Constellations Podcast

Episode 201 – GPS, LEO and the Speed of Decision

Speaker: Ian Canning, President and CEO, Eutelsat America Corporation and OneWeb Technologies Inc. (EACOWT) – 16 minutes

John Gilroy: Welcome to Constellations, the podcast from Kratos. My name is John Gilroy and I'll be your moderator. Today, we'll be talking about strategies to augment and support GPS capabilities. Due to the fighting in Ukraine and the Middle East, disruption in GPS is currently affecting global air travel, but there has been concern about the vulnerability of GPS and other global navigation satellite system signals for decades. Our guest today is Ian Canning, President and CEO of the Eutelsat America Corporation and OneWeb Technologies Inc., commonly known as EACOWT. Ian, how are you?

Ian Canning: Very well, thank you. And thank you for having me here today.

John Gilroy: Good, good, good. Well, I went to your LinkedIn profile, saw your background. Wow. It's going to be pretty impressive. We've got some funny questions for you today. It'd be great.

Ian Canning: I've been around the industry for too long.

John Gilroy: Yeah, I know. It's going to be great. Can you share with us some examples of the overarching problems being experienced by the U.S. government and commercial entities when working with or depending on GPS for position, navigation and timing?

Ian Canning: I think many of us don't realize just how dependent we all are in our day-to-day lives on GNSS, and that's sort of the broadest answer for GPS, yeah? GPS is the U.S. global position satellite system, and then there are multiple services that build up the GNSS services as a total capability. But our phones rely on it, we rely on it for our mapping, we rely on it for knowing accurate time, et cetera, et cetera. It is just pervasive in so many things that we actually do today. And the government are just as reliant on it as commercial entities. And whether that's for timing of banking systems, whether it's for accurate positioning of an airplane, whether it's for just accurate positioning of where your car is, can you actually get home, what are the back roads, what are the routes today, all rely on one form or another of GNSS.

John Gilroy: Yeah, when you talk about banking, I mean that's essential to all Americans and it's really front and center. People never even think about it, do they?

Ian Canning: And banking doesn't naturally rely on GNSS or position, which many people think GNSS is position, but it is position, navigation and timing. And probably one of the most critical components of it is timing and everything yet relies on an accuracy of time.

John Gilroy: For our audience, can you explain the difference between jamming and spoofing and why is timing, again, why is timing so important here?

Ian Canning: So jamming is quite simple. You can imagine, if you put out a strong signal that overrides that GPS signal, that will effectively block it, it will jam that signal. So that's a very simple way of being able to identify it. And unfortunately, the technology to be able to do that is readily available and it's really cheap. Yeah. So that's becoming far more pervasive. Spoofing, that starts getting more challenging. And what you're really trying to do at that point is trick the receiving system to still see a signal for that signal to still look like the traditional GPS signal or the timing signal, but it may be just offset either in a location, it might be offset by 10 meters, yeah, 50 meters or so on. Timing may be slipped by half a second. And you can then start doing all sorts of things within that scope of differentiation.

John Gilroy: OneWeb operates in LEO. How can an operator in LEO enhance resiliency for government communications, particularly in GPS challenged environments?

Ian Canning: So we came to this because the OneWeb network as a highly complex 4G network in the sky is actually very reliant on timing and position to be able to accurately send our signals back and forth and keep that connectivity going. So as we relied on that accuracy and we were starting to go into areas of either jamming or spoofing, we needed a solution to meet the timing and position requirements of our network. So that led us to starting to review what potentials and opportunities were there yet for us. There wasn't anything generally naturally in the market. So that led to us doing some developments that bought an alternative, not saying it's the only one, but an alternative to GPS.

John Gilroy: So Ian, with increasing threats to GPS, as you described them here, including jamming and spoofing, how does a LEO operator help the U.S. government maintain situational awareness and positioning accuracy in these contested environments?

Ian Canning: We have an accessory that effectively actually will gather all of the GNSS signals, so all of them, not just GPS. So that's maybe up to four or five different signals. It will also actually potentially bring in the Iridium signal, which is slightly more robust and it has a different signature. And that allows us to do two things. It allows us to map across those different signals and identify particularly if there's

spoofing happening because it's very rare to see spoofing accurate across all of the signals. So if you can eliminate the spoofing, that is good.

And then should we detect actually a jamming situation or an untrusted source of timing and position, we will then actually go into what's called a holdover mode to actually sustain that signal for up to a four-hour window at 200 nanoseconds accuracy for timing, which is actually pretty accurate timing. And that's what we needed as a network to be able to operate. But we've actually learned that there are many other people that need that level of capability as well, U.S. government being one of them.

John Gilroy: I just cavalierly used that term timing. I never thought it was down to the 200 nanoseconds. I mean, this is very, very precise here. It's not a casual, we don't throw that out there in this community, do you?

Ian Canning: No, you do not. But you hear about it these days. And go back to that banking example right at the beginning. If you think of trading and how accurate trading needs to be and what can be done within timing windows, the accuracy of time is really important.

John Gilroy: Can you explain how a LEO network combined with Iridium could serve as a complementary or backup position, navigation and timing solution where GPS is compromised?

Ian Canning: So as I say, in that scenario where it is compromised, first and foremost, we'll identify what the compromise is. How is it compromised? Is it either spoofed or is it jammed? We'll eliminate where we can any spoofing and then maintain a modulated consistent GPS signal for the system. When we need to, we'll fall into holdover mode. Yeah, and then as I say, for that four-hour window, we'll be able to keep that level of accuracy. Some systems don't need that level of accuracy, so you can hold it for longer. But the 200 nanoseconds was important for us in that four-hour window. At any point in that holdover window, if we reacquire a trusted signal, whether that be from the Iridium network or from one of the GNSS sources, we can then actually re-trigger and sustain that underlying capability.

John Gilroy: Secure and resilient communications are critical for military operations. How do you ensure SATCOM services remain protected from cyber threats and spoofing attempts?

Ian Canning: So I think we all have to acknowledge these days that you cannot stop all of the threats that are actually out there. So you have to mitigate the threats where possible and eliminate them where you possibly can. And to that event, we are doing all of those different things really to try and mitigate the situation and

therefore provide options which provides resiliency to the government and the user community.

John Gilroy: The U.S. military relies on a mix of satellite systems. How do you integrate with existing DoD communication architectures and what steps are being taken to ensure seamless interoperability across services?

Ian Canning: Great question. And something that many, many of us have worked on diligently the years. The DoD had been very reliant on their own constellation of highly secure capability, but the demand for bandwidth, the demand for connectivity is just outstripping the pace at which they can actually deliver it. So that then opens the opportunity for the commercial SATCOM industry to actually come in and augment. And some would actually say we're now probably providing the greater majority of the communications for U.S. and other governments, and that then needs to be seamlessly integrated.

We're blessed that in today's environment of IP networking and so on, it's very much easier to blend IP capability, whether that's through different network technologies of SD-WAN or other capabilities to actually then amalgamate a system and give options to the warfighter. So maybe his preference in an uncontested environment is a very high bandwidth, COMSATCOM solution, but if that should become compromised or unavailable for a reason, then he can fall back into other networks and other solutions and then relying on the government networks for that absolutely critical communications as needed.

John Gilroy: Ian, I don't know if you remember back in 2024, but I was mandated to say zero trust every now and then, but every 10 minutes. Now we have new mandate here in 2025. I got to say AI, so I got to have the AI question. No choice here. So with AI driven analytics and edge computing becoming more relevant every day, are you incorporating these technologies to enhance space-based communications and PNT solutions for the U.S. government?

Ian Canning: I think AI provides us a huge capability enhancer as we move forward. But I think also it's got to be used sensibly and taken full advantage of. AI, machine learning, how do you put all of that together? But I think it allows us to be far more dynamic in our approach maybe to communications. We talked just a second ago about resiliency. There's the joy of orchestration these days between all the different networks and often that orchestration is going to rely on a form of either machine learning or AI to build its knowledge and to build its capability and to bring that situational awareness together to then be able to provide the right picture to enable the right decisions at the right time. And I think that's where AI can really come in in terms of identifying the information, speeding up the decision-making, and then potentially even taking those decisions as we go forward.

John Gilroy: Ian, in a near-peer conflict scenario where adversaries may target GPS and traditional communications, how can the combined LEO and Iridium services ensure uninterrupted connectivity and secure data transfer for military operations?

Ian Canning: As I say, you can never be a hundred percent certain of things and you have to acknowledge that. But in being a LEO network, and we're a proliferated network, there are many satellites up in the network, it's very much harder, let's say, to target taking out a satellite or a constellation as you would've traditionally done in the GEO sense, very easy to point at a known point in the sky and potentially eliminate that satellite connectivity at the time. Much harder when you've got satellites flying at 1,700 kilometers an hour, actually swapping satellites every two and a half minutes, changing frequencies every 11 seconds. It just provides a very highly dynamic environment that's much harder for our adversaries to actually target.

The other thing we have to acknowledge is at times, and particularly in and around GPS and denial of service there, we're not the only ones reliant on position, navigation and timing for our systems. They are too. And that's where that four-hour holdover window really came from. It's rare in the field that you see periods of full denial of service that run longer than that.

John Gilroy: Looking ahead, what role do you see LEO playing in the evolution of U.S. military satellite communications and what capabilities are on the horizon to further support government needs in the GPS contested battle space?

Ian Canning: So going back to we talked about the demand for connectivity is just increasing, increasing, increasing, and that's driven by that need for speed of decision. We're seeing edge compute grow dramatically in the field. That's actually enabling the warfighter in a local environment to be more dynamic. But you need that global situational awareness. So it needs to feed back into the overall CONOP and the overall situational awareness picture. So LEO facilitates that in a different way than traditional COMSATCOM because we have much lower latency, there's a more dynamic network environment.

There's information that we gathered from the networks to be able to see what's going on more readily. So yeah, lots of opportunity for us to do so. And the government are changing their practices too. I think we have to acknowledge that. And they are wanting to use the latest technology and that latest technology doesn't like latency. It likes being connected to a terrestrial network. And sometimes when the warfighter is at the sharp end, that's not where he is, and therefore we bring that as close to him and enable that as closely as we possibly can.

John Gilroy: Ian, I think you've given our listeners a better understanding of GPS resiliency and many aspects thereof. I'd like to thank our guest, Ian Canning, President and CEO of the Eutelsat America Corporation and OneWeb Technologies Incorporated, commonly known as EACOWT.