Found in **Cybersecurity**

10 Takeaways From Cal Poly's Space Cyberattacks Report

A recent Cal Poly report on outer space cyberattacks examines contributing factors behind the rise of space cyberattacks and what is needed to address them.

IN THIS ISSUE

June 25th, 2024

Patrick Lin

Recently at Cal Poly, we released a 95-page report on outer space cyberattacks, funded by the U.S. National Science Foundation. As the first of its kind, it explains not only what is driving this growing problem, but also how to anticipate novel scenarios to avoid being taken by surprise.

Here are the 10 top findings from that report:

Space Cybersecurity is an Invisible Threat

Most people are unaware of how dependent the modern world is on space services. Maybe they understand that GPS is helpful when they need to drive, but it's so much more than that. Also, space systems can be incredibly complex, which means vulnerabilities can slip in across a long supply chain, as well as across the years or even decades needed to build a major spacecraft. As a result, space systems can be 10 years behind on cybersecurity upon launch.

We're in a New Space Race Now

By all accounts, space is getting more congested and contested. For more than a decade, we are seeing exponential growth in the number of objects launched in space, which had been more or less constant since the mid-1960s. Both nation-states and private actors are rushing into space in what some see as another "gold rush" and all that it implies.

Cyberattacks Look to be the Primary Mode of Conflict in Space

The remoteness of outer space means we can’t just swap out a server on a satellite anytime we want, as one example. This puts a limit on how far we can harden cybersecurity defenses, and that cyber insecurity gets worse over time — making space systems an attractive target for hackers. The very serious threat of space debris also pushes us toward space cyberattacks in a conflict: unlike kinetic or physical attacks, cyberattacks generally don’t blow things up and don’t make the debris problem worse.

Failure of Imagination is a Huge Risk in Security Planning

Imagine if defense agencies talked vaguely about “hacking a computer” as their only scenario in securing their networks. That’s not very helpful to cyber defenders given the countless ways and contexts such a hack could happen, and it practically guarantees you’ll be taken by surprise. Something similar is going on in space cybersecurity where typically the only scenarios ever raised are vaguely about “hacking a satellite” or “jamming (or spoofing) signals.” We need a much fuller range of plausible scenarios to avoid tunnel vision.

Existing Taxonomies Don't Help With Imagineering

A taxonomy can help think through a problem-space, and very capable ones exist that catalog the various techniques a hacker could use. But for the purposes of anticipating novel scenarios in outer space, that's not enough, as the next point below also explains. Existing taxonomies tend to be either too technical for an exercise in imagineering or too general to be relevant to the space domain. Imagineering is crucial because threat actors are already creative and resourceful; defenders need to keep pace.

The Who, What, Where, When, and Why are Crucial

More than an inventory of how a hacker might exploit a system, we need to consider a wide range of threat actors, their motivations, their victims, and the space capabilities affected. Together, these variables answer the who, what, where, when, why, and how of a scenario. The ICARUS matrix we've created can generate more than 4 million unique scenario-prompts to kickstart the forecasting process.

Unexpected Scenarios Could Happen Tomorrow

We can be surprised by some space cyberattack scenarios that are possible in the immediate future. Here's one, out of the 42 scenarios we offer as a starting list to begin priming the imagination-pump:

Ransomware: is this an inconvenient time? Data can be more valuable than money, especially if it's critical data that can't be accessed when needed. Imagine if a ransomware attack were initiated on a rocket in mid-launch of a payload worth $1 billion or more. There would be great incentives to pay a ransom of $5 million or even $50 million in bitcoin to prevent a failed mission and lost payload. Similarly, ransom demands for spacecraft returning to Earth would be very difficult to refuse, especially if they were crewed or could potentially crash-land in a heavily populated area.

Diversity of Threat Actors Require a Diversity of Experts to Tackle

Hackers are not a monolithic group, despite stereotypes. They can range from the basement hacker to organized crime to cyber mercenaries to political terrorists to religious cults to chaos agents and many others. As such, their motivations are also diverse, as well as their intended targets and so on. Interdisciplinary teams are thus needed to understand these threat actors and scenarios, which may require different strategies to guard against or in a response. Group-think can be as fatal as tunnel vision.

To Solve a Problem, You Must First Understand It

Our report unpacks seven contributing factors behind the rise of space cyberattacks. A few are mentioned above, such as the new space race, complexity of space systems, remoteness of space, and space debris. Other factors include the well-known ambiguities and gaps in both cyber law and space law, since unclear law doesn't help much with deterrence or keeping the peace. Commercial space in particular is under-regulated, which creates room for misunderstandings and misdeeds; this, in turn, can fuel tensions and resentments, potentially creating a conflict.

The Stakes are Unusually High in Orbit

Related to the first point, most people don't know how much critical infrastructure is in outer space, delivering services and data that the modern world requires every day. Also, with Russia's hacking of Viasat's satellite internet equipment at the start of its invasion of Ukraine in 2022, we're now in the middle of the world's first "space war" where both sides are using space capabilities. Tensions are dangerously high for geopolitics now, and Russia's dramatic declarations that hacking their satellites would be an act of war highlights just how mission-critical space capabilities are to modern militaries.

All this means that the shroud of mystery around space cybersecurity must be lifted to prioritize and attract a broader range of experts and other stakeholders to the problem. Just about everyone in the modern world is a beneficiary of space services, which means we are potential victims, too. For more details, check out our new report here.

Patrick Lin, PhD, is the director of the Ethics + Emerging Sciences Group at Cal Poly, where he is a philosophy professor. He also serves on the U.S. National Space Council's Users' Advisory Group (UAG) and is affiliated with Stanford Law School, Czech Academy of Sciences, World Economic Forum, and Aurelia Institute.

Photo: Shutterstock