Constellations Podcast

Episode 2 – Satellites, Cyber Threats and Sun Tzu

Speaker: Bob Gourley, Co-Founder and Partner, Cognitio – 24 minutes

John: Our guest today is Bob Gourley, co-founder and partner of Cognitio and the publisher of CTO Vision. This is your newsletter, right?

Bob Gourley: It's our blog. And the CTO Vision blog is focused on technologists.

John: Great, great, great. Bob has also written so many books that we can say his last book ... Well, his last book is "The Cyber Threat," which provides business executives with actionable insights into the threat landscape. "The Cyber Threat," huh?

Bob Gourley: Yeah, it's a threat-focused view of cybersecurity, figuring out what the bad guys are doing so you can beat them.

John: Good, good, good, good. Now Bob, I went into your background and we have three hours of your background here. Just give us a little thumbnail sketch with your background so people can get impressed.

Bob Gourley: Well, I don't know about impressed, but I was a Navy intelligence officer for 20 years, analyzing adversaries and trying to figure out what they're going to do next. And then the last several years of that, I was helping the Department of Defense stand up an organization that does computer network defense for the entire department. So we were the first operational joint task force for computer network defense. And then after doing that for several years, that was my baptism in this cybersecurity world, after doing that I worked at TRW at Northrop Grumman and then went back into government as the Chief Technology Officer at Defense Intelligence Agency, a global mission organization. Then from there I left and began consulting and formed this company, Cognitio, to deliver a lot of the high-end technology and cybersecurity consulting to commercial organizations.

John: I just want people to listen to that again. CTO of the Defense Intelligence Agency. No pressure there, right?

Bob Gourley: Yeah that’s right. Well, I tell you, when you have really good bosses that want to get stuff done and when you focus on a mission, stuff just gets done.

John: It's interesting, yeah. When a general wants to get something done, that happens. This isn't the hot seat, that was the hot seat back then. It's interesting.

Also, let's talk about top 25 most influential CTOs in the globe. So you're doing something right.

Bob Gourley: Well, there's always a bit of luck involved, but there's a lot of visibility is brought onto some of the activities that we were involved with at DIA.

John: Yeah, interesting. We're going to talk in general about cyber-attacks and satellite and space and everything else. A lot of the questions I have written down here, we couldn't really have asked 10 or 15 years ago. They're all kind of new. New space and new topics, and this is really a new generation of cyber-attacks, isn't it?

Bob Gourley: In many ways, it is. Now, there's some bad news to that, I ought to say, and that is a lot of these attacks actually begin very simply. Well, actually, now that you make me think about it, some of the oldest, most important lessons learned in cybersecurity are the oldest lessons in humanity, which is when there's a group of bad people that want something, they're going to keep trying and trying until they get it. And you see that throughout human history, whether you're reading Sun Tzu or Thucydides, bad people are going to keep coming and keep coming until they either succeed or until you beat them decisively.

John: My wife teaches classics, so she would have liked your pronunciation of that word. When I think about linguistically, talking about the threat landscape, that's how generals think about the threat landscape. The threat landscape now is in the air, isn't it?

Bob Gourley: It is. It's wherever our technology is, the bad guys are going to find a way to get to it. So something to keep in mind about the threat landscape is the most sophisticated threat actors are organizations, not individuals. It may be a small organization, but it's people working together, bringing different skill sets, and sometimes it's a large well-resourced organization. Those are the ones that really worry me.

John: Front page of The Washington Post, everyone's talking about IoT, and internet of things, sensors, and everything else, but you know there's a whole lot going out in space, as well, isn't there?

Bob Gourley: There is. There's a lot in space that others are depending on, whether you realize it or not. We all know there are weather satellites in space, and this very week it's so critically important to be tracking with precision where hurricanes are going. But we all know and rely upon GPS. It's just mind-boggling how many different industries rely on GPS. We all know that we also rely on satellites for our communications and it's just been a growing dependency. Every industry relies on satellites for communications. We can go on and on. Another key one

that we need to keep in mind is that we rely on satellites for remote sensing in order to do better, more predictive analytics for things like agriculture and mining and resource management. So we're all dependent on space now.

John: Now, Bob, I've got three grown kids. If I was in the car with them and drove somewhere and pulled out an actual, physical paper map, they would start laughing. It's just part of the culture now that you assume that there's geospatial information ready at your fingertips.

Bob Gourley: That's right. It comes over our cell networks or our WiFi networks and it's updated all the time. The GPS tells you exactly where you're located. If there's any kind of outage, we all feel it.

John: There was a TV show called "Star Trek," then there's "Star Trek: The New Generation" or something, but right now we have a new generation of cyber threats and coming from satellites in the aerospace sectors, aren't they?

Bob Gourley: That's right. There have been well-researched attacks, which have leveraged satellite command and control infrastructure to manage bot nets and deploy viruses and malicious code on Earth. And so, it's people who manage satellites having their command and control infrastructure taken over by relatively small criminal groups to manage their bot nets.

John: Clint Eastwood was in a movie called "The Good, The Bad, and The Ugly." I like talking about the bad, the bad guys. So who are the bad guys here? And what are their tactics? Is it a nation-state? Is it the mafia, if they even exist?

Bob Gourley: In general, keep in mind what I said before. It's organizations. You can have a very smart individual hacker who might be a hobbyist and put an antenna on their roof and communicate with satellites.

John: Unlikely, yeah.

Bob Gourley: But I know some of these guys and there are some very creative people who love playing with the space stuff. And fortunately, they're good guys, but they'll put an antenna on their roof and they'll listen to satellite command and control and figure out what it's doing, and if they were bad they could inject malicious stuff. But that's rare. The ones to worry about are the ones that have a little bit more resources. And the ones that are attacking the most are criminal organizations that have found ways to generate money by doing this.

For example, I mentioned running a command and control network for malicious code. Now, that is the most common attack. But the even more well-resourced organizations, the nations, if they decide to attack we're all in deep

trouble. So the attack from, say, North Korea against satellite command and control or against GPS could cause ships to go astray and many, many other impacts. If Russia decided to take out satellites, they could blind us. If China decided to do that, it could just decimate the nation. So the biggest, most powerful threat is the nation-states.

John: Now, you've been in the Navy and I wonder about those Navy ships that collided in the Pacific Ocean. Was this something that was malicious? Was this a judgment in error? Was this a satellite attack?

Bob Gourley: You know, I believe in getting the facts and not jumping to conclusions, but I would say, hypothetically, we need to explore the cyber angle to make sure that it absolutely was not. Because I have seen scenarios where a ship's systems could be attacked. It'd be easier to attack the systems on these large merchant ships, but I've seen no evidence of that. I believe what's happened here in this particular case is not enough time and training and leadership and standard operating procedures need to be followed. And I think that's what the investigation will lead to. But it's certainly okay for us to be thinking through the scenarios. What if it was a cyber-attack?

John: So what can an organization do about these types of threats?

Bob Gourley: You know, there's so many things. First, understand your most important data and your most important needs. So if your data could include things in your enterprise, which needs to be encrypted, your data is also stuff that is on the satellite or the airframe or the aircraft that you're trying to protect. Your data also needs to be communicated. So you need to protect those links. Now, it's a whole science and art about encryption, back and forth between satellites and on satellites. There's a lot of great gear that does that. But frankly, there's a lot of need for improvement.

John: Two days ago, I sat down with Stephen Hull. He's the CIO at Leidos. We had an hour conversation and we talked about artificial intelligence. Now, from his perspective, he thinks that artificial intelligence can help prevent attacks. I think there may be other people that are saying, "Guess what? Artificial intelligence can help us enable an attack, too. It's a two-edged sword."

Bob Gourley: That's right, and we're absolutely seeing this.

John: No kidding.

Bob Gourley: We are. We are absolutely seeing the bad guys leveraging the code that's being produced and provided out in open libraries that anybody can use. If you are a developer, you can download libraries to help you build an artificial intelligence

application. Maybe it's machine learning or a neural network approach, other kind of deep learning. You borrow other people's codes and then you build your solution on top of that. So malicious code, for example, can borrow machine learning capabilities to learn what's on your computer and what seems to be sensitive and only take the right stuff and zip it up and transmit it.

John: Whoever thought that GitHub would be used for something like this.

Bob Gourley: I know, everything the good guys can use, the bad guys can use.

John: You know, most software developers, they put something on GitHub and they think it's for managing a financial application or something. But this is actual malicious code that's up there and under the auspices of helping an organization, they can use it for malicious needs.

Bob Gourley: Right. We can use that example for so many other solutions, too, like AWS, which is one of the greatest benefits to the nation when it comes to cloud computing. Well, bad guys can find ways to stand up AWS instances and use it for things that nobody knows what they're doing but maybe they're breaking passwords, for example.

John: You have storage and compute, they have the whole computer system there ready to AWS, and almost for free.

Bob Gourley: Right. Then another thing, the internet. It's almost like the internet has been designed to serve advertisements to people who browse the webpage. It is very good at delivering advertisements. Well, the bad guys have figured out that they can quickly stand up a shell company, buy some ads, pay for those ads, target those ads to exactly who they want to read the ads. So get you reading ads, and then once that's working insert a little bit of malicious code into the ads, or have the URL that the ad directs you to have some malicious code on it. It's a very targeted precision use of malicious code by using a piece of the internet the way it's supposed to be used.

John: I talked to a Russian who was specializing in cryptography. And he said "Oh, that WannaCry, that's nothing. That's like fake news." He said, "You know, John, that's fake news. That's really not even to be worried about." And so, I think for the general listener or the general reader, it's hard to separate the fake from the real cyber-attacks, isn't it?

Bob Gourley: It can be. You need to get into the details. The facts are extremely important. Forensics are important. So one thing we advise every company to do is make sure you have a good ability to do forensics during an attack and after the

attack. Detect what's going on, store that in ways that researchers can come in and see what exactly happened.

John: Let's go from AWS to the sky. Let's talk about satellites and aerospace. So what do we know so far about attacks that have taken place in aerospace?

Bob Gourley: I'd say at the low end, there have been attacks from the ground to manipulate some of the old satellites, the less protected satellites. On the high end, very recently publicly disclosed, there was an attacked called Turla. The Turla attack was using the satellite command and control infrastructure by global companies in order to manage malicious code on the ground. It was the command and control network that was deploying bot nets. And upon analysis of the attack done by a company called Risk IQ, they determined that it only cost the attackers about $1,000 for some satellite equipment to be able to use the command and control system of these satellite providers.

John: Wow. I would imagine there's a chapter in your book, "The Cyber Threat," that may talk about this.

Bob Gourley: We do talk about the advanced threats and how easy it is to execute. And the reason we talk about it so much is it's also easy to build mitigation strategies to counter these threats.

John: And that's the good news.

Bob Gourley: Yes, that's the good news. You do have to care. You have to raise awareness to the point where people care. And if people care, you can mount economical defenses against a lot of these attacks.

John: If you take a look at the world and try to do a distribution of attackers, some people will look and say, "Well, there may be a geographic area that presents a specific threat." Are there geographic areas that are specific threats in the satellite business?

Bob Gourley: I guess it's very important to analyze things holistically. The Turla attack appeared to be coming out of a criminal group in Russia. One of the key research organizations that found the Turla attack was a Russian company. So both the good guys and the bad guys were there in Russia.

John: It's non-dualism. The front is the back.

Bob Gourley: That's right. But we are and I'm definitely an advocate for the rule of law, and if there's a country that does not have the rule of law and allows criminal syndicates to operate in it, I think civilized nations ought to figure out what to

do about that and establish the rule of law there or don't let them get on the internet.

John: So a lot of people say, "Look, I want end to end protection here. From the service provider, through the teleports, through the public networks." Is that a pipe dream?

Bob Gourley: Yeah, it can be, but there are things you can do to operate securely over a non-secure environment. For example, use encryption, end to end encryption of all of your communications from point to point. If you do that, you can operate over the internet. And when it comes to satellites, use encryption. Now, the current way of encryption is passing old fashion keys around and using high-speed encryption devices. New ways of encryption include something called a one-time pad, which is a massive size key totally random, only two keys exist. One on the ground and one in space. And this one-time pad is unbreakable by any kind of encryption means. You have to steal the pad in order to break the encryption. Things like this are revolutionizing the space architectures.

John: Well, here we are in the middle of NFL season, and coaches are looking at other teams trying to find vulnerabilities in their defense. Well, there's a vulnerability here, a vulnerability there. I would imagine that satellites have unique vulnerabilities, as well, don't they?

Bob Gourley: They absolutely do. And, of course, the challenge is if you have a software patch, it's hard to get it up to the satellite and install it.

John: Yeah.

Bob Gourley: So what do you do? If you allow over the air installation of new software, that's good, but what if the bad guys can do over the air installation of your software and put bad software up there? So these architectures have to be well thought out.

John: When you see what's going on in the space industry now, you see things like high throughput satellites, HTS. Does that make them more or less vulnerable to attacks?

Bob Gourley: Now I think that as long as it's designed in to begin with, it can be done very securely. The throughput is very high, the management of that, the command and control has to be well thought out and extremely secure.

John: Many of our listeners are satellite operators. So what can they do to protect against cyber-attacks?

Bob Gourley: Well, I think they need to keep their brain around the entire architecture. Of course people think about the space piece and the ground control of the space satellites, but do you also think about the admin system and your desktop PCs and the mobile devices that your employees use? Your employees in the satellite company are just like employees in any other company, they are your first line of defense. And an adversary that may want to hack your satellite may start by hacking someone who works in the mail room and use that to get increased access to get to the executives, and use that to get increased access to the technical team. Hop around through the infrastructure and accomplish their objectives. So keep your head around the whole thing and consider what protections you can levy across the entire enterprise.

John: When you look at security measures, are there differences in security measures between protecting the space segment and the ground segment?

Bob Gourley: There absolutely are, and I'm glad you asked that because too frequently we take old models and try to apply them to new things and it just doesn't work. Let me give you an example, for the last three years, I've been participating in a conference called the Global Connected Aircraft Conference. And we have raised awareness and brought information on the threat to the carriers and the many integrators in that world. And the first analogies people started coming up with are, "We would like to protect the cockpit of an aircraft by putting a firewall there."

And that's not a good analogy. You start thinking that through, and our firewalls here in the corporate world are managed by people, and there are security operation centers that make changes to those firewalls and continually manage them. We're not going to fly our aircraft with security operation centers onboard every aircraft. And extend that into space. Some of the old models are very important to use, but we're not going to have a security operation center on every satellite. We're not going to have a CISO and a CIO on every satellite. We have to design in the protections in ways that keep unauthorized access from occurring, even though no one is up there watching it and keeping the firewall configured.

John: If you look at the satellite business in the last few years, you can look at open systems and closed proprietary systems. And you can say, well, your father's Oldsmobile, the old system was proprietary. And the new ones are purpose built. And we use open standards now, and that results in lower costs and maybe innovative applications. But it also brings some risk, doesn't it?

Bob Gourley: It does. Both of these ... I mean, this is a great question, and it's the same question that a lot of us have been debating for 20 years now.

John: Terrestrial systems.

Bob Gourley: Yeah and I think we will continue to have this discussion 20 years later. It's such a very important topic. And so, the short answer is both of them have strengths, both of them have vulnerabilities. Both of them you really have to design in security to begin with. The proprietary systems, you can obscure a lot of things from hackers. The bad news is a proprietary system's generally have more vulnerabilities, they're just not discovered yet. So when a bad guy does discover them, you're going to have to mitigate them quickly. What happens if your proprietary system is in space, and the vulnerability is discovered? And we just talked about how hard it is to patch a satellite. You don't fly a guy up there with a disk. So a proprietary system, it needs to be really, really good.

Now, in the plus column, some of the greatest software code ever written is part of the US space program. There's great engineers developing that stuff, and I think that extends to our commercial providers of capabilities. So proprietary software going on satellites, it's generally well written, and it better be well written. Open source approaches, there's more eyeballs on it, so more chance of catching vulnerabilities before they go into space, but the bad news is that there's still vulnerabilities, and eventually they will be found. And when they are, everybody's going to see them.

John: We start off on the ground, we move to satellites. Let's make the jump to ... Not hyperspace, just outer space here. So is there a connection between cyberspace strategies for satellites and outer space?

Bob Gourley: Yeah, no, I think it's related, but it's very different. We have to think through the specific needs of the satellite systems. We can't use all of our old models just applied to the satellite.

John: Well, here we are in Washington, D.C., and so we got to talk about the regulatory framework. I mean, it's just down the road here, we got to talk about it now. And are there potential rules or maybe guidelines that you can see or suggest in the future for managing some of these cybersecurity threats?

Bob Gourley: Yes. So there's some things I really, really like. One is the NIST Cybersecurity Framework. And NIST for years has been helping pull together best practices. And really, for two decades, they have helped the federal government understand what needs to occur. And then they did this in an open way so the commercial world can borrow ideas. But the Cybersecurity Framework is something different. There they came up with a way that can help everyone get on a common taxonomy at a high level and understand the right words to use when talking about cybersecurity. That framework is easy to understand and easy to implement, easy to put in your policies and can just help all designers

and operators get on the right wavelength. And maybe more important, it can help executives talk about cybersecurity.

John: I love driving up to NIST. I always reset my watch because it's an accurate measurement, it's always really good. But beyond NIST, there's also private and public mechanisms that kind of work. There's these private and public partnerships are taking place with NIST. Are there ones you can suggest that maybe people should listen and learn more about?

Bob Gourley: Yes, so there's several. One of the great constructs that came out of the late '90s was the Information Sharing and Analysis Center. It was probably 1988, the ISAC concept was rolled out. The first was the Financial Services Information Sharing and Analysis Center. There's now an Aerospace Information Sharing and Analysis Center that is for not just aircraft, but for the space industry as well. It's a great way to jump in and learn more about what your peers are seeing and what attacks are occurring, and how to mitigate those attacks. So, that's a great way to do peer based networking and also learn the latest attacks.

John: I want to jump back to our earlier discussion about aircraft. Now, in 2015, there were around 5,000 aircraft that were connected. By 2025, that number could triple. All this interconnection is good. We've got connected cars, and with that this whole mobility concept, there's trouble inherent in that. I keep thinking of aircraft moving and a laser beam and many aircraft and flight control. This is a complex world.

Bob Gourley: It really is. It really is. And I'm trying to think of the right analogy there, but do you remember the movie, "Jurassic Park?"

John: Oh, yeah.

Bob Gourley: And as soon as you see the trailer for "Jurassic Park" and you see there's a lawyer on the expedition, you just know he's going to get bitten by the T-Rex, right?

John: Yeah. Everyone's praying that he gets bitten by the T-Rex.

Bob Gourley: Yeah.

John: I'm putting money on the dinosaur.

Bob Gourley: And then when that happens, you're like, "Aha! I knew." And some of us are starting to think that way about this coming globally connected all transportation devices, all aircraft, all cars, all barges, all rivers, and your entire internet of things at home, 600 devices in your home will have chips. And I'm

starting to think back to the movie "Jurassic Park." Something big is going to happen, and we're all going to say, "Aha! I told it was going to happen."

John: Yeah. When you look at the number of satellites out there ... I mean, they're not just putting one satellite the size of a Chevy in the sky. They're putting eight and 10 and all kinds of satellites coming up there, and I want to talk about the trouble with tribbles. I mean, if you look in the sky now, all of a sudden there's debris, there's new satellites, there's interference issues. I mean, there's issues now that if my son were to go into aerospace, he would be dealing with issues that I couldn't even conceive of today.

Bob Gourley: Right. And so, a lot of these satellites are purpose built. They're using commercial, off the shelf hardware and software and sensors designed for other things. And they're being seeded all over the globe. I guess the good news is a lot of those are designed with a low life cycle in mind, and will deteriorate shortly. So you see them with new ones. So they do have a way to continually upgrade these satellites, and there's a need for new approaches, I guess is what I would say.

John: I'm not going to end this podcast without a plug for your book. Tell us about "The Cyber Threat" and where can I get it?

Bob Gourley: Well, "The Cyber Threat" is available online at theecyberthreat.com or at Amazon.com. But "The Cyber Threat" is really to help executives understand the threat and what they should do about it. It makes the key point that cybersecurity is not just an IT issue. The technology's incredibly important, but reducing digital risk is a responsibility of every executive and every employee. So I wrote this book with that in mind. It's not a technical book, it's a business executive leadership book.

John: And digital risk is not just financial, it's also in the area of controlling satellites and executives have to understand exactly what's going on in the sky in order to manage it well in the future.

Bob Gourley: Right, absolutely. It connects to everything. If there's an attack against space systems that causes your delivery trucks to be late, that's an attack that impacted your business.

John: The pizza delivery guy could be impacted by what's going on in outer space, then.

Bob Gourley: That's right, that's a fact.

John: That's not good. I'd like to thank our guest today, Bob Gourley. He's co-founder and partner of Cognitio, and publisher of CTO Vision, and also the author of "The Cyber Threat," if I'm not mistaken.

Bob Gourley: Right.

John: Thanks a lot, Bob.

Bob Gourley: Thanks.