IAF SYMPOSIUM ON SECURITY, STABILITY AND SUSTAINABILITY OF SPACE ACTIVITIES (E9)
Cyber-based security threats to space missions: establishing the legal, institutional and collaborative framework to counteract them (2)

Author: Dr. Timiebi Aganaba-Jeanty
Arizona State University, United States

Mr. Samuel Rugi
United States

IS DECLARING "SPACE" AS CRITICAL INFRASTRUCTURE THE BEST DEFENSE AGAINST CYBER THREAT?

Abstract

All elements of the space system are vulnerable to attacks, ranging from complex counter space capabilities that could be used to disrupt, deny, degrade, or destroy space systems, to basic cyberattacks that attack supply chains, which the space sector is vulnerable to because of how long the supply chain is. This means that all satellites are vulnerable to cyber intrusion if even one part of their shared supply chain is corrupted.

While the effects of directly targeting a space asset could be catastrophic, not only to the space environment, but also as a result of geopolitical rivalry and tensions in other domains, the consequences of a cyberattack on space infrastructure can be anything from temporary disruption to complete mission failure. The threat is further escalated by the ease at which such threats can be materialized from low costs to entry and a wide pool of capable adversaries, from simple hackers to sophisticated state actors.

Increased efforts have been made to articulate what a day without satellites would look like. There would be significant implications from the loss of satellite-based timestamps, which play a critical part in everything from credit card readers and stock exchanges to the systems that keep track of transactions, right up to the need to declare a state of emergency and call on the military to restore order. This has led for a call in the United States, for space assets to be viewed as "critical infrastructure"- assets essential for the functioning of a society and economy. This designation applies to the Space Sector in the United Kingdom. One reason this could be favourable is because the 2018 Department of Defense Cyber Strategy outlines a "defend forward" policy for addressing cyber threats to US critical infrastructure, possibly including pre-emptive action.

However, some commentators argue, that the challenge to designating GPS, for instance, as critical infrastructure has been that the way "the the Department of Homeland Security tries to protect infrastructure is by gathering commercial entities from each sector in various forums to discuss issues, develop best practices, gain understanding, consider possible government actions," and that this model that could not be applied easily to a government owned satellite system like GPS. Also, if space systems are declared critical infrastructure, commercialization is complicated, particularly due to time delays caused by government funding approvals.

This paper assess the pros and cons of this approach.