Constellations Podcast

Episode 28 – Cyber threats, Zero Trust and The Bane of Security

Speaker: Greg Touhill, President, Cyxtera Federal Group – 25 minutes

John Gilroy: Welcome to Constellations, the podcast from Kratos. My name is John Gilroy and I'll be your moderator today. We have a special guest in the studio and we have a special studio. Today, we're broadcasting from the Newseum in Downtown Washington, D.C. and somehow we managed to get Greg Touhill off the stage for about a half hour to share his thoughts with us and who's back on the stage, as soon as he leaves the studio. He's the president of Cyxtera Federal Group, a company that provides enterprises, government agencies and service providers an integrated, secure and cyber-resilient infrastructure platform for critical systems. Before Cyxtera, Greg was Brigadier General in the U.S. Air Force and served as the first U.S. Federal Chief Information Officer and also Deputy Assistant Secretary in the Office of Cyber Security and Communications. Greg has a wealth of knowledge in cyber security. Today we're going to talk about the evolution of cyber threats, talking about how public and private sectors can secure their satellite infrastructure and finally delve more into this public/private partnership that we've talked about earlier.

Well, Greg, let's jump right in here. Until recently, satellite networks have been mostly standalone systems. Increasingly, satellite networks are integrated with terrestrial networks, creating a hybrid system. Has this integration increased susceptibility to cyber security?

Greg Touhill: I think so, John. You know, frankly during my time in the Air Force, I was involved in the space business for a long, long time and folks that go online will see that I'm sporting the Master Space Badge on my uniform. But, as we took a look at it, frankly, the space infrastructure is a lot of different pieces. We talk about the actual satellite platform being a system of systems, but as you take a look at the satellite network and how it works, it really is a system of system of systems and it starts with developing the code and the designs and the like for the platforms and the software. Then, you've got to consider all of the different terrestrial networks for transmitting, then sharing that information. You've got the manufacturing facilities. You've got the boost phase and then once you launch it and you get that satellite up in space, you have to have the means of controlling it and getting the information from it. Each one of those segments is critically important and needs to be secured.

John Gilroy: Now, I've read about attacks like jamming, denial of service, hacking. Can you describe maybe a couple of these or the ones you can share with us?

Greg Touhill: Sure. Well, frankly, when it comes to the transmission of information to and from the satellite while it's up in orbit, that's really where you have to take a look at the radiofrequency spectrum and jamming is just one of many type of things that folks can try to employ for a denial of service purpose. And we have some methodologies and some capabilities to try to burn through that jamming and to neutralize that. But, still, it's something that as you were designing your space segments, you want to make sure that you are resilient enough to be able to deal with jamming incidents. Now, from a hacking standpoint, as previously mentioned, there's lots of different segments in that system that gets up in the air from design, all the way to the control of the satellite and even the satellite software on board while it's up in orbit.

So, you want to make sure that you are controlling the environment and securing each segment, such that you cannot introduce any unexpected changes into the software. You want to make sure that you have positive control from conception all the way to operation.

John Gilroy: You were at a CyberSat Conference about a year ago in Tyson [Tyson's Corner, VA]. I was in the audience and you had a real fascinating approach there and you talked about the Star Wars scenario. Well, what do you mean by that? And you talked about how, perhaps, one of these systems could be designed with a backdoor and vulnerability we won't know about until it's up in space and then we go back to George Lucas, huh?

Greg Touhill: Absolutely. And frankly, it takes many, many years from conception to actual launch to operation and the life cycle for these satellites, we say, "Okay, this particular communication satellite has got about a 10-year lifespan once it goes up on orbit." We're finding that a lot of the satellites, they are designed so well, that they will last a lot longer than the original design. But, what we don't necessarily talk about is the lead time to get it up to launch and using that Star Wars analogy, which we learned the back story in Rogue One, one of the designers of the Death Star designed the famous six meter port in there as a material flaw or weakness that the rebels, of course, in Rogue One discovered and were able to take to ultimately get to Luke Skywalker to fix.

As we were taking a look at our satellite technology and not only just the bird, itself, but the ground segment and every step along the way, we need to make sure that there is no six meter ports deliberately put in and then check it so that we have a software flaw or design weakness that could be exploited elsewhere.

John Gilroy: All the exploits today are based on identity and financial theft in the commercial world and they are increasingly becoming a bigger threat in space. So, what is driving this and what degree of danger does this pose to the United States?

Greg Touhill: Frankly the risk continues to go up as we become more and more reliant on software and software intensive systems because they are exceedingly complex and, frankly, complexity is the bane of security. You want something that is complex enough to thwart and deter potential adversaries. But, you also want the simplicity for the operators so that they can effectively operate the different systems that are out there. So, as we take a look across the entire supply chain from, like I said, the conception of the idea to the actual operation of the finished product, you have to be secure by design. And, as you are doing your initial requirements, documents, as you are doing your original designs, you have to include the think like a hacker mentality in your design, all the way to your production and your operation.

John Gilroy: Secure by design. Let's go back to Star Wars. I can't help myself here. So, let's say we have a satellite out there and it's going to last 10, 15 years. Should we design these to be retrofitted for increased cyber security or is that even conceptually possible?

Greg Touhill: Well, for some, yes, you can do some software patches by pushing them up to the satellites, themselves. But, it's not like you can send somebody up there and do a manual reboot or reload, so you have to be able to take a risk-based approach and say, "You know what? I'm not going to be able to go out and physically touch that satellite, but if I can do a software patch, then you have to take a look at first of all do I want to do that because that could open up a risk, a threat factor. And then, two, if I do want to do a software patch, then how do I secure that link so that an adversary cannot get at it, that only a trusted, known and authorized source can push a patch." So, once again, that gets back to the secure by design and those are options that most of our design teams are already working on and great companies that are out there working with the U.S. Government to build and design these satellites as well as our communications companies, they are already addressing a lot of these issues.

John Gilroy: If you go to Google Trends and type in the word existential threat, you'll see a big hockey stick in the last four or five years. Where, 20 years ago, it wasn't used that often. So, let's talk about existential threats here and real threats. Cyber attacks on satellites could affect the military system, military threats. Are these really imminent or are these just something that's a frightful theory that may or may not take place?

Greg Touhill: Well, you know, without disclosing any classified material, I'll tell you the threat is real and that during both my military and my federal service, I saw plenty of evidence that led me to be convinced that nation state actors and criminal groups have now discovered that the satellite supply chain is something that is of great interest to them from the standpoint of first, theft of intellectual property and then secondly, potential competitive advantage for nation states. So, I'm convinced that making sure that that supply chain for the satellite

systems, that supply chain needs to be secured by design and for those things that weren't necessarily designed for security in mind, we need to do the proper compensating controls to make sure that the material weaknesses that are existing in the system are properly compensated for to protect them.

John Gilroy: Let's go from the satellites to the ground. We just talked about space-based assets. What about attacks mounted against ground station network? Are they vulnerable there as well?

Greg Touhill: Yeah, absolutely. And when I was in the Air Force, one of the things that we were looking at was beyond just the cyber. We took a holistic risk management approach, so we were looking at the physical security, the personnel security, the processes. Really, it's important to take a look at people, process and technology when you're looking at risk and that certainly fits with the cyber risk model as well. So, from the ground station standpoint, if you go for example to Schriever Air Force Base in Colorado, which is one of the main space command locations, there are some facilities where you're doing the retinal scans, you are doing the standing on the scale as you are going into the areas just to make sure that we have a very identity-centric positive control over who has access to the most sensitive gear.

And while it sounds kind of James Bond, it needs to be in a lot of different locations and, further, when it comes to the cyber standpoint, you need to have that identity-centric approach as well. You need to have that zero trust model when you are dealing with your software and the operation of systems and as I was pivoting from federal service into the private sector, that was one of the considerations that I took because I see that not only in the space and satellite area, but throughout the entire economy. We need to make sure that we adopt that zero trust model.

John Gilroy: Twenty years ago, when I said the word satellite, I'd think of you know, something like a big refrigerator out there in the sky and maybe two of them, maybe three. What is happening now is we see constellations of satellites going up in LEO and MEO orbit. I mean, there are dozens and dozens of them going up there. Do more satellites just increase the risk or does the sheer number actually give you some backup? Is this is a good development or a bad development, Greg?

Greg Touhill: Well, it really depends on your perspective, John, but it's a great question. We do see significant constellations that are out there and for example, the Iridium constellation which is a low Earth orbit, it's got dozens of satellites that are up there and, by the way, I really used them to great effect when I was the Director of Command and Control Communications and computer systems for Allied Air Forces in the Middle East. I mean, they gave us some great capabilities that nothing else could have, particularly in the early stages of operations in

Afghanistan. We want to have a robust network that is out there, but you have some other things that are caused by having all these satellites up there. First of all, there is still an issue with space debris. It gets very cluttered up there and we don't want collisions with a rogue piece of booster that goes out there and could collide with something. So, space debris is a problem that continues to increase and we've got to keep our eye on that.

Secondly, we also have a lot of other folks that are putting up stuff out there. It used to be just the Soviets/Russians and the United States. But now, a lot of countries are putting up stuff. The commercial folks are going up there as well. It's now a very congested environment, in some regards. While the math indicates, oh, there is plenty of open space up in space, actually it is becoming more and more congested and that becomes an issue when you are talking about frequency congestion, you are talking about physical space, you are talking about orbital space and the like, so it is something that those of us who watch and participate in the space and satellite business, we are concerned about and we are keeping a close eye on.

John Gilroy: Now, Greg, in a few minutes, you will be on stage at this cyber security conference here and I think of Equifax and breaches and there is a new Argentinian Social Network called Taringa which sounds kind of exotic. Sounds like a dance.

Greg Touhill: Bueno!

John Gilroy: Muy bueno! Tango Taringa. So, how do we protect ourselves with these massive networks? Earlier, you talked about networks. How do you protect from these massive networks?

Greg Touhill: Well, it's a great question and it gets back to what I was saying about, as I was pivoting from Federal service into the commercial world. Where was I going to go? And I decided to adopt the Gretzky model, if you remember Wayne Gretzky?

John Gilroy: I do.

Greg Touhill: Gretzky said that he was successful because he skated to where the puck was going to be, not where it is. And I said, that's a great strategy for life and as I took a look at the cyber world, that's where I'm pretty good at and where's the puck going to be? And that's really where I embraced the zero trust model because the standard perimeters that we were used to in the past, that perimeter mentality, I think, is dead because everybody is mobile, you're using multiple devices. I flick back and forth between about six or seven devices during the day and I'm not necessarily anchored to an office. I'm using multiple

applications, multiple operating systems, but I want to make sure that I'm secure by design and that zero trust model works for me and I think it works for every used case out there now and into the future.

So, I think as we take a look as a society and trying to protect national prosperity and national security, and I don't think you can have one without the other, so you have to look at both. The zero trust model and the software-defined perimeter technology that implements it best is really where I recommend both to my friends in the government as well as my clients out there across the commercial as well as the public sectors. That's really where the puck is already arriving and where it's going to be for the foreseeable future.

John Gilroy: Now, it's one thing to talk about zero trust, but implementing it is one thing a little different there. When you talk about artificial intelligence, analytics and machine learning, I guess these are all tools that you can use for zero trust, is that right? Is that how you view them or is that separate from the category of zero trust?

Greg Touhill: I'd place them separately because you know, really zero trust is a model that ... you know, Forester came up with the term zero trust model back in 2010, but it's really kind of a security concept that says, you know what? I can't trust anybody on the outside and we kind of felt that way for years anyway, but as you take a look at the reality of today and the loss of the perimeter and where the perimeter is really the person, you really can't trust on the inside, either and you shouldn't. You know, Snowden really kind of proved that for us, didn't he? So, as you take a look at the realities of today with a mobile workforce and your information is everywhere. It's on premise, it's in the cloud, it's co-located in data centers, it's on mobile devices, it's everywhere.

You need to have that micro segmentation. You need to be able to have that encrypted link between the user and the data that they are trying to access and you really need to have that personal identity-centric view to security down to the data level.

John Gilroy: I'm going to quote a gentleman by the name of Greg Touhill here. He was at a CyberSat Conference last year. I'll read you the quote and you tell me if he makes any sense or not. He said, "We need to have the approach that I might be able to live through the battle I've lost, but I don't want to lose the war." Oh, the old Pyrrhic victory, huh? I mean, so what did you mean by that, as far as cyber security and satellites go?

Greg Touhill: It's really a discussion on resiliency. I know that I'm going to take a punch from a hacker or an insider threat, you know.

John Gilroy: Threats can happen.

Greg Touhill: It's going to happen and you don't want to have that dimensional line type of mentality where it's an all or nothing. We take a look at the cyber landscape differently now than we did five years ago and like I said earlier, the perimeter is dead. I may take a punch. I have to expect I'm going to take a punch. I grew up with brothers. I know I'm going to take a punch, but I've got to keep on going, so from a cyber standpoint, that's really where that zero trust and software-defined perimeter comes into play. Traditional hackers, what they will do is they will bore through. They could even leverage existing VPN's. They will hijack credentials, they will come in looking, smelling and acting like a legitimate user. They will drill in, they will get a toehold, they will escalate privileges and then they will move laterally throughout your network.

Well, you know, that's really where I'm seeing the software-defined perimeter thwarts that, just defeats it, and having an identity-centric approach that authenticates first, integrates multifactor authentication and role-based access control so that I verify the user, I set up that encrypted link to my environment and I only serve up what you're authorized to see and when you're authorized to see it and from where you're authorized to see it. Having that kind of granularity, I think, is critically important. And, even if I do have a bad actor, now I've reduced the attack surface down to a point of one because I take away the ability to elevate privileges and move laterally. In today's realistic and cyber environment, you absolutely need to do that.

John Gilroy: Two hours ago, Steve O'Keeffe from MeriTalk was on stage and he talked about in the Federal Government, they have 3,000 different products to choose from, just when it comes to cyber security and everyone wants the new, shiny thing and the new stuff and maybe the new shiny thing may distract them from managing risk. Is it always a new product, a new bell or whistle, or maybe it's just going back to RBA, role-based access? I mean, that's from 30 years ago.

Greg Touhill: Well, you know, frankly we've got too many tools in the Federal Government, as well as in the private sector. Collecting tools isn't the way to go. What you want to do is you want to make sure that, first of all, the tools that you have you're using them properly and I don't think that I have found my satisfaction in the public or private sector, where folks are actually using what they have, well. And we certainly find that with the U.S. Cert going out and doing incident response, the vast majority and I would say the number is well over 95%, although their official doctrine says it's 85% or above. You know, folks aren't configuring systems right. They're not doing the right things right themselves, because they're task saturated and having too many tools just makes it more complex for an already over-tasked workforce and that's where I like the software-defined perimeter technology that I was mentioning because frankly, it retires and

provides and off ramp for all those VPN's. Well, actually doing what the VPN does, even better.

We installed it at one particular Government cyber range where they had a firewall that had over 20,000 rules and you installed software-defined perimeter technology on it and took it down to 10 rules and the supervisor said to the firewall administrator, "Well, that frees you up to do all those other tasks you say you don't have time for." So, it's time to start cleaning house on some things that are adding too much complexity and just aren't cutting it anymore because VPN's are 22 years old. They're old enough for me to take out for a beer and in cyber age, using Touhill's law of one human year equals 25 computer years, I think it's time that we start looking at some of the older stuff and retiring it for stuff that's simpler to use and operate and does a better job.

John Gilroy: We are sitting here at a cyber security conference and earlier I got a cup of coffee and I stumbled on a gentleman by the name of Dr. Ron Ross. He works over at NIST. This guy's so smart, he needs a wheelbarrow to carry around all his brains. I mean, this guy is way smart and I keep thinking of NIST, the Government and you, and it's a public/private partnership. Well, maybe you don't have all the answers and maybe well, Ron probably has all the answers, but you may not and Ron and may not, but maybe combined this is a two and two is five or maybe two and two is eight situation, you know? Public/private partnerships.

Greg Touhill: Absolutely. Ron and I had breakfast today, together.

John Gilroy: Like minds, I hope?

Greg Touhill: Well, and I've been friends with Ron for years and he's terrific. He is, in fact, one of those brilliant folks who is continuing his Government service. You know, he's a retired Army officer and Ron is a national treasure. I've been a firm believer in public and private sector partnerships and that's one of the reasons why, on behalf of Cyxtera, I represent our company in the IT Sector Coordinating Council, which is one of those public/private sector partnerships that DHS sponsors on behalf of the Government. I do think it's a responsibility of us in the private sector to, in fact, share as part of that cyber neighborhood watch, what we're seeing in the private sector with the public sector and, on the same token, I think it's a responsibility of Government to be sharing with the private sector as part of that cyber neighborhood watch. Because, if we don't work together, then that just increases the risk for the country and it gets back to what I said about we're all in this for protecting national prosperity and national security and you can't have one without the other.

John Gilroy: We're going to take this satellite discussion and make it more personal and more human and maybe more general here and I'm going to quote you again, Greg. You wrote that we're raising a generation of folks who are freely surrendering their privacy. Your privacy. Giving up information and not recognizing the value of it. Boy, that's a big, big topic to talk about, but it reads directly to cyber security, doesn't it?

Greg Touhill: Absolutely and, you know, one of the examples that I use with my students at Carnegie Mellon, is the fact that we have a lot of folks who say, "Hey, you know, you've got to put into your social media thing, your birthdate, where you're from and all sorts of information." This is the same type of stuff that some folks are using for recovery data to accounts that they have elsewhere, like your bank accounts and things that are very sensitive. Why would you want to give up your birthday? Why would you want to give up some of this information, particularly when crooks could use it against you. So, one of the things that I tell my students is make up an internet birthday, something that you can post out on the internet as this is my birthday, but it's not your real birthday.

And it sounds pithy, but it gets my students thinking about what kind of information they have, its value, who could use it against you and let's not forget that there are, in fact, cyber crooks out there, criminals that want to gain personal information so that they can take over your identity and get access to such things as you wealth, your fortune, your intellectual property and the like. Your information has value. There are companies out there that collect and aggregate information and then they resell it. So, there's already a value model on your information and you should be defending and protecting and knowing the value of the information that you are the possessor of.

John Gilroy: Well, Greg, unfortunately here, we're running out of time. I'd like to thank our guest, Greg Touhill, President Cyxtera Federal Group.