# AEROSPACE

★ ★ ★ AMERICA ★ ★ ★

## TOMORROW'S BLACK BOXES

**Should they be the same, ejectable or virtual? We take you inside the debate.**

PAGE 20

SEPTEMBER 2019 | A publication of the American Institute of Aeronautics and Astronautics | aerospaceamerica.aiaa.org

AIAA SHAPING THE FUTURE OF AEROSPACE

# SMALL SATELLITES, BIG WEAK

**Constellations of microsatellites are starting to provide imagery, communications bandwidth and weather data to customers quickly and affordably. So what could possibly go wrong? Plenty, unless this sector gets its cybersecurity house in order. The good news, reports Debra Werner, is that some are starting to do just that.**

BY DEBRA WERNER | werner.debra@gmail.com

# NESS

Earlier this year, a U.S. Air Force officer visited a microsatellite operator to warn of the danger of criminals or nation-state hackers breaking into the company's network to disable satellites or steal intellectual property such as satellite designs or software.

"It scared the hell out of me," says the CEO, who asked me not to publish the company's name for fear of making it more of a cyber target.

The visit from the Air Force officer was a sign of changing times. For decades, government agencies or multinational corporations controlled the vast majority of satellites, and many of those satellites were as large as school buses. Data was received and commands were sent through private networks backed by sophisticated security apparatuses.

Now, startup companies are hooking up simple microsatellites (weighing 10 to 100 kilograms) to the internet for affordability and the convenience of customers, including the Air Force in some cases. Imagery, weather data and communications bandwidth are delivered this way. Commands to the satellites travel through the internet to satellite ground stations and up to space.

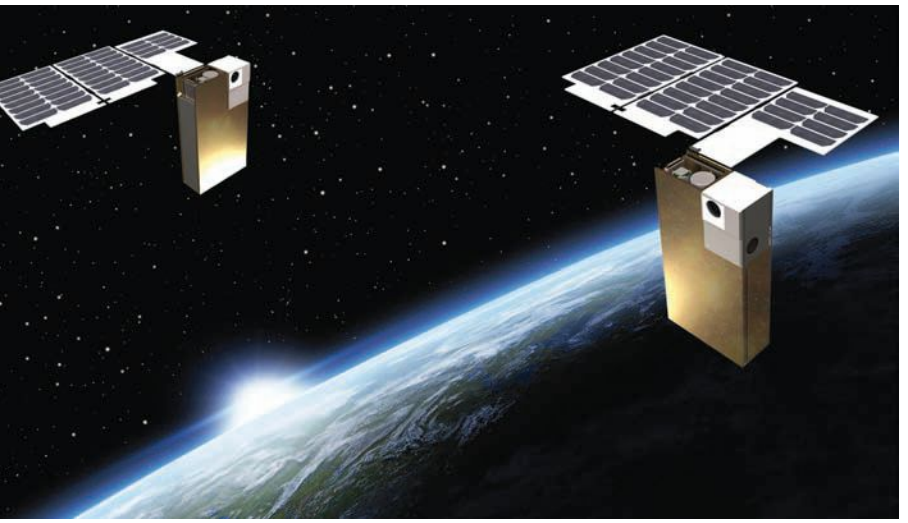
Cybersecurity experts are sounding the alarm about the vulnerability of this new way of doing business.

"Microsatellites are completely driven by software and completely networked. That's where the vulnerability comes in," says Sam Adhikari, operations and research vice president for Sysoft Corp., a big-data analytics company in New Jersey, and chair of AIAA's Aerospace Cybersecurity Working Group.

Cyber experts don't necessarily think companies must disconnect their satellites entirely from the internet. In our example, the CEO quickly hired outside experts to identify and shore up vulnerabilities in the firm's private computer network and its connections with the internet. They warned that an employee on an overseas trip could unwittingly create a conduit to the company's satellite constellation and blueprints by firing up a laptop on public Wi-Fi. So, employees are no longer allowed to bring their work laptops on many such trips. Instead, they travel with blank laptops containing no information about the company or its satellite constellation. When employees return from overseas, the laptops they carried are wiped clean to prevent any malware they may have picked up from spreading to corporate networks.

### Adapting cybertactics to space

On Earth, cybersecurity professionals set up servers called honeypots that are identical to those of the internet or a company's intranet, except that they are laced with spyware. The honeypot strategy takes



▲ **Gunsmoke-L microsatellites** are "information collection" spacecraft in development for the U.S. Army. They are representative of the new class of satellites whose cyber connections could be attractive to hackers.
Dynetics

advantage of the fact that cyberattacks don't typically come out of the blue. Hackers must observe networks closely for months or even years, poking at firewalls and investigating network security before attempting to break in. By tracking the behavior of a hacker at a honeypot, cybersecurity experts can create the equivalent of a fingerprint or signature for the hacker, learn his tactics and develop defenses.

Cybersecurity companies have adapted this concept to microsatellites. Satellite honeypots look like every other satellite in a constellation but instead of relaying communications or gathering imagery, their job is simply to record hacker behavior. How are hackers approaching the network? Are they identifying vulnerabilities? What do they do once they gain access?

With that information, satellite operators can safeguard other satellites in the constellation.

"I can't tell you very much" about this defense mechanism, Adhikari says, "but I can tell you the decoys are out there."

Overall, the name of the game is predictive analytics. Patterns of behavior of would-be hackers are continuously compared to the behavior of those who are authorized to communicate with individual satellites, whose day-to-day operations are logged. Based on subtle differences, the software can predict the presence of a hacker.

## Fighting back

The U.S. once hesitated to publicly attribute hacking, but that is no longer the case. In July, FBI Director Christopher Wray told lawmakers that China is responsible for almost all of the 1,000 cases of intellectual property theft that the FBI is investigating. China's Foreign Ministry spokeswoman Hua Chunying dismissed the allegation of cybertheft as "baseless."

Some of the U.S. allegations center on space technology. "China has a well-understood and effective national strategy to become the global, dominant space power," a key part of which is to "penetrate and dominate elements of the global space industrial base while developing their own strong national space industrial base," according to the report "State of the Space Industrial Base: Threats, Challenges and Actions," released in May by the Air Force Research Lab and the Pentagon's Defense Innovation Unit.

No matter the origin, the intrusions are increasingly sophisticated.

"We're not talking about your average, run-of-the-mill hacker who's trying to steal some credit card information," says Frank Backes, who leads federal space programs at Kratos Defense and Security Solutions in San Diego, whose products include network operations centers and satellite communications networks. "We're talking about a state-sponsor kind of threat, where the state is interested in the design of your satellite, your satellite communications infrastructure and where vulnerabilities might exist."

To strengthen U.S. cybersecurity, the White House National Security Council and the interagency Space Science and Technology Partnership Forum in April announced formation of the Space Information Sharing and Analysis Center, or Space ISAC, in Colorado Springs, Colorado. This nonprofit organization will help companies flying satellites work with government agencies to analyze satellites and ground networks looking for physical and cyber threats, share information and respond if attacked.

Kratos, the Department of Homeland Security's National Cybersecurity Center, the Mitre Corp. and Booz Allen Hamilton, the management and consulting firm headquartered in McLean, Virginia, were first to sign on as members of the Space ISAC. Additional international organizations, companies and national laboratories are in the process of signing up, including satellite builders, space launch companies and satellite operators.

Space ISAC dues-paying members commit to working cooperatively to prepare for and respond to threats, share information on vulnerabilities, incidents and threats with other members, and spread the word about the organization.

The Space ISAC was created, in part, to respond to a presidential Space Policy Directive and to the U.S. National Cyber Strategy. The Trump administration's Space Policy Directive 3 issued in June 2018 says the United States must promote "space safety standards and best practices across the international community." While it doesn't mention cybersecurity specifically, it's implied, says Scott Kordella, Mitre executive director for space systems.

The National Cyber Strategy, released in September 2018, highlights "evolving cyber threats" and says the administration will "work with industry and international partners to strengthen the cyber resilience of existing and future space systems."

## Bold step

To sharpen cybersecurity, the Federal Communications Commission is considering making satellite operators encrypt communications between spacecraft and ground stations. Most satellite operators already encrypt telemetry, tracking and command messages to prevent anyone from hijacking a spacecraft or intercepting communications. But without a federal requirement, some microsatellite operators choose not to encrypt because it's an added expense and can slow communications traffic.

The FCC's proposed rules published in February would require operators of satellites with onboard propulsion to encrypt telemetry, tracking and command information. The comment period closed in April, but no final rules had been issued as of Aug. 1.

Encryption of satellite communications is critical because ground stations are "the soft underbelly" of satellite networks, says Marc Jamison, a retired U.S. Air Force colonel who heads Cyber Checkmate Consultants, a firm based in San Antonio that advises companies on cybersecurity. "If someone is able to implant themselves in your ground stations, they can take control of your satellites."

## How bad can it get?

Space experts say it's unlikely a hacker could hijack a satellite and crash it into another. The hacker would need extensive knowledge of orbital mechanics plus a feedback loop to gauge the progress of such an attack. Still, no one wants to risk a hacker disabling a satellite, stealing Earth imagery or disrupting communications.

"Maintaining positive control over your spacecraft is very important," says Steve Nixon, president of the SmallSat Alliance, a nonprofit industry association that advocates for expanding the roles of small satellites in government programs.

Cybersecurity experts are particularly concerned about cybersecurity at some of the startups with fewer than 100 employees that are building microsatellites. They generally don't employ chief security officers or hire anyone trained in securing networks.

"Big companies building the megaconstellations aren't the only ones we need to help," says Kordella of Mitre. "How will the smaller companies, who will be operating satellites in low Earth orbit along with them, protect themselves and therefore their neighbors as they fly?"

## Protecting the crown jewels

Like all satellite builders, firms developing microsatellites should consider cybersecurity long before their satellites reach orbit, says Adhikari of Sysoft.

Engineering documents for spacecraft and ground networks should be stored in computers with no


▼ **A team at the U.S. Air Force's Arnold Engineering and Development Complex** in Tennessee prepare a microsatellite for a test. U.S. Air Force/Jacqueline Cowan

links to the internet. Engineers should scrutinize the commercial hardware and software they install in satellites and ground stations.

Companies also need to routinely monitor communications traffic so they can detect anomalies.

Even if they take all those precautions, foolproof security is impossible. "Focus on being adaptive, prepared and resilient so you can evolve as threats and vulnerabilities evolve and continue functioning when an issue does arise," says Michael Johnston, who leads Booz Allen's space and nuclear business.

Unlike large government contractors that purchase satellite parts exclusively from carefully vetted suppliers, microsatellite builders often buy computer chips and other parts off the shelf. Those parts could have built-in backdoors offering hackers a way to bypass traditional mechanisms for authenticating satellite commands. You don't know unless you do a vulnerability analysis, Jamison says.

Small-satellite developers also tend to pick up software from GitHub or other commercial vendors. "If you are talking about putting something on orbit in a year, you can't necessarily do a bunch of scrubbing on what that software is and what it does," says Ryan Speelman, principal director of the cybersecurity subdivision at the federally funded Aerospace Corp. in Los Angeles, which conducts research and development for the Air Force and National Reconnaissance Office, the agency that buys and operates U.S. spy satellites.

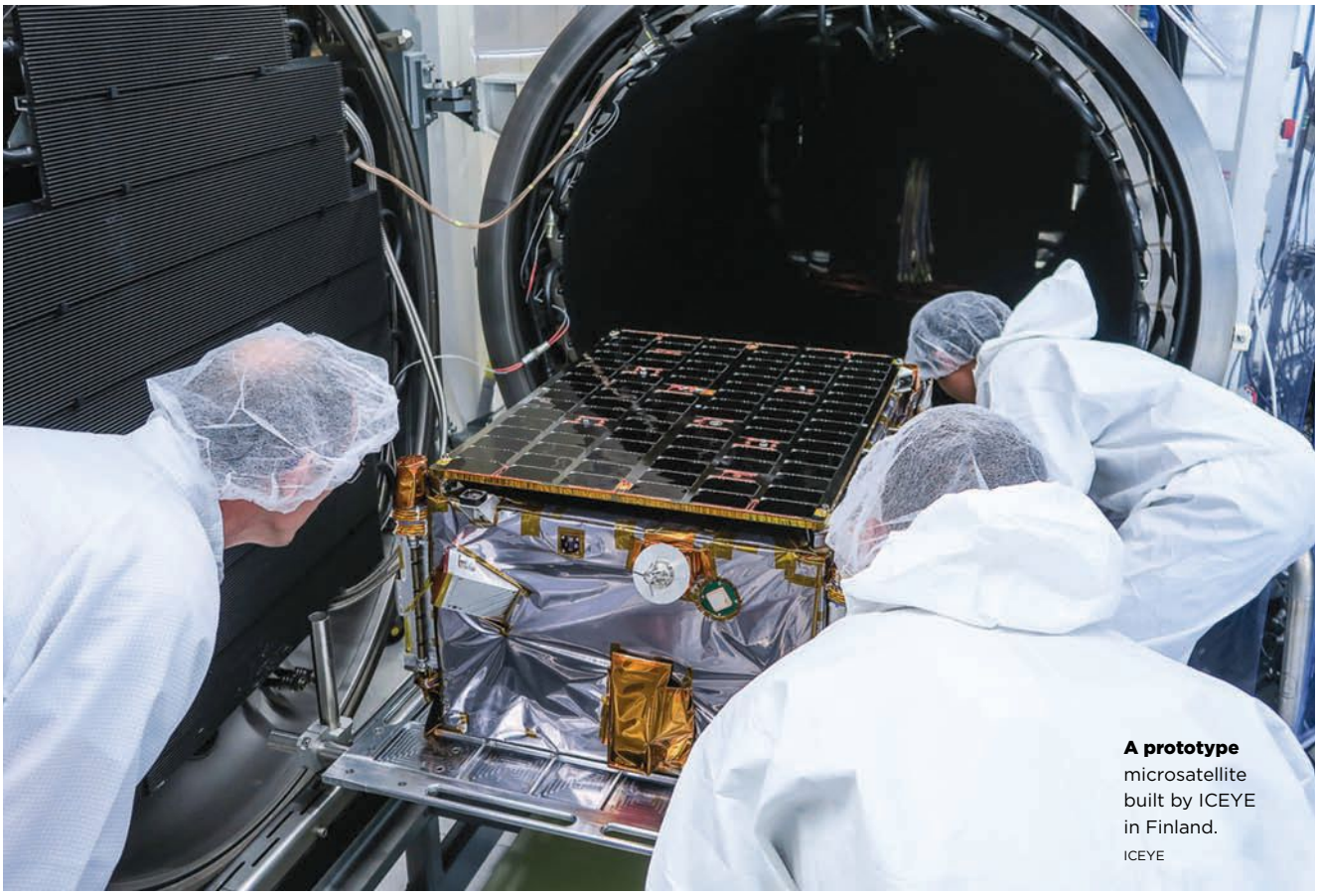
To remedy the problem, the Aerospace Corp. wants to make it easier for satellite operators to detect intrusions. Microsatellite builders could add the intrusion-detection software to their flight software. Larger spacecraft could carry an intrusion-detection computer that would be equipped with artificial intelligence to assess threats.

Both versions would notify satellite operators when anyone outside their trusted network penetrates a satellite's defenses. Aerospace Corp. also wants the software or hardware to reveal the source of cyberattacks. With that information, satellite operators could quickly fend them off, Speelman says.

He thinks quick attribution of cyberattacks could help discourage them. Hackers generally believe they won't get caught. "If you can rapidly attribute the attack, you make it a much less attractive mechanism for an adversary," he says.

The first prototype of the Aerospace Corp. intrusion detection system could fly in 2020. Until then, microsatellite operators like their counterparts flying billion-dollar spacecraft will turn to cybersecurity experts in government and industry for advice on the best way to fend off attacks. ★

*Staff reporter Cat Hofacker contributed to this feature.*



**A prototype** microsatellite built by ICEYE in Finland.
ICEYE