Found in **Opinion**

Why Space Cybersecurity Needs More Imagination

The ICARUS matrix is designed to unlock a range of possible cyber scenarios to plan for threats.

IN THIS ISSUE

October 30th, 2024

Patrick Lin

In our recent Cal Poly report, we introduced the ICARUS matrix to generate novel scenarios in outer space cybersecurity. It's meant to guard against a failure of imagination, a key risk for any security planning.

In conversations about space cyberattacks, at least unclassified ones, only a couple generic scenarios are typically trotted out — namely something about "hacking a satellite" and "spoofing (or jamming) signals" such as GPS. But this grossly understates the risk.

Compare that to worrying about "someone hacking our computers" in everyday cybersecurity. It's far too vague for practical guidance, as there are countless ways a threat actor can break into digital systems. Limiting yourself to just a few generic scenarios can create tunnel-vision and practically guarantees you'll be taken by surprise.

And hackers love to surprise us. Humans are incredibly creative and resourceful (when we want to be), so we'll continue to be caught off-guard by future zero-day exploits and inventive tactics not seen before or expected. But there's hope: if attackers can imagine it, so can defenders.

For space systems, the challenge is even more daunting. They're among the most complex technologies ever invented and can have much wider attack-surfaces and more vulnerabilities than other systems have. To avoid tunnel-vision, the ICARUS matrix is designed to be an imagination-pump, unlocking a full range of possible cyber scenarios. The name is an acronym for "Imagining Cyberattacks to Anticipate Risks Unique to Space."

With ICARUS — click here for a customizable download — more than 4 million scenario-prompts can be generated, as the starting bones of a scenario. In our report, we describe a sample set of 42 scenarios, ranging from immediate threats to more distant possibilities.

For example, one scenario is about what ransomware looks like against space systems. If the extortion occurred as a billion-dollar payload were in mid-launch, or as astronauts were reentering to Earth in a capsule, the incentive to just pay up would be nearly irresistible.

Or think about the 1938 “War of the Worlds” radio broadcast that incited panic since many listeners didn’t realize it was only a fictional drama of an alien invasion. Today, if audio data of what sounds like a xenomorphic language were slipped into the listening feeds of METI, that news story could potentially crash financial markets and spawn other chaos in a similar way.

How Does ICARUS Work?

Right away, you might see that the ICARUS matrix — a 5 x 20 lookup table — looks like something out of a Dungeons & Dragons gaming manual. That’s by design so that it would be useful in simulation or tabletop exercises, but also to organize thinking around space cyberattacks.

The five columns capture the major categories of interest: threat actors, their motivations, their methods, the victims or stakeholders involved, and the space capabilities affected. The 20 rows contain different variables for each category, which aren’t meant to be complete but only an initial set of variables.

The idea is to pick a variable from two or more columns as a scenario-prompt. For instance, if we pick organized crime as our threat actor, fraud as their motivation (e.g., stock-price manipulation), and a payload launch as the space capability it wants to sabotage, that can be the start of a scenario to be further developed. Critical-thinking questions in our report assist with that development.

ICARUS imposes a method to the dark art of "imagineering" security threats. The matrix helps to answer the main questions about a scenario: the who, what, where, when, why, and how. The threat actor is about who; the motivations are about why; the method of attack is about how; the victims or stakeholders are a different who question; and the space capability affected is about what.

Note that when and where are only indirectly captured here, as they aren't really variables but dependencies. For a scenario about hacking Voyager 1, the where would be beyond our solar system in interstellar space, because that's where Voyager 1 is. For a scenario about hacking a Martian colony, the when would be in the distant future, around 2050 or much later, because it will take us that long to set up an off-world colony, if ever.

Not all variable combinations make sense or are plausible. That's OK since it's still instructive to understand why those combinations don't work. For example, a man-in-the-middle attack (the method of intercepting and altering communications data) would be unlikely on satellite signals down to Earth (the capability affected), because there's no obvious "middle" in that scenario; those signals reach an attacker's satellite dish about the same time as they reach other dishes.

Why Not Other Taxonomies?

While ICARUS resembles a taxonomy, it's not formally one since there can be overlaps among the variables. Still, it can be useful like a taxonomy by wrapping a logic around a problem-space to systematically explore it. A taxonomy can help identify or track certain elements, map their relationships to other elements, discover patterns in the domain, and so on.

Other cybersecurity taxonomies exist and are very capable, but they weren't what we needed. Some were too technical or detailed, which is great for their purposes but not so useful for our broader audiences that include policymakers and interdisciplinary researchers. Other taxonomies were too general or simplified, again fine for some purposes, but they didn't account for the unique features of the space ecosystem and space capabilities.

Those taxonomies also weren't designed to produce scenarios. They address how a threat actor might exploit a system, but not so much the who, what, where, when, or why. Not all cyber incidents are alike, so a one-size-fits-all remedy or response doesn't exist. The details matter, and scenarios can fill in those blanks.

Above all, scenarios are invaluable because they tap directly into our psychology. Whether it's around prehistoric campfires or digital ones today, humans are hardwired for stories, which is what scenarios are. Imagination helps to tell new stories, the kind that hackers are also scripting. These stories bring to life the urgency, dramatic stakes, and human impact that a technical taxonomy cannot.

The work of space security is both an art and a science, more so than other less-complex domains. Imagination bridges the twin worlds of the creative and the analytic, closing a feedback circuit that powers a flashlight into the future — the power of foresight. Even a tiny glimpse into what's possible can be most illuminating to avoid surprise and plan more effectively.

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.