Ep. 72: The cyber domain

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 to another episode of the Sword and Shield. I'm Chief Master Sergeant Chris Howard, senior enlisted leader of the 960th Cyberspace Operations Group and today actually have a guest with me that's going to ask me a bunch of questions. I have... I'm Samantha Mathison, I am the 433rd Airlift Wing public affairs specialist but I also serve as the 960th cyberspace wing PA liaison with the 433rd office. You're also the brains and the fingers that make all of this happen. Right? So you're our editor, you're the person in charge of all these podcasts. So I wanted to take an opportunity to say thank you for um the past year's work, right? We've managed to develop a lot of content. We've been able to have a lot of great conversations Um and all the great work that you've done is what makes that work. So thank you. Yeah and we're actually just recently passed by the 70 episode mark. I don't know if you're aware of that. She was not, wow. There's that much of me talking out their own. Not just you. I mean Miss Frances Martinez has done quite a few resiliency messages. You know and of course the boss? Yeah. Yeah, of course Colonel Marriage and we've had a lot of guests. Some have been re occurring like Casey marriage case files. She's been on quite a few times and I can't think of anyone else right now. Sorry. But Good. Right. Well there's so much out there now so it's hard to remember everything. Yeah. Yeah. And so um anyway I just, the reason I wanted to have this discussion with you chief and come on board is because I know absolutely nothing really about cyber or the cyber domain or what it's really about. I know some things but I am by no means an expert. Um, I know PA things but I don't really know cyber, I did not grow up in the cyber world and sometimes you all start talking about things and I'm completely lost. It sounds like Greek to me. So is it okay if I go ahead and ask you some questions and you can fill us in and break it down for us. I will do my best. I'm not I don't have a doctoral thesis in this; I can give you the novice level um with what experience I have. Yes let's go ahead and dive with this awesome. So for our listeners out there who may not have a cyber background, can you just give us an all around layman's term, picture of what is cyberspace, what is cyberspace? Right. So I have been asked that question a few times, I've thought about it quite often. And then how do I break it down to individuals that are not in it? Right. So when we talk about a lot of our mission partners, um when we talk about the air domain, the land domain c domain, these are things that each one of us have probably experienced that we've been to the beach, touch the ocean, you know what that domain is? I walk around or take a I'm on land. Right. Some of us have flown, you know, whether you're taking an air flight or whatever. So we've experienced each of those domains. So the next domain. When we talk about spaces, I've seen

pictures, I know that there's satellites out there, I can see things flying out there. Right. Um I know these things exist. So when we talk about cyberspace it's a little bit more nebulous. Right? So I think of the Matrix. Right? I think of these things that are totally different and abstract. So how do we define what cyberspace is? And the reality is cyberspace is all digital domain. Right. There is no it's global. There's no real hard defining thing that you can look at. It's a bunch of in use devices. So when we talk about computers and we talk about smartphones, we talk about just about any electronic item and they're all connected? So then we hear the term cloud. Right, What's the cloud? What's the cloud? Um and you know, you have this nebulous thing of this big picture. And does that mean that ones and zeros are flying back and forth? Is it just some kind of big open space that just magically travels? Um and the hard reality is that all of this is a mixture of different levels of hardware and software that break this domain into something unique. Um and pretty organic. What do you think about it of the way it grows? But you get all the wires that connect the devices, and then you have all the wireless devices. Right. So now we do have our connections in most cases for the Wi-Fi, which then still goes to hardware, which then goes to servers and databases and all these things. Right. So it's all digital and then based on quality of service tagging and um development of different lines and routing packages makes it somewhat organic. It's breathing. It's living. And then when you add the unique user experience, um then that really changes that domains. You know, we have gaming, everybody games, right? Or most people gave everybody uses their phone, all of this stuff is connected. Right? So, um, and for each change in application for each uh-new server that gets brought online, that domain further expands. Um you know, we talk about the Internet of things. Any kind of degree Bryant you go into now has at least a small slice of the Internet of things every time you buy something now it's almost always connected to the Internet. So for each one of those new devices that gets connected the domain grows and grows and grows which then leads us to the business of cyberspace right? As the domain grows um there's one more entry point into this nebulous cloud. So I think that kind of leads us to the next question. Right? Yeah. So that was an amazing explanation and I'm not gonna lie to you if you geeked out a little bit but I warned you before we started. Yeah no I think it's amazing that this show is for everyone. So I appreciate that awesome explanation. But the let's tone this down a little bit. Let's talk specifically 960th. And how it fits into the cyber domain. Like what do we do to fit into that picture and to support the Air Force reserves objectives in cyberspace? Okay. Right so uh going back to where I finished off with the last piece. Right so we have all these different connections. The DOD has to protect all of the connections all the pieces and all the information that falls into our specific domain, a portion of the larger cyberspace domain. Um So the Air Force they do you have different agencies you know when we talk about you know off cyber specifically when we talk about 16th Air Force then we talk about the cyber wings that are underneath that with the 688th and 67th cyber wings um the 69 9 60 it specifically comes into play. There is an associate to both the 67th and 68 siblings. And then what we do is we provide that surge capacity and on demand capacity to both of those wings and the weapons systems they specifically has. We are actually the only reserve cyber wing currently and we are the only cyber wing that actually has all of the weapons systems

encompassed within our wing. Uh that is really cool. I actually didn't know that. So all the units that we have, each specific unit has its own weapons system. Is that right? For the most part, there are a couple of units that do have similar weapons systems um that are still associates to individual units. Right? But for the most part, yes, we do have a different weapons system for each unit, which is kind of unique. Right? And then when you look at the complexity of what that does for a wing like this, we have geographically separated units, all with the individual mission sets supporting red Gap units and that's across the whole Continental U. S. So then the other piece is that when we talk about traditional domains, when we talk about land, sea and air using Air Force specifically as an example. Um a fighter wing would have probably one airframe maybe two. Right. And it's all housed and built to focus on that airframe and that mission set and support that mission set. So, you know, they're standing about all of that stuff is built towards that. When we talk about cyber and having six different unique weapons systems. Now, think about what kind of support that requires and all the different levels of knowledge that you have to have throughout the organization to ensure that we are getting after that mission set appropriately and well resourced appropriately and we're executing the mission appropriately while meeting all of the normal demands. Day to day. Air force work definitely sounds very intricate and complicated. Can it? Uh I like to for an analogy, right. Um those old school, late night TV shows where they have the guy that comes out with the spinning plates and how many we can get going. I would say that we have probably close to 14 different plates spinning at the same time, trying to keep those wobbling while managing the TR aspect of uh a lot of our airmen. Yeah, that certainly sounds extremely challenging. Um I can't even imagine how y'all do this, but of course, you know, for the greatest air force in the world I think, but so we make it happen. So one thing I wanted to ask is we call or each unit has what's called a weapons system. So traditionally weapons systems tend to look more like uh missiles or airframes or something like that. So can you just describe what a weapons system in the cyber domain looks like? So yes, when we talk about weapons systems, we think of ballistic, we think of kinetic, right? We think of aircraft with missiles. We think about, you know, ships with missiles. We think about aircraft bombs. We think about remember the bullets, you know, we think of an M-16, you know, when we talk about infantrymen and we talk about marines, they carry their M-16, they land in there um, in their location and then they fire their weapons to be effective. Um what does a weapons system look like? So when I first came into cyber, I tried to attribute that to basically an airman with their laptop. Right? Um to get the visual effect of it. But going back to explaining what is the cyberspace domain. Um and what does that look like? As far as infrastructure, the weapons system is a unique combination of hardware and software and algorithms. Right? So what we have is applications through software attached to individual hardware at different locations throughout the domain to give us the desired effect. So we have things that are looking at information collecting information, analyzing information and providing feedback to our individual airmen are operator in the seat, which then can leverage other software and hardware to either protect the domain, identify and isolate risks. Isolate potential threats. Quarantine those threats. Then break them down and then also then provide feedback and eventually

a response to each one of those threats as you know, so it's really hard to kind of grasp blood to me at least you know, visual expectation of that. But you know, if you're thinking about an aircraft, we're talking about reconnaissance aircraft with the that maybe even be armed, right? Let's even look at a drum. So the drum, we have a camera, it's providing feedback. That's our eyes and ears. These pieces of hardware sensors are drawing in that information. Um, and then you know, we have analysts looking at that and then we're able to fire for effect. So a drone would be pulling that information providing into the operator, the operator making the decision on what that's gonna, what that actually is defining what the target is getting authorization and firing boom boom boom. Similar in cyberspace we have our operator in front of their device, they're getting information. They're seeing what this looks like there are analyzing it, making a determination and then they're able to defend a fire against it. Awesome. So my understanding based on everything you just said is each weapons system is unique depending on the emission set of the unit. Is that correct? Right. So to go a little bit further. Right? Give you a very broad term and apologize on all weapons systems but specifically some of the software and specifically some of the hardware that gets used helps define what each ant at what level within the domain also defines what that was weapons systems responsible for. So going back to traditional communications, I'm going to get out for a second and apologize and hopefully I don't lose you. Um you know, there's multiple layers, right? Um and there's different gates. Right? So communications uh you know your phone and your Internet and all that stuff gets co located into two pipes and stuff like that. So you know bigger pipes just keeps on going all these different streams to large pipes. Right? So within weapons systems there the different layers of those pipes to see what's going on defining being to peel out and then do different things at different levels as well as each different weapons system has different applications and software and algorithms that all look for specific things as specific threats and get after that. And I do have to add one more definition. Right? When we talk about the cyber domain and the nine sixties specifically, so 960th it is uh predominantly focused on DCO, which is defensive cyber operations. So a lot of this please take with a grain of salt is defensive perspective. We haven't really talked about any of the offensive side of the house. Um but that's because 960th is DCO-centric. Okay. Yeah that was a lot. I know I apologize I'm trying to make it is as exciting as possible, but no, it's good, it's good. So I mean you're learning to be something and that's the whole point of this podcast, honestly, you know, not just me learning something but explaining our purpose and reasons for being here uh to our audience as well, you know, So um I appreciate that geek out moment. Good morning again. So from a PA perspective, as one of the interesting things I've run into working closely with the 960th is the sensitivity of information and offset concerns. And so I just want to throw this out there chief and you can have your input too. But I know sometimes people think like there isn't a lot of stories that get put out there about cyber and the extent of what we're doing and how far reaching our impact is. Um and so just wanna put out there to the audience that sometimes we choose not to tell stories just because it is too sensitive and there are obsolete concerns because we are functioning in a defense capacity and PA ties into that, you know, when it comes to what stories we tell versus what we choose

not to tell. And so that's a constant um struggle ideal with a lot of the times, I'll get a story idea from someone or someone will say, hey, you know, this unit did this awesome thing, you know, and I'm like, wow, that would be a great story to tell, Let's do it. And then just for someone to turn around be like, that's really sensitive. I don't think that's a good idea. So, um, I don't know chief if you have any input on that, but I think probably some clarification. Right? So I've been working in special programs um and secure missions for wow, 20 years. You're aging yourself chief for 20 years, right? Um, so what we're really looking at is not just individual stories; it's the co location of information quite often. Right? Um, there are some things that are just flat out we can't share because it would, you know, kind of tip our hand to a technique or a tactical procedure that we might use or maybe it lends itself to give our adversaries and idea of some of our capabilities that we were wanting to keep tight in some occasions. That's even; it may be able to allow our adversary to actually attribute um some things to us specifically, which is not always what we want to do. Um then we talk about specifically within cyberspace and going back to the all that information floating in the cloud. Right? So here's a large degree of information and when we talk about a second and for info-sec, um we're really trying to keep from all this information to be co located to give our adversaries a clear picture of what our capabilities are, you know, what resources we have and what we're capable of actually doing against them. That information is valuable, right? Because then they can defend against it. They can find holes in it. Um and it's very important. So when we put all that stuff together in cyberspace, even a small story about movements and or you know new purchases of equipment or um maybe what this airman was doing or what location they were doing it and you know, cyberspace is uh it's a data trove, right? It is just think of it, it is a landfill of information, right? That's just there. So if you think about resources, if you have the right kind of tool, the right kind of mining tool and you go through that land meal, the landfill, you're gonna be able to find all kinds of resources. You can find all kinds of information; you can find all kinds of products. I'm gonna be able to find all these things that you might be able to use for something else. And cyberspace kind of does that as well. So all this data is out there. All this information is out there with the right algorithm and the right um searching and techniques. You could put together a pretty clear picture of what's going on and think about that from an individual perspective. You know, go back to the Internet of things, all of the things that you have your microwave that's now link No I looked into that one of those things creepy. Um your refrigerator, I can find out what's in my refrigerator on an app now in some cases, right? Um I can look at cameras in my house and all this stuff, right? So if that's at your level, imagine that from an enterprise level, like the Air Force specifically and how I can grab all that information if it's not encrypted, it's not secure and if it's not defended and what I can tell about an individual or an organization, yep. Exactly, chief. I mean, you hit on a lot of excellent points there. It's about not displaying or tipping our hand too much when it comes to patterns and then also what our adversaries can infer from that information. So yeah, and it's not again, we don't want to you know, not share these stories or we don't want to you know, highlight the good things that are going to do. But on occasion that risk is just not worth that, that reward. Exactly. Yeah. So it is a struggle to get these stories told

because cyber Airmen in in our wing are doing a lot of amazing things, but at the same time it's got to be strategic storytelling. So it's definitely been an interesting experience that this past couple of years Working with a 960th trying to get these stories told and right, sometimes it does feel like we get handcuffed or we get barrier and in where we can't do certain things. Um and sometimes we overuse it right. But you know, it's always in the effort or in the vein of let's make sure we're doing the right thing so that we don't give away too much and then put ourselves at a detriment. Yeah, exactly. And you know, I've seen personally seen the reach of the swing and the airmen that are working in it and what they've been involved with and everything and it is way more far reaching than I anticipated when I first came on board. However, again got to be careful about what stories we tell and how we tell it. Exactly. And I would stick with the fact that this domain is global and we're in it, yep. So one last thing I wanted to touch on chief is going through and working with the 960th. You know, there's been a lot of discussion about the great power competition. Can you just geek out with us one more time and just kind of explain how we fit into the great power competition that's happening right? You know, that is an exciting and scary question. I want the same things. Right? Again, we're going back to the different domains, right? The way I try to leverage that is is for a nation or even an individual to get into the air domain. Quite expensive right, billions of dollars. We talk about the sea domain aircraft carriers, billions of dollars. I'm sure you can nickel and dime that down to smaller, smaller crafts and different resources, even land domain, you know, to have that kind of dominance. But the question I have for years, how much does a laptop cost in comparison? Not that much. Few $100. So the cost of entry into cyber domain is fairly inexpensive. When we talk about the great power competition, when the we look at how this domain is defined, when we look at the fact that there's so many different entry points that the domain is constantly growing. Uh, the Internet of things. There's so many different touch points that are now vulnerable right? As the expanse of going away from hardwired lands into Wi-Fi networks, you know, and some of those uh Wi-Fi networks are large. Right? You think about a major metropolitan city um, you think about all of these open spaces um yes Wi-Fi can be secure but I have billions the b of potential entry points and I have a cost of entry so low that you know, it's really easy for bang for the buck for nation. Right, So emerging nations or even larger nations, quite often we talk about the great power competition. We talk about china. Talk about Russia, you know, to have effects in this domain is pretty cost effective. Right? So when we talk about the Internet of things again, when we look at all of the different domains that now connect within this domain. Right? You have all of these different connections, all the parts and pieces um that come into play, I think about the supply chain issues, we're having to date right now, all of these things do end up being connected. Um, look at the couple of the ransom ware attacks in the past year; all of these things come to play, right? So, uh, the great power competition and how we get involved in that um, is really from a defensive perspective, right? We understand that the threat is real, the threat is out there and the threat is cost effective for adversary. What we have to do is ensure that we minimize the amount of vulnerabilities we have. Right? So as much as we dislike those annual trainings right there for a reason, give us at least a cursory thought of some of the threats that we

have, um, you know, insider threat, actual hardware threats are and even sent some unintended threats through phishing, spear-phishing and you know, some of the link attacks that occur. Right? So the whole idea is that if we as an organization are getting after that and we are able to thwart our adversaries, whether it's a great nation, you know, appear nation near pure nation or even just a lone wolf and we have most of these threats or these opportunities for them to gain access limited and tracked and flags so that we can then thwart that. So then as we project out from there when we talk about offensive campaigns if our house is secure right? If our fortress is secure and we have everything here and then we have we can keep our stuff moving and now we have to prevent our adversary from doing the same much like they do to us. Right? So the crazy part about our domain being global is that everything is connected one way or another there's a route somewhere somehow that most of these things can connect to. So everything has access, everything can be vulnerable. And then it's through a good defensive posture that we can actually be prepped and defend our house. So that way we can maintain and keep moving our mission forward while then thwarting our enemy. No, I can't really get into too many actual details but when it goes to the great power competition um and we talk about cyberspace, it's evolving every minute we are gaining speed. The Internet or in the Internet of things is growing. A new device gets connected every second or multiple devices per second. And that domain is expanding which means every new device leads to one more vulnerability which then also leads to one more thing you kind of have to ingest in this big piece of data, the data cloud and then prevent it from being a threat to us specifically. Um and then of course building the right algorithms using artificial intelligence using good old fashioned hard work having operators in place and making sure that we are, you know, constantly testing and training against those different threats and getting everything I could get into a lot more details. I can make out a lot more long, much longer on that, but I don't want to lose these people uh too far into that. I just can only emphasize the fact that we as individuals do take technology for granted at times and for each new piece of technology, make sure that you go through the process of securing it so that you limit that threat to yourself as an individual and then limited as a threat to the greater good of the nation. Right? You have to make sure that that's all squared away so that they're not collecting that on you that way they don't have an entry point into our networks and that we are keeping our house secure so that we can continue our we have life and prevent our adversaries from preventing us to meet our nation's call so shameless plug here that I'm gonna put out to the audience. Um and because this I think directly applies to what you just said about checking your devices. Uh please please on social media check your privacy settings, make sure they're set the way you want them to and then look over the information you're putting out there. You know, sometimes are not sometimes actually our adversaries are looking at our members Facebook profiles or Instagram profiles or twitter pages and feeds, you know, so uh just shameless plug right here from PA. Please be careful. We have to put a hook in for another episode but that leads me to one thing that I'd like to throw out their critical thinking. Yes, right. Um and when we talk about social media, we talk about how we ingest information and data is making sure that we are critically looking at what has been presented to us, how it's being presented to us

and then also making sure that we are validating sources and validating the information and not just ingesting plenty. This is gonna look at this as a fine meal. That is a big mac. I'm just going to swallow and go right, yeah, there's definitely some nonsense I've seen out on in Facebook land, you know, I'm not gonna lie and then, you know, I've known people who have completely bought into it and it's not even realistic, it's like do these people science? But anyway, chief we're getting pretty short on time. So I just wanna punt one last thing to you, Is there anything that we didn't cover that you wanted to bring up or talk about any last messaging for our gladiators out there. Um Yes, so cyberspace is exciting and if there's plenty of opportunities here in cyberspace um at different levels for anybody that's interested in being part of this domain, part of this mission set by all means ask questions, reach through our P A. Reach through the website, ask us questions more than willing to answer any kind of questions you may have. Um but also make sure that you critically think and make sure that you keep yourself secure because you all out there are important to us and your success is our success. And if we can get a little bit out of that, that's a huge win for me. Um and I want to thank everybody out there for what they do every day, keeping this nation safe. All right, well chief, I think this wraps up our episode. So gladiators I have to finish off with uh you know, thank you for everything you do. Thank you for answering your nation's call. Um thank you for your sacrifice and thank you for all that you do every day in securing this nation and getting after our mission sets that are in front of us. And remember get out there and stab the enemy in the face through cyberspace.