THE CONVERSATION

Academic rigor, journalistic flair

Complex space systems like the International Space Station could be vulnerable to hackers. NASA, CC BY-NC

To guard against cyberattacks in space, researchers ask ‘what if?’

Published: July 3, 2024 8:23am EDT

Patrick Lin

Professor of Philosophy, California Polytechnic State University

If space systems such as GPS were hacked and knocked offline, much of the world would instantly be returned to the communications and navigation technologies of the 1950s. Yet space cybersecurity is largely invisible to the public at a time of heightened geopolitical tensions.

Cyberattacks on satellites have occurred since the 1980s, but the global wake-up alarm went off only a couple of years ago. An hour before Russia’s invasion of Ukraine on Feb. 24, 2022, its government operatives hacked Viasat’s satellite-internet services to cut off communications and create confusion in Ukraine.

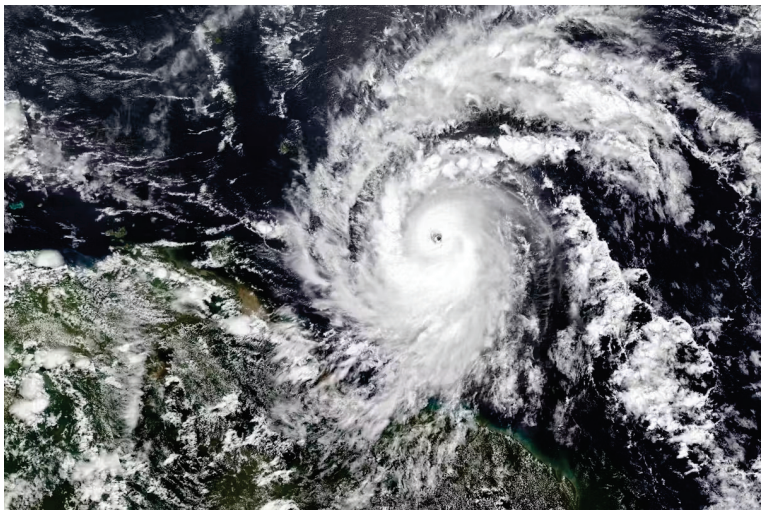
I study ethics and emerging technologies and serve as an adviser to the U.S. National Space Council. My colleagues and I at California Polytechnic State University’s Ethics + Emerging Sciences Group released a U.S. National Science Foundation-funded report on June 17, 2024, to explain the problem of cyberattacks in space and help anticipate novel and surprising scenarios.

Space and you

Most people are unaware of the crucial role that space systems play in their daily lives, never mind military conflicts. For instance, GPS uses signals from satellites. GPS-enabled precision timing is essential in financial services where every detail – such as time of payment or withdrawal – needs to be faithfully captured and coordinated. Even making a mobile phone call relies on precise coordination of time in the network.

Besides navigation for airplanes, boats, cars and people, GPS is also important for coordinating fleets of trucks that transport goods to stock local stores every day.

Earth-observation satellites are "eyes in the skies" with a unique vantage point to help forecast the weather, monitor environmental changes, track and respond to natural disasters, boost agricultural crop yields, manage land and water use, monitor troop movements and much more. The loss of these and other space services could be fatal to people vulnerable to natural disasters and crop failure. They could also put global economics and security at serious risk.



Many satellites are crucial for tracking natural and human activity here on Earth. NASA

Factors in play

In our report, we identified several factors that contribute to the increasing threat of space cyberattacks. For instance, it's important to recognize that the world is at the start of a new space race.

By all accounts, space is becoming more congested and more contested. Both nation-states and private companies, which are underregulated and now own most of the satellites in orbit, are gearing up to compete for resources and research sites.

Because space is so remote and hard to access, if someone wanted to attack a space system, they would likely need to do it through a cyberattack. Space systems are particularly attractive targets because their hardware cannot be easily upgraded once launched, and this insecurity worsens over time. As complex systems, they can have long supply chains, and more links in the chain increase the chance of vulnerabilities. Major space projects are also challenged to keep up with best practices over the decade or more needed to build them.

And the stakes are unusually high in space. Orbital trash zips around at speeds of 6 to 9 miles per second and can easily destroy a spacecraft on impact. It can also end space programs worldwide given the hypothesized Kessler syndrome in which the Earth is eventually imprisoned in a cocoon of debris. These consequences weigh in favor of space cyberattacks over physical attacks because the debris problem is also likely to affect the attacker.

Moreover, given critical space infrastructure and services, such as GPS, conflicts in space can spark or add more fuel to a conflict on Earth, even those in cyberspace. For instance, Russia warned in 2022 that hacking one of its satellites would be taken as a declaration of war, which was a dramatic escalation from previous norms around warfare.

Conjuring scenarios

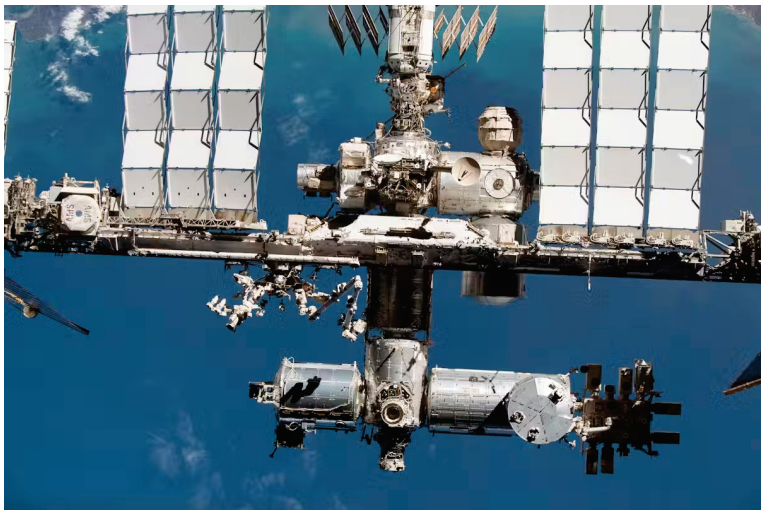
Even security professionals who recognize the severity of this space cybersecurity threat face a major challenge. At least in nonclassified forums, only a couple of under-specified scenarios are typically considered: something vague about satellite hacking and something vague about signals jamming or spoofing.

But failure to imagine a full range of possibilities can be devastating for security planning, especially against hackers who are a diverse set of entities with diverse motivations and targets. These variables are vital to nail down because they reveal clues about which strategies and levers defenders may find most effective in a response. For instance, an attack by a state-sponsored hacker may require a different approach than, say, one by a criminal hacker after money or by a chaos agent.

To help with this piece of the security puzzle, our report offers a taxonomy – the ICARUS matrix – that captures these variables and can create more than 4 million unique combinations of variables, which we call scenario prompts. ICARUS is an acronym for “imagining cyberattacks to anticipate risks unique to space.”

Here are three of the 42 scenarios we included in the report.

A 3D or additive printer can be an invaluable resource for quickly creating parts on demand on space missions. A hacker could gain access to a printer on a space station and reprogram it to make tiny imperfections inside the parts it prints. Some of these built-to-fail components could be parts of critical systems.



A hacked 3D printer could be used to introduce faulty parts to a space station. NASA, CC BY-NC-ND

A hacker could corrupt the data from a planetary probe to show inaccurate atmospheric, temperature or water readings. Corrupted data from a Mars rover, for example, could falsely show that an area has significant subsurface water ice. Any subsequent mission launched to explore the site further would be wasted.

In 1938, a radio drama about an alien attack instigated a panic when many listeners didn't realize it was fictional. Similarly, a hacker could access the listening feeds of the Messaging Extraterrestrial Intelligence, or METI, project and insert something resembling alien language in METI's transcription. They could then leak it to the media, potentially creating panic worldwide and moving financial markets.

Other scenarios in our report involve such things as insider threats, AI vulnerabilities, false flag attacks, ecoterrorism, ransomware during a launch, as well as more distant scenarios about asteroid mining, off-world colonies and space pirates.

Stories for better security

People are hardwired to respond to stories, whether shared around prehistoric campfires or across digital platforms today. Thus, crafting novel and surprising scenarios can help bring to life the invisible threat of space cyberattacks, as well as spotlight nuances across different scenarios that may require interdisciplinary experts to tackle together.