US military project to prevent hackers targeting satellites, recognizes rising threat of cyberattacks in space

June 27 2024, by Sharon Lemac-Vincere

Credit: Pixabay/CC0 Public Domain

The US military recently launched a groundbreaking initiative to strengthen ties with the commercial space industry. The aim is to integrate commercial equipment into military space operations, including satellites and other hardware. This would enhance cybersecurity for military satellites.

As space becomes more important to the world's critical infrastructure, the risk increases that hostile nation states will deploy cyber attacks on important satellites and other space infrastructure. Targets would include spy satellites or military communications satellites, but commercial spacecraft too.

The US Department of Defense believes its new partnership, called Commercial Augmentation Space Reserve (CASR), would enhance US national security and the country's competitive advantage in space. It would go some way beyond the relationship between government and private contractor that already exists.

In some cases, the commercial sector has advanced rapidly beyond government capabilities. This situation exists in numerous countries with a space capability and may apply in certain areas in the US too.

The governments of some nation states are therefore confronted with a choice. They could utilize bespoke systems for protecting their satellites, even though these may be outdated, or they could use other commercial—and potentially more advanced—"off-the-shelf" components. However, the commercial hardware may be less well understood in terms of its vulnerabilities to cyber attacks.

Nevertheless, the US military believes that CASR will give it advanced strategic capabilities, and that potential risks can be minimized by actively avoiding over reliance on any single commercial entity.

The supply chain aims to transition the US military from a restricted pool of commercial suppliers to a broader spectrum of partners. However, there are risks with a bigger pool of commercial suppliers too. Some might be unable to meet the demands of military contracts, could run into financial instability or encounter other pressures that hinder their ability to supply critical components.

New priorities

In 2022, there was a cyber attack on the KA-Sat consumer satellite broadband service. It targeted the satellites delivering the broadband and disrupted the service.

There are many ways to attack another state's satellites, such as anti-satellite (ASAT) weapons, which are often designed to physically destroy or disable the spacecraft. However, compared to ASATs, cyber attacks can be carried out in ways that are cheaper, quicker and more difficult to trace.

Part of the critical need to prioritize cybersecurity as a result of this strategy is that the US is an attractive market for global players in space. This strategic shift by the US Department of Defense is therefore likely to encourage more global companies to participate.

Resilience to cyber attacks in the space industry has not always been a top priority. It is likely to take time for this to enter the thinking of major players in the space sector.

This historical lack of emphasis on cybersecurity in space highlights an obvious need. There are also inconsistencies and gaps regarding the basic cyber requirements for government and industry, which vary depending on the stance of each nation state.

The US military claims that interoperability in military standards—the ability of different hardware to work seamlessly together—will strengthen the new public-private relationship. It has also left the door open for commercial standards to be adopted in certain instances. But there's a risk that shifting from military standards (which are typically more stringent than commercial standards) could undermine military assets and lead to the same adverse consequences the strategy seeks to avoid.

Despite the best intentions, the complexities of working with many more and newer commercial partners could also lead to inconsistencies in the application of standards across different projects and systems. Commercial cybersecurity standards are unlikely to prioritize the same level of security required for military applications, especially under extreme conditions.

In light of these challenges, the success of these initiatives hinges on having leaders who are proactive and well informed. Being able to act across the commercial and defense sectors will require key skills—one of which is being informed and educated on cybersecurity.

Recently, I developed an executive space cybersecurity course with postgraduate credentials in partnership with the International Space University. This executive-level course attracted professionals from various sectors, including the legal profession, regulators, consultants, commercial businesses and investors.

By bridging the gap between different sectors and disciplines, the course fostered an all-round, multidisciplinary approach to space cybersecurity. Executives were able to gain a deeper understanding of the interconnectedness of various systems and the potential vulnerabilities that can arise. This not only enriched the learnisng experience but also encouraged participants to think outside the box and explore new strategies for mitigating cyber threats in space.

As the Pentagon and the commercial space industry forge ahead with their groundbreaking collaboration, it is important that those making decisions understand the critical nature of cybersecurity. This shift is not without its challenges. But it also presents opportunities for innovation and new partnerships which could shape the future of space exploration and lead to new approaches to cyber security for satellites and other space infrastructure.

Provided by The Conversation

Citation: US military project to prevent hackers targeting satellites, recognizes rising threat of cyberattacks in space (2024, June 27) retrieved 30 June 2024 from https://techxplore.com/news/2024-06-military-hackers-satellites-threat-cyberattacks.html