The US must secure its supply chain in the face of anti-satellite weapons

www.c4isrnet.com

At the 34th National Space Symposium in April, U.S. Air Force Secretary Heather Wilson announced that the service is taking steps to secure its satellite networks by working with allied forces, commercial satellite owners and international organizations to share satellites currently in orbit.

Testifying before Congress, Director of National Intelligence Dan Coats warned that U.S. adversaries “continue to pursue anti-satellite [ASAT] weapons as a means to reduce U.S. and allied military effectiveness.” While the threat is serious and sharing allied satellites provides a measure of security, the Air Force will not be able to preserve America’s edge in space unless it focuses on securing the satellite supply chain here on Earth.

Already, states like China, Russia, North Korea and Iran have developed or demonstrated the capacity to create ASAT systems. The spectrum of ASAT weapons includes both missiles and cyber means intended to deny access to, disrupt or destroy U.S. satellite systems. Because ASAT weapons can target both military and commercial satellites, ASAT operations can threaten everything from our ability to collect intelligence or conduct military operations to American firm’s ability to engage in global commerce.

The goals of the Air Force’s initiative is to ensure the security of the service’s space assets by deterring adversaries from targeting its satellite network by decreasing the time required to build and launch

Here's an artist's rendition of a Wideband Global Satellite in orbit. Industry officials want to knwo what role commercial satellite providers could play in the program's next iteration (Air Force Space Command) a new satellite. To achieve this goal, the Air Force will add additional satellites to its global network and distribute its satellite network across an array of space assets in both geosynchronous and low-Earth orbit.

NASA classifies satellites in low-Earth orbit as systems that operate at an elevation between 150 and 2000 km with an orbit time ranging between 90 minutes and a few hours, while satellites in geosynchronous orbit operate at an altitude above 35,780 km and can take 24 hours to complete a circular orbit.

While the Air Force initiative seeks to secure satellites in space, the plan is insufficient to protect U.S. military and civilian capabilities because it does nothing to address supply chain vulnerabilities, which may result in the infiltration of malicious software and hardware prior to launch.

A detailed new report from the Secure World Foundation puts this threat in its proper context. According to “Global Counterspace Capabilities: An Open Source Assessment,” the three primary access points for targeting a satellite are the supply chain, the land-based infrastructure that interacts with the satellite, and the actual satellite while it is in orbit. Of the three access points, the supply chain and land-based infrastructure are ideal targets of opportunity for attackers because they are the most accessible.

While the land-based infrastructure and government employees that interact with U.S. satellites operate under strict physical and information security protocols in restricted access facilities, companies that provide satellite components rarely follow such rigorous security measures to maintain the integrity of the products they are supplying to the U.S. government. Thus, contractors and sub-contractors may be highly susceptible to infiltration, thereby allowing malicious actors to install remote access points that can bypass any security features later installed on the system and leaving even the most hardened defenses completely ineffective.

Supply chain threats are neither new nor unique to the space industry; however, the utility that satellites provide to the U.S. make the systems an ideal target for state and non-state actors who wish to hinder the ability for the U.S. to conduct operations around the globe.

The threat of ASAT systems is particularly significant for the U.S., which is heavily reliant on satellite networks for the command and control of both government and commercial assets. Depending on which satellite is targeted, possible effects of an ASAT attack could be anything from an increased time required to mobilize forces to respond to a conflict to an inability to use GPS systems on the battlefield, or to a hindered ability to conduct missile strike operations.

In the current threat environment, it is imperative that the U.S. harden its satellite networks at both the hardware and software levels. Securing those satellite systems begins with the supply chains that provide the essential components for satellite construction and end with regular security updates for the entire satellite. Supply chain infiltration remains an ongoing threat to national security and more needs to be done to protect these supply chains from cyber infiltration, espionage and exploitation.

Once the Air Force recognizes that the supply chain is vulnerable, the question becomes how to secure it. One critical step is to ensure that contractors begin planning to mitigate the threat, perhaps by developing a formal supply chain risk management plan. An effective response should also consider technology, such as blockchain, that can help to verify transactions. In all likelihood, the best approaches will emerge from a period of trial-and-error. The important thing is to start now.

Trevor Logan is a cyber research associate at the Foundation for the Defense of Democracies project on Cyber-Enabled Economic Warfare. Follow him on Twitter @TrevorLoganFDD.

■