybe a shift of a lotta these companies are going to be more interested in saying, hey, we had a problem here. We had a breach, we've got a problem. And then, that makes life a lot harder for the adversaries if we're gonna come together, at least in America, and come together between academics, industry, and government to create attribution and do what we can to not let them hide in the shadows anymore. - Right, well, it leads to blind spots, right? So, we as a greater community within the cyber environment, aren't sharing those issues, then we're vulnerable, right? I think that's the importance here is no matter which industry you're in or what subsect of business you may be in, if we're not up channeling that to somewhere, and then monitoring it, then all we're doing is letting 'em use that against somebody else, right? And I think that that sense of community when we talk about cyber environment is gonna be key as we grow in the great power competition, because the fact is we're under siege as a nation, we're under siege as businesses because there's all kinds of different parts and pieces that this information can be leveraged to someone else's benefit. - Yeah, I think America needs to lead for the world, like we've done in so many other areas, right? So, some of these other countries that are, they're having the same problems we are, and maybe they're not equipped to deal with it. Maybe they're not sure what to do about it. And I think if we can lead and show or bring in all those communities together and to make this really hard on our adversaries is best for the whole world. And we may not do it like, we're not going to say, hey, we're going to lead and we're going to show you how to do it. We just need to do it, not take credit for it. But I saw this morning, like 16th Air Force and their cyber advisory post an article about Microsoft, they're sharing what they learned about, how they're able to, whoever did SolarWinds, attacked the supply chain, how they're able to disguise what they're doing, right? That's knowledge that can be shared across, and hopefully that doesn't happen again, and that we get better. And then if we do that, then it makes it easier for our partners and allies to build, to implement those things that we already learned, and kinda speed up closing the gap for those other countries. - Right, and that just adds to the barrier cost, right? The more that we can do, the more we can share, the more flags we can identify, the more techniques that we can identify, things that we can share as a community will then cause that barrier of entry to rise, right? So that nobody can just walk in with a laptop and a couple of moments of thought, and get after your business. That information, whether it's national intelligence or if it's business practices or business processes that are considered key to that success of that business or operation can get away to an adversary or to someone with some malice. - Yeah, and so you can't just cut off the head, and then hopefully it all stops, right? Because then all the legs are going to go somewhere else and create all these little, it's similar to the way we approach terrorism, right? And so, the terrorism, if I'll say, community, the adversaries, the bad terrorists, all terrorists are bad, but I think the way they've been able to survive, they created these cells, right? Individual groups of people with limited support. And that's why

they've been able to operate like cyber adversaries and these assistant, these persistent threats have done that. They've got these little tiny cells, some are kinda spored by nation states, some aren't, they're kinda doing their own things. It's very loosely, a loose network, and they're not connected really. And so, how do we handle that from a strategy perspective, I think is really interesting. It's not the old build a wall, and put a moat in, and then make a drawbridge. They figured that a long time ago. And so, I think that the approach has to be, we're gonna clearly identify who we're targeting in the great power competition, again, China and their approach I think is the long war, right? They're in it for decades and centuries. That's not really been our approach in America. We're fixated on what's right in front of us. And Russia's somewhere in between. And I think their level of interaction on the world stage is largely determined by who's in charge at the time. And we know the current regime there's probably going to be there for a long time. - Right, it goes to that infinite game, right? And playing the infinite game out, right? The rules are going to adjust. There's going to be small wins, but it's not the game is over. And I think that's the biggest shift in the psychological perspective of this is that we gotta take a different approach to what winning looks like and understand that the game doesn't end necessarily. If we're looking at it from a short-term game and or from a game perspective of that eight rounds and we'll find a winner is the wrong strategy. It's more of understanding that this win is going to then start the next piece of the game. And the rules may adjust based on that win, and continue to play that out, and going forth with the mentality of that. Yes, we've got short-term goals, short-term gains that we're gonna aim here, but that win will lead to the next game, to the next game, to the next game, to the next game infinitely, right? - Yeah, and I think the, well, I'll say the West loosely, countries associated traditionally with Western society, we've got a very strong group of academia in this business specifically that we're really sharing back and forth with. They're not going to allow us to not think about certain areas and parts, and certainly the supply chain is going to get a lot of attention right now. And so, we're gonna put a lotta effort into figuring that out and getting partnerships and relationships so that at least with government, that we don't have a breach of this kind of level before. But we can't ignore those other areas, like you talked about. - Yes, exactly, right? So yes, this is the fire today, but we also have to be looking at all right, because of this stepping back and looking at it, if this part, this supply chain was vulnerable, what other vulnerabilities do we have? And how can I look at taking, what lessons learned from this particular situation and apply that to other sectors or avenues of approach? - Yeah, and then as senior leaders in our government change out and move, it'll be interesting to see where that focus is. And really, if you follow the money, that's what we think is important. And so, Cyber Comms right now made a proposal that they want to have more control over the cyber budget and where that goes in order to help that. And I think we're going to see further discussions about what is cyber's role in defense of America. - Right, and that's where you, Sir, and us as leaders here at the wing, really start putting the emphasis of the due diligence our environment, right? In putting forth that effort to look at those avenues. - Yeah, I think it's really important for us to have these conversations and figure out where we fit in. A lot of our members are in the defense community in their civilian jobs as well. And so, we all have a role to play

there. We should be having these discussions with our families and our kids, and it's just exposing people to more and more of what's out there, what's concerns are, what the issues are, informed them so when it comes voting time, simply by voting in their local state, and the approach that that administration that's running, even at the governor and the County level, can have impact on America, and what we're doing, and how we're defending, and where we go, is the Reserve gonna play a bigger role in defense inside our borders? Possibly. - Right, I think that pontificating comes with a lot of different options, but I definitely see that the Reserve's going to play a key role operationally across the board. When we look at that strategic depth, when we look at potential changes in how that force is going to be made up, there's definitely an avenue for us to advocate for individuals and for reservists to be key, right? Going back to the point that you were making that a lot of these individuals work in the cyber community in this environment outside of the reserve duty, what thought processes are they using in corporate America that can then be leveraged, or what other training are they getting, and what other exercises, how are they honing their skills on that side that can then be brought here to the Reservists? And then, how do we implement that or help that get changed through the whole enterprise of DOD. - Yeah, and they can share what they learn and what they're doing in the civilian job, even with their small work center or the group or their squadron. And it's really important for them to leverage that for us to continue to get better, right? And so, make it better than it was yesterday is our motto, and making sure everybody's ready to contribute when called upon, and we don't know where that's gonna be. It's maybe not gonna be traditionally when we look at what a traditional deployment used to look like as we're shifting away from Middle East, and more to the great power competition and what that means. So, there's a discussion even about the Biden Administration yesterday in the news about what they're going to do with Iran and how are we going to handle that. So, all these things have implications into our business and what our future looks like. So, I'm just gonna ask all of our airmen out there to continue to stay sharp, and continue to train, and be ready when called upon. - Definitely, Sir, having that diligence to deterrence really comes into play, and honing those skills, and being able to geek out, and really start to think out these problems. Don't block your thought process to, well, that's never happen before, or we've never seen this before. Start to really critically think and look at some of the things that maybe we haven't looked at before so maybe we stop the next SolarWinds. - Yeah, and it just takes one airman, right? So, in our business, one airman can have a massive impact on our national security and the health of our nation, and health of our allies and partners, so that's exciting. - Yeah, and a shout out to one of our units, right? After COVID hit, we had one airman in the 689th that was key in expanding our capability within VPN. And that's a true testament to what a reservist can do as just one airman. - Yeah, just releasing the power and enthusiasm and let 'em go. It's exciting for us that we can be such a big contributor on the national stage. - Yes, Sir. - All right, great discussion, Chief. Again, we can talk about this for hours and hours. - Yes, definitely. - And so, again, I appreciate it, and thanks to Sam too. She's behind the board all the time. She doesn't get a lotta props, but she's doing all the hard work, and we just have to sit here and talk and pontificate about our thoughts. - Yeah, just like any other team,

right? Everybody has a piece, and Sam, if she doesn't take this, capture it, and package it out there, then it's just two old guys sitting chit-chatting, or recording on a computer, so thank you, Sam. - Yeah, can't do without ya, appreciate you and the whole team. So, until next time everybody, we're out here. (Paper rustling) (Upbeat music)