Space as a War Domain

The threats looming in orbit, and the tech needed to thwart them.

Amanda Ziadeh

Mon, 09/10/2018 - 10:48

Photo Credit: BrendanHunter/iStock

Outer space is home to many of the nation’s dependencies, including satellites that provide TV channels and advanced communications, and robots and aircraft that allow us to explore outside Earth. But it’s also a new war domain, and all those systems pose potential cyberthreats.

“Cybersecurity is a major part of our space resiliency,” said retired Lt. Gen. Kevin McLaughlin, founder and president of McLaughlin Global Associates LLC and former deputy commander of the U.S. Cyber Command.

McLaughlin spoke Sept. 6 on a panel at the Billington Cybersecurity Summit in Washington, D.C., about the cyberthreats associated with space systems and how to thwart them.

Securing the nation’s weapons systems is a must, and the government is adding space to that spectrum. For example, in the Defense Department’s FY2019 budget request, “space and cyberspace as warfighting domains” is recognized under the National Defense Strategy, and DOD plans to prioritize investments in cyberspace capabilities, including operations to ensure it can use space and cyberspace even while under attack.

The Air Force also created the Cyber Resiliency Office of Weapons Systems last year with focuses in acquisitions to analyze all platforms of each cyberspace system for vulnerabilities, McLaughlin said. And at the tactical level, DOD works with industry to develop cybersecurity-focused capabilities to help secure the command and control side of its space systems.

But the more active U.S. becomes in space, the more vulnerabilities there are, and room for inadvertent situations, Victoria Samson, the Washington office director of the Secure World Foundation, said in the panel with McLaughlin. It’s not always clear what happens to space systems or satellites when they go down because they’re unreachable, but if misunderstandings happen on Earth, imagine those that can happen in orbit.

So, What are the Threats to Cyberspace Systems?

George Gonzales, the chief of the operations branch of the Air Force’s MILSATCOM Ops Support & Sustainment Division, broke down the space system into three major segments: space, end-user equipment (which usually interacts with the system passively) and ground command and control.

”To me, the most vulnerable, the most interesting aspect of that system of systems is the ground command and control system,” he said in the panel with Samson and McLaughlin. If that system is compromised, an adversary can reach many other systems in government that it manages and touches — even software, processors and user data.

So, those ground controls are the most important to fortify, according to Gonzales.

But it’s the entire space system supply chain that creates the pieces, too, McLaughlin pointed out. All the parts and pieces that are deployed, and all the systems touching are integrated and interconnected, down to the industrial base that builds the systems and the vulnerabilities those may have. From a cybersecurity perspective, those layers have to be analyzed for flaws.

The space community as a whole needs to use the broader cyberframework that already exists for complex IT systems, McLaughlin said.

Securing Cyberspace

The commercial sector has a huge role to play, considering many of the satellites in orbit belong to industry. The security of satellites sent up 25 years ago will vastly differ from the security of those sent in the next 10 years.

But “you’re only as strong as your weakest link,” Gonzales said. If the commercial industry adopts risky and vulnerable practices, all the systems in space become vulnerable, too.

Ideally, Gonzales said he’d like industry to work with all its partners — in and outside government and internationally — and “work to a certain set of standards to fortify their systems.” This way, the community can implement the same kinds of cybersecurity standards across the board.

McLaughlin even suggested making space one of the nation’s 16 critical infrastructure sectors, and to create structures within it and form an Information Sharing and Analysis Center specifically for space to share best practices and threat intelligence.

“If it’s working in other areas, why not think about applying that to space?” he asked.

And Samson agreed, information sharing and transparency about threats and attacks is something both industry and government should prioritize and invest in to secure cyberspace systems, she said.

What About Technology?

McLaughlin said the cyberspace community will also have to focus on new features, because aside from the large IT systems on the ground, space is a unique domain.

“I do think the machines that we fly in space, they are unique because we put them up there,” he said, and those can’t be pulled back down when something goes wrong.

That will require autonomy, and the ability for these systems to self-heal, self-service and self-program when needed. We’ll need to have that level of sophistication on the cyberside of those attributes for the part of the system we can’t get to in space, McLaughlin said.

And for the space systems in orbit, these defenses and new capabilities will have to be designed in-depth and upfront, Gonzales said. The satellite industry and manufacturers will need to start designing agility into their systems, with the proper capacity, processing and memory.

Gonzales pointed to artificial intelligence and machine learning, too, so a satellite becomes capable of monitoring itself.

“So it’s self-aware, self-healing . . . those kinds of things have to be baked into the design upfront,” he said.

View printer friendly version

space
cyber
cybersecurity
DOD
Air Force
AI