Navigating the cybersecurity threats and challenges in MilSatCom

18 September 2024 Adam Jeffs, Editor, SAE Media Group

Jennifer Krolikowski, former CIO for Space Systems Command, shares her views on the threats, challenges and solutions for securing MilSatCom against cyber-attacks.

Image Credit: MIT Lincoln Laboratory

As the cyber landscape evolves alongside increasing threats to satellite communications, the importance of cybersecurity in the MilSatCom space is becoming more critical than ever. However, there is often uncertainty around how the complexities of securing sensitive communications and ensuring resilience against sophisticated attacks should be navigated.

SAE Media Group spoke with Jennifer Krolikowski, CEO at Plan Z and former Chief Information Officer for Space Systems Command, ahead of the Global MilSatCom 2024 conference, where she will chair the cybersecurity focus day. Krolikowski discussed the key threats and vulnerabilities in SatCom cybersecurity and what needs to be done to secure against them.

SAE Media Group: What are the major vulnerabilities that current SatCom cybersecurity has?

JK: Any time you are dealing with ones and zeros, there is a chance someone will try to compromise your system and exploit your data. For space systems, there are three routes for an attacker to try to breach the system: the ground system, the uplink/downlink and the space vehicle. Each has different techniques and barriers to entry for exploitation.

Unfortunately, exploitations are dynamic, meaning as software is updated throughout the years in any of those segments, new vulnerabilities can and do emerge. Just because you patch a particular vulnerability today, it does not mean your system is secure forever. Cybersecurity is an ever-present concern, just like adding functionality is. I would venture that the major vulnerability to a system is complacency towards its security throughout its entire lifecycle.

SMG: In what way are these vulnerabilities most likely to be exploited? What are the most prevalent threats?

JK: A hacker is going to try to find the easiest route to take in order to get into a system. Making the process too lengthy or too costly for their perceived gain often deters them from pursuing a system. This is where they love finding back doors, especially as we are moving towards systems of systems. In the world today, we want *everything* to be connected so we can more easily accomplish a workflow or a kill chain.

However, when each of these individual systems are built in a silo, they often have different security requirements or risk tolerances. For example, a high

value asset like missile warning would naturally have more protection controls in place during its design and operation than, say, a weather satellite.

But now, as you are linking these two systems, vulnerabilities can be introduced to the integrated system as a hacker may find an easier way to get into the weather system and subsequently get access to the missile warning system. Vulnerabilities that develop at the integration seam need to be addressed in order to secure the ecosystem as a whole.

SMG: What are the primary challenges the industry faces with regard to getting SatCom cybersecurity where it needs to be?

JK: The biggest woe that a lot of CIOs face, and I saw this as a CIO myself, is the balancing of resources between security and functionality. Many see it as an 'either or' rather than a symbiotic relationship. If a system is hacked and taken offline, your functionality and availability goes to zero, regardless of the hardware 'availability' requirements levied and built into the system.

However, you do not want the system to be so heavily protected that the users cannot even use it. So there is a balance that must be struck. That balance ultimately depends on the risk one is willing to assume, and the costs associated with mitigating that risk, versus accepting the risk and suffering the consequences if it realises into a problem.

The other big challenge stems from the creation of the ecosystems I mentioned before and the vulnerabilities that start to form at the integration seams. Each system may be secure in its own right, but as you bring them together, is that seam as secure as it should be? Typically, many authorising officials care about what is in their specific boundary and work to secure what is inside that. There has yet to be much identification as to who is responsible for the security between those now integrated systems.

SMG: How will the current technologies and strategies need to be developed to ensure the security of SatCom assets against cyber-related threats?

JK: The biggest way one can help is by designing security into the system while it is in development instead of trying to shoehorn it in at the end when you are trying to deploy it. Waiting until the end puts the operator or user in an untenable position where they need to decide if they will send the developer back to refactor the system to make it more secure, thereby delaying capability and increasing costs, or if they will take the system as is because the functionality is so dire and assume the risk of it being exploited. Either way, it is a losing proposition.

The other aspect is that security needs to be recognised as something to be addressed in every phase of a system's lifecycle. Security is not a 'one and done', because rarely are our systems 'one and done.' Think of the cell phone and how that has evolved over time. The phone of today looks nothing like the phone 10 years ago, so we should not expect the security controls to be the same either.

As nothing can be tested to completely rule out every issue, the system has to be flexible enough to be 'fixed' quickly when a vulnerability is discovered and starts being exploited.

SMG: The Global MilSatCom 2024 conference will feature a full day focused on cybersecurity, why is it so important that the industry comes together to collaborate on this issue?

JK: Communication is the cornerstone of all military action. Comms are used to transport data or information so leaders can communicate decisions to command-and-control forces to take action and win. Without comms, it would be extremely difficult to prosecute wars with any hope of success.

Therefore, it is vital that we ensure resilience in all aspects of the SatCom system, from the data being transmitted to each element of the system involved in the transporting, so the communication functionality can endure.