Research: Cybersecurity in Space

Outer space is no longer just the final frontier for exploration; it's a critical domain for national security, communication, navigation, weather forecasting, and several aspects more of our lives here on Earth. More and more computer platforms are being sent into orbit and beyond. Inevitably, these systems must prioritize functionality above all else; as a result, efforts to protect the space system from failure overly the fact that malicious incidents are happening right now. The time when users could trust the operators and any commands they gave the machine it's entirely different from what the deal is today. Just ask yourself. Why would any entity or person take any action that could jeopardize the multimillion-dollar satellite program from a country? What could possibly motivate someone to do that?

As worldwide reliance on space-dependent services grows, so does the need for robust cyber defense to protect these. This is the digital age, and nearly anything with software can be hacked and/or be vulnerable to malicious and non-malicious threats. American intelligence agencies have warned of cyberattacks against the country's satellite infrastructure and foreign espionage targeted at the country's space sector. Cyberattacks, fake companies, or traditional espionage techniques might be employed by foreign intelligence agencies to get confidential data on US space capabilities or advanced technology. American satellite systems may be interfered with or compromised by using counterspace technologies like hacking or satellite jamming. Safeguarding our satellites and space assets from being targets for cyberattacks and hostile operations is essential for national security and continued technological progress. **Because our reliance on space technology is growing, the U.S. Government should allocate resources to**

cybersecurity in space assets such as satellites, space stations, and communication networks.

Since the 1950s, spacefaring governments have prioritized outer space as part of their national security agenda. In today's world, space-dependent services including the Global Positioning System (GPS), product transportation, manufacturing, communication, energy and water management, and space systems are invaluable to governments, critical infrastructure, and economies. In 2023, there were over twenty-two thousand Satellites in orbit being tracked by the U.S. Space Force, which is a number continuing to grow (Greatwood). In addition, to connect with remote assets, global networks rely on satellites. To coordinate military operations and economic operations, these networks heavily rely on both terrestrial and space assets.

The importance of protecting space infrastructure's cybersecurity is made more urgent by our growing reliance on it, yet doing so represents several obstacles. Nations and individuals are learning to disrupt, hack, or even destroy satellites and the data they transmit. Numerous cybersecurity disasters have been documented in academic publications. NASA was one of nine entities that fell victim to the enormous cyberattack known as the SolarWinds break in 2021. The agency leadership referred to this massive intrusion as a "wakeup call" in terms of safeguarding the networks that NASA relies on to store and distribute critical technical data.

A deep connection exists between space systems and the critically important infrastructure industries, such as the energy industry, as evidenced by another recent attack on a major international satellite internet provider. The attack appeared to have as an unexpected side effect the disruption of remote access to thousands of wind turbines (Greig). This took place during the active stage of the invasion of Ukraine, with a plausible hypothesis that it was caused by malware attributed to Russian actors. Since so many essential operations pass via space, any cyberattack or breach [on national assets] would severely affect a wide range of critical operations, as stated by Greatwood.

Satellites and other space assets each day become more reliant on digital systems, making them potential targets for cyberattacks. Cyberattacks were difficult to carry out in the past since most space infrastructure was built using specialized fixed-function hardware and software. The programmable, standard hardware and software found in many of the new satellites are now vulnerable to the same threats and weaknesses as other systems that use the same components (Fidler). These vulnerabilities that have arisen from the implementation of newer (but needed) software raise concerns about the security and integrity of the data that is carried by the space systems. We understand from *Cybersecurity for Space* that "once a malicious actor gains access to the computer on the ground that communicates with a space system, there is almost implicit trust and no further defense in depth for the space system or systems that communicate with that terrestrial computer" (Oakley 18). Protection of space assets must work in both ways: for earth-based systems and space-based systems.

Our planet is orbited by an extensive amount of trash. Every time a satellite, rock, or other object is launched by humans and placed high enough above the Earth, it is with the intent of leaving it there for several years, decades, or even longer. Of course, the space is incommensurably big; this is not to say, however, that collisions are impossible or that their likelihood would decrease as space becomes more accessible (Oakley 144). These non-malicious threats represent a tangible danger to the space infrastructure where millions of dollars have been invested, and the data that they collect. This kind of vulnerability can be reduced by continuously monitoring the space environment for potential threats. Detect and track Anti-Satellite Weapons

(ASAT) activities to respond promptly (Kirshner). If attacks are perpetrated, reliable backups must be kept up to date every time possible.

Space agencies can just wish their assets had coverage. The significance of cybersecurity for space assets cannot be overstated, especially considering the substantial investments required to deploy these assets into space. As space becomes increasingly integrated with other sectors, both public and private, the necessity to safeguard these assets from cyber threats grows exponentially (*European Space Agency*). Cybersecurity measures are essential to protect data integrity, ensure the continuity of space operations, and prevent the disruption or destruction of these valuable assets (Kavallieratos and Sokratis). Therefore, investing in cybersecurity for space assets is not only prudent but imperative to maintain the advantages and protections that these assets provide. The cost of cybersecurity fades in comparison to the potential losses from compromised space assets, making it a wise and necessary allocation of resources.

There is a huge financial challenge in allocating substantial resources to improve cybersecurity for space assets, especially those created prior to cybersecurity being a serious concern. Kaczmarek states that adapting older equipment can come at a high cost and that there is no assurance that the modifications would be profitable ("Cybersecurity for Satellites"). Additionally, because technology is developing so quickly, these expenditures could become outdated very quickly after they are made, creating a vicious cycle of ongoing expenses that provide declining returns ("Cybersecurity in Space"). Prioritizing cybersecurity for older space systems may also take money away from other important projects, such as the creation of new, inherently secure space technology or essential public services (Greatwood). Given the limited government budgets and the need for fiscal prudence, the allocation of resources must be carefully considered, balancing the immediate cybersecurity needs against the long-term strategy of space asset development and utilization.

The implementation of cybersecurity in space is a matter of international collaboration. Agencies like the National Aeronautics and Space Administration (NASA) and Departments of the U.S. government like the Department of Commerce, as well as international organizations like NATO, and the private sector must all work in concert to allocate resources effectively. This collaboration should involve sharing intelligence on potential cyber threats, developing standardized security protocols, and investing in cutting-edge encryption technologies to protect satellites and other space assets from cyberattacks. Furthermore, joint cyber defense exercises could be conducted to prepare for and mitigate the effects of potential cyber incidents. By pooling resources and expertise, these entities can create a fortified defense that not only protects already millionaire assets but also ensures the safety and reliability of the critical services they provide to the world.

In conclusion, the imperative to fortify cybersecurity in space is not merely a precautionary measure but a necessary investment in our collective security and prosperity. The digital age has brought in unparalleled advancements and conveniences, yet it has also exposed new vulnerabilities, particularly in the critical infrastructures that orbit our planet. The escalation of cyber threats in tandem with our growing dependence on space-based technologies accentuates the urgency for dedicated resources to shield these assets. The allocation of resources toward the implementation of cybersecurity measures in space is a strategic imperative that aligns with the principles of national security, economic stability, and technological innovation. It is a commitment to safeguarding the integrity of our space assets, ensuring the continuity of services that are now integral to our way of life, and preserving the peaceful use of outer space the more we can. As humanity navigates the complexities of the 21st century, the precaution to protect our space infrastructure from cyber threats will serve as a pillar for a secure, interconnected, and resilient global community. Thus, it becomes binding to the U.S. Government, in collaboration with international partners and private entities, to prioritize and allocate the necessary resources for the development and implementation of robust cybersecurity strategies in space, thereby fortifying the frontier that has become vital to modern existence.

Works Cited

"ESA Practices Cybersecurity." *European Space Agency*, 2019, www.esa.int/Space_Safety/ESA_practices_cybersecurity. Accessed 31 Mar. 2024.

Fidler, David P. "Cybersecurity and the new era of space activities." *Digital and Cyberspace Policy Program*, Apr. 2019.

Greatwood, Duncan. "Securing The Final Frontier: Why Cybersecurity In Space Matters Now." *Forbes*, 27 Sept. 2023, https://www.forbes.com/sites/forbestechcouncil/2023/09/27/securing-the-final-frontier-why-cybersecurity-in-space-matters-now/?sh=173000ca3e36. Accessed 22 Mar. 2024.

Greig, Jonathan. "Viasat Confirms Report of Wiper Malware Used in Ukraine Cyberattack." *The Record from Recorded Future News,* 1 Apr. 2022, therecord.media/viasat-confirms-report-of-wiper-malware-used-in-ukraine-cyberattack. Accessed 29 Mar. 2024.

Kaczmarek, Sylvester. "Cybersecurity for Satellites Is a Growing Challenge." *The Space Review: SpaceNews*, 26 Feb. 2024, www.thespacereview.com/article/4747/1.

Kaczmarek, Sylvester. "We Need Cybersecurity in Space to Protect Satellites." *Scientific American*, 20 Feb. 2024, www.scientificamerican.com/article/we-need-cybersecurity-in-space-to-protect-satellites/.

Kavallieratos, Georgios, and Sokratis Katsikas. "An Exploratory Analysis of the Last Frontier: A Systematic Literature Review of Cybersecurity in Space." *International Journal of Critical Infrastructure Protection*, vol. 43, 2023, p. 100640, https://doi.org/10.1016/j.ijcip.2023.100640.

Kirshner, Mitchell. “Model-Based Systems Engineering Cybersecurity for Space Systems.” *MDPI*, 25 Jan. 2023, www.mdpi.com/2226-4310/10/2/116. Accessed 29 Mar. 2024.

Oakley, Jacob G. “Cybersecurity for Space: Protecting the Final Frontier”. 1st ed., *Apress L. P*, 2020, https://doi.org/10.1007/978-1-4842-5732-6. Accessed 29 Mar. 2024.