Defense Systems
Information Analysis Center

DSIAC TECHNICAL INQUIRY (TI) RESPONSE REPORT

Technologies and Strategies to Protect Satellites From Electronic and Cyberwarfare

Report Number:
DSIAC-2019-1198
Completed November 2019

DSIAC is a Department of Defense
Information Analysis Center

MAIN OFFICE
4695 Millennium Drive
Belcamp, MD 21017-1505
443-360-4600

REPORT PREPARED BY:
Travis Kneen
Office: DSIAC

ABOUT DSIAC

The Defense Systems Information Analysis Center (DSIAC) is a U.S. Department of Defense Information Analysis Center sponsored by the Defense Technical Information Center. DSIAC is operated by SURVICE Engineering Company under contract FA8075-14-D-0001.

DSIAC serves as the national clearinghouse for worldwide scientific and technical information for weapon systems; survivability and vulnerability; reliability, maintainability, quality, supportability, and interoperability; advanced materials; military sensing; autonomous systems; energetics; directed energy; and non-lethal weapons. We collect, analyze, synthesize, and disseminate related technical information and data for each of these focus areas.

A chief service of DSIAC is free technical inquiry (TI) research, limited to 4 research hours per inquiry. This TI response report summarizes the research findings of one such inquiry. For more information about DSIAC and our TI service, please visit www.DSIAC.org.

ABSTRACT

DSIAC was tasked with determining what is being done to mitigate the impact of electronic and cyberwarfare technologies on satellites, specifically communication and navigation systems. DSIAC reached out to subject matter experts for input and contact information for further discussions with the inquirer. Open-source research was performed, and relevant information is summarized. Due to the sensitive nature of these technologies, further research would likely move into the classified domain. The results are compiled in this report and an additional response by the Cyber Security & Information Systems Information Analysis Center that was delivered separately.

Contents

1.0 TI Request

1.1 INQUIRY

What technologies and strategies are being assessed to mitigate electronic and cyberwarfare (CW) threats to GPS and communication satellites in space?

1.2 DESCRIPTION

The inquirer is interested in what can be done to protect space global positioning system (GPS) and satellite communication (SATCOM) satellites, specifically Navstar and Space-Based Infrared System from near-pierce CW and electronic warfare (EW) threats.

2.0 TI Response

DSIAC performed searches for information on technologies and strategies to mitigate electronic and CW threats to GPS and communication satellites in space using open sources and the DTIC Research and Engineering Gateway database. Additionally, subject matter experts (SMEs) from the Old Crows, Resilient Navigation & Timing Foundation, and the Cyber Security & Information Systems Information Analysis Center (CSIAC) were consulted for additional information and input. The CSIAC report was delivered separately. This report contains the relevant information that was delivered to the inquirer.

2.1 CYBERSECURITY WARFARE MITIGATION

The federally-funded research and development centers say in a new report that space and cybersecurity policy is prepared for the challenges created by meshing space and cyberspace, especially for the spacecraft. The Aerospace Corporation says that not enough is being done in government policy or manufacturers to protect and monitor satellites from cyberattacks. Targeting satellites and the resulting sensor, communication, and position, navigation, and timing (PNT) data is not just an issue for military satellites but also commercial craft that provide similar services [1].

Cyberattacks against space capabilities are similar to cyberattacks against nonspace systems as they often involve attempts to feed user-provided information to a system that causes software to perform in unexpected ways. Any cyberattack requires four things—access, vulnerability, a malicious payload, and a command-and-control system. Three primary points of access exist for exploitation, attack, and service denial of space assets in the cyberdomain—the supply

chain, extended land-based infrastructure that sustains the assets (ground stations, terminals, companies, and end-users), and satellites [2].

Aerospace Corp. has a few recommendations to better protect satellites and other similar assets:

- Intrusion detection and prevention by leveraging signatures and machine-learning to detect and block cyberintrusions as craft payloads.
- A supply chain risk management program to protect against malware inserted into parts and modules.
- Software assurance methods within the software supply chain to reduce the likelihood of cyberweaknesses in flight software and firmware.
- Logging onboard the craft to verify legitimate operations and aid in forensic investigations after anomalies.
- Root of Trust functions to protect software and firmware integrity.
- A tamper-proof means to restore the spacecraft to a known cybersafe state.
- Lightweight cryptographic solutions for use in small satellites.

Satellites/spacecrafts are not the only devices in space vulnerable to CW attacks. In fact, it is traditionally the ground stations that communicate with the satellites that are the focus of cyberattacks in order to corrupt data or disable/destroy the craft. However, other possible targets of attacks throughout the supply chain, such as third-party codes and commercial-grade components, are being used in place of military-grade parts to reduce lead times and costs [1].

In the 2018 paper "Job One for Space Force: Space Asset Cybersecurity," published by the Harvard Kennedy School's Belfer Center for Science and International Affairs [3], Gregory Falco reviews some of the major cybersecurity threats to space systems, evaluates steps taken by companies and government agencies to secure such systems, and proposes policy recommendations to streamline cybersecurity for space systems in both the private and public sector. He mentions that NASA tackled some security issues by implementing stricter access control policies to guard against phishing attacks to steal credentials, creating teams to focus on the security of specific missions (instead of one overarching cybersecurity team), and encrypting data during storage or transfer. Falco suggests that space asset organizations consider the following options to better fight potential cybersecurity threats:

- Employ existing cybersecurity standards and develop new standards for space systems where needed.
- Establish cybersecurity capabilities for mission systems and internal network/server systems.
- Build a security culture.
- Utilize appropriate security tools that are available, such as data and communications encryption.

- Cooperate with security researchers.

However, he mentions that national policy needs to provide additional guidance on space system security. He suggests clarifying critical security requirements to include underlying systems, assigning responsibility and liability for cybersecurity, making space asset organizations accountable for cybersecurity, and expanding 32 CFR 237 to require all space asset organizations report cyber incidents that either affected or could affect national security. With the creation of a Space Information Sharing and Analysis Center (Space ISAC) in 2019, Falco suggests that it encourages collaboration among space-relevant organizations, establishes information sharing requirements, documents and maintains space system cybersecurity best practices and standards, and cooperates with ISACs for other critical infrastructure sectors that rely on space systems.

The Space ISAC was created to support the White House National Cyber Strategy, which calls for the government to work with industry to strengthen the cyber-resilience of existing and future space systems. Kratos Defense & Security Solutions is the first founding member and one of over 200 companies (including satellite and launch vehicle manufacturers and their supply chains) to join the group. Members of the group would provide the ISAC with data to analyze, and then the information would be shared through a secure portal so companies can determine the best methods of defeating the threats as new satellite/spacecraft are developed and built [4, 5].

The National Security Agency/Central Security Service (NSA/CSS) established a Cybersecurity Directorate to unify the NSA's foreign intelligence and cyber-defense missions. This directorate is charged with preventing and eradicating threats to national security systems and the defense industrial base. This new approach to cybersecurity better positions the NSA to collaborate with other U.S. government organizations like the U.S. Cyber Command, Department of Homeland Security, and Federal Bureau of Investigation, as well as share information with their customers so they are better equipped to defend against malicious cyberactivity [6].

One way the Defense Advanced Research Projects Agency (DARPA) is seeking to protect space assets is to develop a satellite program that relies on cheaper satellites residing in low-Earth orbit (LEO) rather than the large, expensive, and monolithic systems residing in the geosynchronous orbit that have become vulnerable to attacks and would take years to replace if degraded or destroyed. DARPA's Blackjack program seeks to develop enabling technologies for a global high-speed network backbone in LEO that enables networked, resilient, and persistent military payloads that provide infinite over-the-horizon sensing, signals, and communications capabilities. The program focuses on cheap, potentially commercial off-the-shelf components and low-cost, interchangeable payloads with short design cycles and frequent technology upgrades in order to stay ahead of malicious attack capabilities. In particular, the Blackjack program has three primary objectives [7, 8]:

1. Develop payload and mission-level autonomy software and demonstrate autonomous orbital operations, including on-orbit distributed decision processors.
2. Develop and implement advanced commercial manufacturing for military payloads and the spacecraft bus.
3. Demonstrate payloads in LEO to augment NSS assets. The driver will be to show LEO performance that is on par with current systems in geosynchronous orbit with the spacecraft combined bus, payload(s), and launch costs under $6 million per orbital node while the payloads meet size, weight, and power constraints of the commercial bus.

To develop the science, technology, and architecture needed for autonomous satellite protection systems Sandia National Laboratories launched a 7-year mission called the Science and Technology Advancing Resilience for Contested Space. This mission focuses on three critical areas—threat-defended hardware to protect satellite processors, circuits, and systems from attacks; cognitive analytics or software algorithms that can rapidly and independently detect, adapt to, and defeat threats; and sensor protection that shields sensors from harm [9].

Even beyond the individual organization's and nation's security, this is an issue being addressed by the North Atlantic Treaty Organization (NATO). In the 2019 research paper "Cybersecurity of NATO's Space-Based Strategic Assets" [10], the various potential vulnerabilities of space-dependent strategic systems are addressed. While NATO and the NATO Communications and Information Agency are currently working on protecting NATO's space-dependent systems, this paper delves into potential policies and roles that NATO could be involved in to help shape the future of the space domain and how it is protected/attacked.

2.2 ELECTRONIC WARFARE (EW) MITIGATION

Finding information involving EW is difficult because EW capabilities are very sensitive and conducted exclusively in the classified domain. EW is defined as military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or attack the enemy. There are EW weapons specifically designed to interfere with an adversary's radio frequency transmissions to or from a satellite, otherwise known as jamming. Three principal areas of concern for counterspace jamming include global navigation satellite systems signals, SATCOM, and synthetic aperture radar imaging. The "Global Counterspace Capabilities: An Open Source Assessment" report published by the Secure World Foundation [2] compiles known open-source EW capabilities of the People's Republic of China, Russian Federation, and the United States.

The U.S. military launched the Navigation Warfare (NAVWAR) to develop a strategy for how the military could conduct defensive and offensive operations to protect the country's use of PNT capabilities while also interdicting or preventing adversary use of these capabilities. The NAVWAR defensive measures seek to prevent adversarial EW countermeasures from

interfering with operational use of GPS in two ways—developing a new military signal (M-code) and developing new receivers that can utilize M-code and incorporate improved antijam and anti-spoofing technology. While not a defensive measure, the Counter Communications System (CCS) program was initiated as a broader counterspace capability development program. The CCS is an EW system maintained by the 21st Space Wing located at Peterson Air Force Base, CO. With continuing funding allocations, the CCS is most likely a high-priority program for the U.S. military and likely offers a very effective SATCOM jamming capability [2].

2.3 SMEs

DSIAC reached out to SME organizations for additional support and information to help answer this question. Since this inquiry touches on cybersecurity concerns and technologies, CSIAC was contacted, and one of their analysts prepared a separate report [11] that was delivered to the inquirer. DSIAC also reached out to the Association of Old Crows, who supplied the contact information for the Resilient Navigation & Timing Foundation President Dana Goward. Dana is an expert in GPS signal and user protection, a member of the President's National PNT Advisory Board, and a senior advisor to the U.S. Space Command's (SPACECOM's) Purposeful Interference Response Team [12].

Beyond the people that DSIAC contacted, organizations that would potentially have useful information would include SPACECOM, the U.S. Cyber Command, and the National Air & Space Intelligence Center.

REFERENCES

[1] Clark, C. "US Must Improve Cyber Protection for Sats: Aerospace Corp." *Breaking Defense*, https://breakingdefense.com/2019/11/us-must-improve-cyber-protection-for-sats-aerospace/, 7 November 2019.

[2] Weeden, B., and V. Samson (editors). "Global Counterspace Capabilities: An Open Source Assessment." Secure World Foundation, https://swfound.org/media/206408/swf_global_counterspace_april2019_web.pdf, April 2019.

[3] Falco, G. "Job One for Space Force: Space Asset Cybersecurity." Harvard Kennedy School Belfer Center for Science and International Affairs, https://www.belfercenter.org/sites/default/files/files/publication/CSP%20Falco%20Space%20Asset%20-%20FINAL.pdf, July 2018.

[4] Erwin, S. "Space Information Sharing and Analysis Center to Be Based in Colorado Springs." *SpaceNews*, https://spacenews.com/space-information-sharing-and-analysis-center-to-be-based-in-colorado-springs/, 8 April 2019.

[5] Space ISAC. https://s-isac.org/, accessed 14 November 2019.

[6] Pittore, N. "FAQ: NSA/CSS Cybersecurity Directorate." NSA, https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/1912825/faq-nsacss-cybersecurity-directorate/, 23 July 2019.

[7] Keller, J. "DARPA to Brief Industry on Developing Artificial Intelligence and Cyber Security for Military Satellites." *Military & Aerospace Electronics*, https://www.militaryaerospace.com/computers/article/16726612/darpa-to-brief-industry-on-developing-artificial-intelligence-and-cyber-security-for-military-satellites, 5 September 2018.

[8] Thomas, P. R. "Blackjack." DARPA, https://www.darpa.mil/program/blackjack, accessed 18 November 2019.

[9] Seffers, G. I. "Teaching Satellites Self-Defense." SIGNAL, https://www.afcea.org/content/teaching-satellites-self-defense, 21 October 2019.

[10] Unal, B. "Cybersecurity of NATO's Space-Based Strategic Assets." Chatham House research paper, https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf, July 2019.

[11] Patch, C. "Satellite Protection From Electronic Warfare and Cyber Effects." CSIAC Technical Inquiry Response, CSIAC, November 2019.

[12] Resilient Navigation & Timing Foundation President. Personal communication, 8 November 2019.