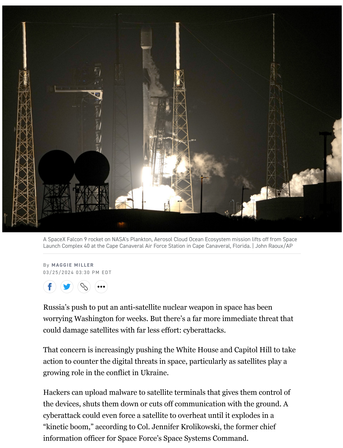
CYBERSECURITY

Officials plan for new age of cyber threats to satellites

The Biden administration and Congress are stepping up efforts to counter cyberattacks on satellites and other space infrastructure.



A SpaceX Falcon 9 rocket on NASA's Plankton, Aerosol Cloud Ocean Ecosystem mission lifts off from Space Launch Complex 40 at the Cape Canaveral Air Force Station in Cape Canaveral, Florida. | John Raoux/AP

By MAGGIE MILLER
03/25/2024 03:30 PM EDT

Russia's push to put an anti-satellite nuclear weapon in space has been worrying Washington for weeks. But there's a far more immediate threat that could damage satellites with far less effort: cyberattacks.

That concern is increasingly pushing the White House and Capitol Hill to take action to counter the digital threats in space, particularly as satellites play a growing role in the conflict in Ukraine.

Hackers can upload malware to satellite terminals that gives them control of the devices, shuts them down or cuts off communication with the ground. A cyberattack could even force a satellite to overheat until it explodes in a "kinetic boom," according to Col. Jennifer Krolikowski, the former chief information officer for Space Force's Space Systems Command.

Any widespread attack against satellites could take down everything from GPS navigation to text message services to weather forecasting — and hackers could achieve that without a huge budget or years of expertise.

That's a far more pressing threat than that of a nuclear weapon in space — a concern that lawmakers have been focused on since reports emerged last month that Moscow is making preparations to put an anti-satellite nuclear weapon in space.

"The barrier to entry and to create an effect is definitely a lot easier in the cyber world," Krolikowski said. "The fact is, they could do something a lot cheaper and create a much larger effect."

And there are no global treaties banning cyberattacks on satellites and other space systems, as there are for deploying nuclear weapons in space. That means global consequences for a cyberattack would be far less certain.

Russia is among the nations already weighing this possibility. The U.S. intelligence community said in its 2023 report on global threats that Moscow's efforts in space included pursuing " jamming and cyberspace capabilities."

Sen. Mike Rounds (R-S.D.), ranking member of the Senate Armed Services Committee's cyber subcommittee, argued that for those watching threats to the nation's cybersecurity, "space is at the top of the list" of areas of concern.

These disruptions would be on a level not yet seen by Americans in their day-to-day lives. Frank Cilluffo, director of Auburn University's McCrary Institute for Cyber and Critical Infrastructure, said this could include "everything from navigation, to communication, to commerce, to clocks."

"It may not sound sexy or important, but if you can manipulate clocks, nanoseconds can have huge implications from a national security perspective, as well as from an economic perspective," Cilluffo said. He cited the potential disruption of stock trading and negatively impacting the ability of Americans to use their personal mobile devices.

A major concern is that satellites and other space systems are operated from a range of networks, all vulnerable to attacks. Darron Makrokanis, chief revenue officer for Xage Security, which counts U.S. Space Force among its clients, warned that a breach anywhere in the supply chain of products that support satellites could be catastrophic.

"Everything from ground communication systems to timing systems to ignition systems, aviation systems, GPS systems, there's so many different pieces of the puzzle that have to come together, interoperate," Makrokanis said.

An expert at Google Cloud's Mandiant, granted anonymity to discuss sensitive research, stressed that even small changes from attacks could be enough to disrupt operations, such as changing the orientation of a satellite in orbit, or triggering a diagnostic test at the wrong time.

Moscow has already proven its satellite disruption capabilities. In the early hours of the full-scale invasion of Ukraine in February 2022, Russian hackers attacked satellite provider Viasat, causing major disruptions to Ukrainian military communications. The attack had a much wider impact outside the battlefield, temporarily knocking out everything from internet access for individuals to disrupting wind terminals across Europe for weeks after.

Since then, Ukrainian forces have become increasingly reliant on SpaceX's Starlink satellite connections on the battlefield, as have civilians in reoaptured cities for internet access, further highlighting the importance of space.

"We are so dependent on our space assets and then you see things like Starlink, how incredibly important it's been to Ukrainians on the battlefield," Senate Intelligence Chair Mark Warner (D-Va.) said, warning that a nuclear weapon or cyberattack in space "would wipe out" systems for every country involved in space.

There are global efforts afoot to establish guardrails. The United Nations Institute for Disarmament Research is leading a program to study what more can be done to increase security in space.

And the federal government has taken steps in recent years to shore up space security. In 2019, Former President Donald Trump signed into law legislation standing up the Pentagon's Space Force, an entirely new armed service. One of Space Force's key focuses is cybersecurity, which has included training "cyber guardians" corps to better respond to cyber threats against infrastructure in space, and is reportedly looking to expand its cyber workforce.

Civilian agencies are also involved. Cybersecurity and Infrastructure Security Agency Director Jen Easterly said during a recent event at the German Marshall Fund that cyber threats to satellites are "up there" on her list of concerns.

CISA plans this year to examine whether more specific performance goals are needed for the security of space systems, an agency spokesperson said. It also plans to strengthen its ability to support U.S. critical infrastructure organizations that rely on space-based capabilities if such a cyberattack were to occur.

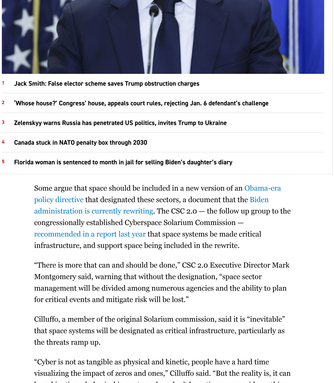
"Space infrastructure plays a vital role in the reliable and efficient operations of much of our nation's critical infrastructure," CISA Executive Director Brandon Wales said in a statement.

On Capitol Hill, Senate Homeland Security Chair Gary Peters (D-Mich.) and Sen. John Cornyn (R-Texas) last year introduced legislation to increase the cybersecurity of satellites. The legislation would require CISA to develop online cybersecurity resources for companies that rely on satellites, and require the White House to roll out a federal strategy to counter cyber threats to satellite systems.

The legislation was approved by the committee in May, but has not yet received a vote, though an aide to Peters said the senator is "exploring all potential paths forward for the bill."

Some experts say much more work remains. While satellites are included in the communications sector, space in general is not designated as one of the 16 federal critical infrastructure sectors, a group that currently includes dams, food and agriculture organizations, government agencies and emergency services.

MOST READ



1 Jack Smith: False elector scheme saves Trump obstruction charges
2 'Whose house?' Congress' house, appeals court rules, rejecting Jan. 6 defendant's challenge
3 Zelenskyy warns Russia has penetrated US politics, invites Trump to Ukraine
4 Canada stuck in NATO penalty box through 2030
5 Florida woman is sentenced to month in jail for selling Biden's daughter's diary

Some argue that space should be included in a new version of an Obama-era policy directive that designated these sectors, a document that the Biden administration is currently rewriting. The CSC 2.0 — the follow up group to the congressionally established Cyberspace Solarium Commission — recommended in a report last year that space systems be made critical infrastructure, and support space being included in the rewrite.

"There is more that can and should be done," CSC 2.0 Executive Director Mark Montgomery said, warning that without the designation, "space sector management will be divided among numerous agencies and the ability to plan for critical events and mitigate risk will be lost."

Cilluffo, a member of the original Solarium commission, said it is "inevitable" that space systems will be designated as critical infrastructure, particularly as the threats ramp up.

"Cyber is not as tangible as physical and kinetic, people have a hard time visualizing the impact of zeros and ones," Cilluffo said. "But the reality is, it can have kinetic and physical impact...and we don't have time on our side on this one."

FILED UNDER: CYBER SECURITY, RUSSIA, MIKE ROUNDS, SPACE FORCE, UKRAINE.