Space Cybersecurity: A Survey of Vulnerabilities and Threats

Ulpia-Elena BOTEZATU[1,2]
[1]National Institute for Research and Development in Informatics - ICI Bucharest
[2]Romanian Space Agency
ulpia.botezatu@ici.ro, ulpia.botezatu@rosa.ro

Abstract: This article examines the critical need for cybersecurity in the space domain, presenting a comprehensive analysis of vulnerabilities, threats, mitigation strategies, and relevant standards and resources based on a survey of relevant space engineering-related literature. The study highlights the growing importance of preventative measures against cyberattacks and emphasizes the need for a robust understanding of cybersecurity risk management within the space sector. Key findings underscore the necessity for specialized cybersecurity standards and training programs tailored for space system professionals. The paper underscores the importance of integrating security considerations throughout the entire development lifecycle, from initial design to verification and validation, and advocates for ongoing research and collaboration to address the evolving landscape of cyber threats within the space domain. The article concludes with recommendations emphasizing a multi-layered approach to cybersecurity in space systems, fostering a secure and resilient future for this vital infrastructure.

Keywords: Cybersecurity, Space systems, Cyber threats, Cyberattacks, Artificial intelligence, Machine learning.

INTRODUCTION

While space systems represent a critical enabler in greater society's dependency on digital frameworks for communication, navigation, and defense, the connectivity of space systems with terrestrial networks makes them increasingly vulnerable to many forms of cyber threats. Cyber incidents against space systems, like malicious interference and spoofing of signals, may lead to impacts that go beyond simple disturbances; they touch on national security, economic stability, and even human lives. (Wang et al., 2023).

The field of space cybersecurity presents distinct challenges attributed to the physical seclusion of satellites, their extended operational durations, and the intricate nature of securing assets positioned in orbit. These systems endure sustained exposure to vulnerabilities, further exacerbated by limited chances for updates or physical intervention (Johnson, 2022). Events such as GPS jamming and cyber operations sponsored by states targeting satellite networks highlight the pressing need for cybersecurity frameworks specifically designed for space (ENISA, 2022). The present paper conducts an examination of prevailing vulnerabilities, strategies for mitigation, and the necessity for ongoing research and collaboration in order to safeguard this essential infrastructure (CCSDS, 2020).

https://doi.org/10.54851/v6i2y202405

CURRENT LANDSCAPE OF SPACE CYBERSECURITY

Space Systems and Cybersecurity Threats

Space systems underpin critical civilian and military operations, from communications to national defense (Egli, 2023). These systems, by their nature, rely heavily on uninterrupted data transmission, command, and control, which leaves them exposed to various attack vectors, such as jamming and spoofing, that compromise operational reliability. Jamming disrupts signals, while spoofing manipulates satellite navigation data, resulting in errors that can have catastrophic outcomes (Humphreys, 2019). Due to the increasing number of legacy systems in space that were designed without cybersecurity in mind, these vulnerabilities demand urgent remediation (Stiennon, 2020).

Several attack vectors can compromise space systems (Botezatu, 2023). Jamming, one of the most common techniques, disrupts satellite communications by flooding the satellite's signal with noise, making it impossible for the satellite to receive or transmit data accurately. Spoofing attacks involve sending false signals to satellites, misleading navigation systems and creating inaccuracies in location-based data (Humphreys, 2019). Advanced types of cyber attacks encompass malware infiltration and command injection, which take advantage of weaknesses within satellite software or ground stations to obtain unauthorized access to the satellite. As an illustration, an attacker may implement harmful commands to modify a satellite's orbit or deactivate its payload (Egli, 2023).

Ground stations function as the primary command and control hubs for satellite functionalities and are especially vulnerable to cyber attacks because of their linkage to worldwide networks. Weaknesses may arise from threats posed by insiders, deficiencies in the supply chain, or outdated cybersecurity measures. The intricate nature of space systems, coupled with the diverse range of stakeholders—including government bodies, private sector firms, and international organizations—exacerbates the challenges associated with the establishment of uniform cybersecurity protocols (Stiennon, 2020). A large portion of the satellites currently launched into space were designed before cybersecurity became a major concern; thus, there are many legacy systems that remain with core vulnerabilities. This requires a proactive and adaptive approach to the security of space systems to be able to implement sophisticated detection, prevention, and response mechanisms against evolving threats (Botezatu &Vevera, 2024).

Recent Cyber Incidents in Space

Theneedforadvancedcybersecuritymechanisms is reflected in the growing number of cyber-related incidents targeted at space infrastructure. In 2019, the U.S. Department of Homeland Security reported various critical location incidents of GPS signal interference believed to be supported by state actors. Such interference threatens the safety of both civilians and military personnel operating on accurate satellite navigation for critical activities that include transportation and logistics, as well as precision munition guidance (DHS, 2019). A more serious incident occurred in 2022 when the KA-SAT satellite network, operated by Viasat, was attacked, shutting off internet services across Europe just before the Russian invasion of Ukraine. The attack, against the satellite's ground-based network infrastructure, knocked out modems and left tens of thousands of users-military units included-without satellite communication capabilities.

A notable example is the 2022 Viasat KA-SAT attack, which disabled internet services across Europe before the Russian invasion of Ukraine. This attack highlights the strategic nature of space infrastructure and its vulnerabilities to cyber incidents during geopolitical crises (DHS, 2019). Such incidents signal the necessity for preemptive cybersecurity measures to protect satellite communication and prevent widespread disruption (Egli, 2023).

The escalating incidence of state-sponsored cyber operations, in conjunction with the emergence of non-state entities equipped to execute advanced cyberattacks, highlights the pressing necessity to reevaluate current cybersecurity frameworks. The formulation of robust and flexible defensive strategies is essential for protecting space infrastructure against prospective threats, thereby guaranteeing the security of critical services within an ever more competitive environment (Botezatu, 2024).

SURVEY OF VULNERABILITIES

Hardware and software deficiencies, consequences of human errors, and problems with third-party elements and services-the complex designs, human factors, and supply chain risks-make the systems of space entities vulnerable in many ways. This section reviews hardware and software deficiencies, the consequences of human errors, and third-party component and service challenges.

Hardware and Software Weaknesses

The extended operational life of satellites leaves them vulnerable to increasingly sophisticated threats. Many space systems, developed decades ago, operate with outdated components and communication protocols (Sinha & Banerjee, 2021). Compounding this, many communication protocols lack encryption and rely on obsolete standards, making them highly susceptible to jamming, spoofing, and data manipulation (Chan et al., 2022).

A very serious weakness lies in the communications protocols used for command and control. Often, these are proprietary, unencrypted, or use very old standards, which make them particularly vulnerable to third-party interception, data manipulation, or disruption. Vulnerable communications open the way for significant disruptions, particularly in the presence of RF interference, spoofing, or denial-of-service attacks. Moreover, software utilized in space missions is often highly specialized and may not experience the same thorough testing protocols as software that is more frequently deployed, thereby elevating the probability of discoverable bugs or vulnerabilities (Chan et al., 2022). Additionally, environmental conditions, including radiation exposure and extreme temperature variations, significantly affect the reliability of hardware and amplify security threats, underscoring the importance of resilience in both hardware and software for effective space cybersecurity.

Human Factor

The human factor is a substantial contributor to vulnerabilities in space systems. Insufficient cybersecurity awareness, poor training, or simple human errors can lead to serious security lapses. Inadequate security practices, such as the use of weak passwords, improper access management, or unsecured communication channels, create exploitable weaknesses in space operations. The specialized nature of space missions means that personnel often prioritize mission-specific tasks over cybersecurity, leading to gaps in security awareness and practices (Ewert, 2023).

Insider threats further complicate the human factor in space cybersecurity. Employees or contractors with legitimate access to critical systems may intentionally or unintentionally introduce vulnerabilities. This could range from sharing credentials to inserting malicious software or tampering with hardware. To mitigate these risks, space organizations must implement comprehensive training programs, enhance operational cybersecurity protocols, and adopt a security-first mindset across all levels of personnel (Kaspersky, 2020). Training programs and rigorous access controls are necessary to mitigate human vulnerabilities. Strong access control mechanisms and monitoring tools are essential to limit the damage that insider threats can cause.

Supply Chain Risks

The supply chain for space systems is another significant source of cybersecurity vulnerabilities. The globalized and multifaceted nature of supply chains introduces risks associated with third-party components or services. Many space missions rely on commercial off-the-shelf (COTS) hardware and software, which, while cost-effective, may not meet the stringent security requirements necessary for space operations. Given the complexity and global nature of space system supply chains, securing the supply chain is critical to maintaining system integrity (Hui, 2022).

Compromised supply chains can lead to the insertion of malware or tampered hardware components, jeopardizing the entire mission. Moreover, adversaries may target suppliers or logistics providers as an entry point to introduce vulnerabilities before these components are integrated into a space system. Addressing these risks requires a robust vetting process for suppliers, the implementation of strict procurement policies, and the conduct of thorough security audits. By securing the supply chain, space organizations can significantly reduce the risk of cyber threats and improve the resilience of their systems.

TAXONOMY OF CYBER THREATS

In general, the cyber threat in space systems is complex, targeting many components and exhibiting a wide range of vulnerabilities along the hardware, software, and communication infrastructures. This section will review the various threat types, such as APTs, and the position of AI/ML in offense and defense.

Types of Cyber Threats

Space systems are susceptible to various categories of cyber threats, all of which possess the capacity to interfere with critical services and operations: Jamming is defined as the intentional interference with radio frequency (RF) signals, thereby hindering communication between satellites and ground stations. Adversaries can incapacitate services such as communication, navigation, and earth observation by inundating satellite signals with noise. Such attacks can have a profound effect on both civilian and military infrastructures, as evidenced by earlier occurrences of GPS signal disruption (Humphreys, 2019).

Spoofing involves an attacker sending fake signals to satellite receivers, thereby fooling the receivers into processing counterfeit information. This might give wrong GPS coordinates, leading to navigation errors that could eventually lead to accidents or military mistakes. The more advanced spoofing techniques become, the more serious the risk to critical infrastructure relying on satellite-based navigation (Borre & Akos, 2021).

Malware and Ransomware: Malicious software could penetrate space systems either through ground segments or in the process of updating satellites with new software. This could potentially disrupt operational activities, leak critical information, or provide unauthorized access to system capabilities. Ransomware-which attacks targets by encrypting critical systems or data-presents a unique threat to space operations, holding vital infrastructure hostage until a ransom is delivered. The escalating complexity of malware and ransomware aimed at space systems underscores their increasing significance within the realm of cybersecurity (Kaspersky, 2020).

Advanced Persistent Threats

Advanced Persistent Threats (APTs) are generally characterized as state-supported or meticulously structured cybercriminal endeavors that specifically aim at particular systems with prolonged goals. These entities concentrate on penetrating systems and preserving clandestine access for protracted durations, thereby enabling the accumulation of intelligence or the disruption of space operations. APTs may direct their efforts toward satellites, ground stations, or even comprehensive supply chains with the objective of undermining national security or instigating extensive disturbance (Egli, 2023).

Advanced Persistent Threats are a specifically serious threat to space infrastructure due to the stealthy and long-lasting nature of the attack. Many of these attacks involve complex tactics, including spear-phishing, Day Zero exploits, and social engineering. Once an intrusion has been made, attackers can disrupt satellites or military communications, or steal proprietary data for use in espionage. The rampant number of nation-state-sponsored APTs calls for the immediate development of advanced detection and response methods, which would protect the space infrastructure (CISA, 2022).

Artificial Intelligence and Machine Learning-based Threats

Artificial Intelligence (AI) and Machine Learning (ML) are increasingly employed in both offensive and defensive cybersecurity applications within the space sector. Offensively, AI-driven tools can automate cyberattacks, making them more efficient and adaptable. Intelligent malware, for example, can evolve to evade detection by traditional security systems, while AI-powered algorithms can optimize jamming or spoofing attacks based on real-time feedback, further increasing their effectiveness (Harrison & Pearson, 2022).

AI and ML, on the defensive side, have great potential to enhance cybersecurity resilience. These will contribute toward enhancement in detecting anomalies, automating responses toward fresh emerging threats, and prediction of vulnerabilities by way of large-scale data analysis. AI-based systems can identify patterns in data that human operators may miss, thus leading to faster and more accurate responses towards cyber incidents. Nonetheless, the dual-use characteristics of artificial intelligence and machine learning pose difficulties, since opponents may utilize these identical technologies to augment their offensive capabilities (Zhou et al., 2023).

MITIGATION STRATEGIES AND BEST PRACTICES

In general, this will involve the development of a comprehensive approach to space system cybersecurity, including prevention, risk management, and application of standards for the entire system life cycle. This section highlights the main strategic approaches to securing space systems; it emphasizes a secure-by-design approach and the need for continuous monitoring.

Proactive Strategies and Secure-by-Design Methodology

Preventive approaches are urgently needed to mitigate the growing cyber threats against space infrastructure. A secure-by-design approach should be followed, from the early stages of system development to the final verification and validation processes, in order to ensure that cybersecurity is embedded within the core structure of the system architecture.

The adoption of sophisticated encryption methodologies and secure communication protocols is essential for the protection of data integrity and confidentiality during the transmission processes between space assets and ground stations. Effective encryption strategies are instrumental in thwarting unauthorized access or alteration of sensitive data (Chan et al., 2022).

Regular Software and Firmware Updates: Due to the long operational hours of space systems, keeping software and firmware up-to-date is a core countermeasure. Over-the-air updates, when possible, allow for quick action against vulnerabilities due to powerful fallback strategies, securing space systems against identified threats (Sinha & Banerjee, 2021).

Penetration Testing and Security Assessments: The implementation of routine penetration testing and security evaluations for both terrestrial and space-based systems facilitate the early detection of vulnerabilities prior to their potential exploitation. By mimicking cyberattacks, organizations can evaluate their defensive mechanisms and make requisite enhancements, thereby fostering a proactive approach to security (Harrison & Pearson, 2022).

Threat modeling and risk assessment are critical components for space organizations, which are required to create threat models and perform continuous risk evaluations to recognize and rank possible attack vectors. By comprehending the probability and repercussions of different threats, these organizations are able to distribute resources effectively and concentrate on the most pressing risks (CISA, 2022).

Ongoing Surveillance and Response to Incidents

As space systems are continuously monitored, this will support the need for a secure cybersecurity posture. In addition, it allows for early warnings through automated tools that detect anomalies and conducts real-time analysis of threats. Continuous monitoring makes it possible for organizations to act quickly on emerging risks and take remedial measures before they compromise critical systems.

Incident Response Planning: An effective incident response strategy is crucial for facilitating swift recovery following cyber incidents. In the context of space systems, this encompasses the orchestration of responses in collaboration with international partners, the establishment of failover protocols, and readiness for possible loss of command and control. Thorough planning is instrumental in mitigating the effects of cyberattacks and safeguarding the continuity of operations deemed mission-critical (Ewert, 2023).

Regulations and Standards in Guiding Secure Operations

Adherence to international standards and guidelines is important to formulate uniform cybersecurity practices across the space sector. Several basic standards exist to provide a minimum framework for safeguarding space systems:

CCSDS - Consultative Committee for Space Data Systems: CCSDS provides recommendations over securing operations of space missions, especially regarding data transmission, network security, and the use of encryption. These recommendations set a baseline for building secure systems in space (CCSDS 2020).

ISO 27001: This international standard outlines the requirements for implementing an information security management system (ISMS), which can be adapted to space operations. ISO 27001 focuses on systematically managing sensitive information, making it a valuable tool for safeguarding space-based assets (Zhou et al., 2023).

NIST SP 800-160: This standard emphasizes systems security engineering and promotes the integration of security throughout the system development lifecycle. By adopting a secure-by-design philosophy, space organizations can develop more resilient systems that are capable of withstanding both current and future cyber threats (NIST, 2016).

Continuous Improvement and Lifecycle Security

The protection of security in space systems requires continuous improvement and attention throughout the entire life cycle of the operation. Here, periodic security assessments, updates, and resilience tests are done to reduce any newly detected vulnerability. Further, the infusion of artificial intelligence and machine learning can also enhance threat detection and response capabilities to ensure that space systems remain secure in an increasingly hostile cyber environment Harrison & Pearson, 2022.

RECOMMENDATIONS FOR A MULTI-LAYERED APPROACH TO SPACE CYBERSECURITY

Space systems require a comprehensive approach to defense, addressing multifaceted nodes of cyber threats. This would involve physical security, network security, software security, and, importantly, international cooperation in terms of informationsharingandreadinesstoactinresponse.

Defense-in-Depth Strategy

Space infrastructure protection requires a defense-in-depth strategy. This would include multiple layers of security, each focusing on different potential attack vectors:

Physical Security: Ground stations, data centers, and other physical assets should be protected by physical barriers, biometric controls, and surveillance systems that deter unauthorized access (CCSDS, 2020, 2022).

Network and Communication Security: Encrypted data transmission and use of strong authentication protocols are paramount for securing satellite communication. Intrusion Detection Systems IDS and firewalls add to network integrity protection (Chan et al., 2022).

Software and System Hardening: Consistently updating software, applying patches, and enacting strategies such as secure boot procedures and redundancy protocols guarantee that space systems maintain their resilience in the face of advancing cyber threats (Sinha & Banerjee, 2021).

Collaboration and Information Sharing

Given the global nature of space activities, cooperation at the international level and intelligence sharing of threats are imperative for a robust cybersecurity framework.

Establishment and standardization of cybersecurity protocols, such as those by the Consultative Committee for Space Data Systems and the International Organization for Standardization, allow for the realization of consistent security practices in space missions (CCSDS, 2020). Entities such as the Space Information Sharing and Analysis Center (Space ISAC) enable the exchange of attack methodologies, vulnerabilities, and strategies for mitigation, thereby enhancing the capacity of organizations to react swiftly to evolving threats (Space ISAC, 2021). Global partnerships, including coordinated incident response drills and research initiatives, improve worldwide readiness and collaboration in safeguarding space systems from cyber threats (Hui, 2022).

CONCLUSIONS

The Cybersecurity framework relating to space systems is faced with complex problems emanating from specific vulnerabilities in hardware, software, human elements, and the supply chain. These are exposed to a range of threats including jamming, spoofing, malware, and advanced persistent threats. Adversaries are increasingly using AI and ML, making the sophistication of cyber-attacks on space infrastructure continuously growing.

The approach to mitigation includes defense-in-depth, such as secure communication protocols, encryption, periodic updates, and thorough security testing. Organized risk management methodologies involve the application of frameworks like ISO 27001 and CCSDS standards. System hardening introduces principles of secure by design, together with continuous monitoring, narrowly targeted personnel training in the space industry. Security is further enhanced by cooperation across the industry, including information sharing.

The following crucial areas need further research to strengthen space cybersecurity:

- AI and ML open up great avenues for defense, such as advanced threat detection and response mechanisms that are automated. Further research needs to be invested in adapting these technologies to the special conditions of space operations, focusing on real-time anomaly detection and predictive analytics.
- With the advancement of quantum computing, conventional encryption techniques are increasingly becoming outdated. It will be essential to investigate quantum-resistant algorithms and to incorporate quantum cryptography in space communications to ensure the security of forthcoming space systems (Zhou et al., 2023).
- The international nature of space missions demands the creation of incident response guidelines that are globally harmonized. Investigations should look into the challenges involved in cross-border coordination and how best to automate response capabilities to mitigate the effects of cyberattacks.

Space cybersecurity will involve the collective efforts of industry, governments, and research institutions. There is a need for collaboration on developing international standards, sharing threat intelligence, and executing joint cybersecurity initiatives. Governments can encourage international cooperation, establish policies, and fund research that will help move forward space cybersecurity.

Organisations should pay considerable attention to cybersecurity, using secure-by-design methodologies and performing regular updating in order to reduce the impact of emerging threats. Training for space professionals should be enhanced to develop a workforce capable of dealing with these emerging threats. With further expansion in space, a coherent and proactive approach is necessary to ensure longterm security and resilience within key space infrastructure.

REFERENCE LIST

Borre, K. & Akos, D. (2021) Global Navigation Satellite Systems (GNSS) Spoofing and Its Countermeasures. *Journal of Navigation*. 74(2), 239-258.

Botezatu, U.-E. (2024) Cybersecurity in the Era of Space Domain Awareness. *Romanian Cyber Security Journal*. 6(1), 29-38. doi:10.54851/v6i1y202403.

Botezatu, U.-E. (2023) Attempted Cyber Security of Systems and Operations in Outer Space: an Overview of Space-based Vulnerabilities. *Romanian Cyber Security Journal*. 5(1), 67-76. doi:10.54851/v5i1y202306.

Botezatu, U.-E., & Vevera, A.-V. (2024) *Cyber Orbits: The Digital Revolution of Space Security*. IntechOpen. doi: 10.5772/intechopen.1005235.

Chan, T., Lopes, A. & Smith, D. (2022) Space Communication Protocols: Challenges and Security Solutions. *IEEE Communications Surveys & Tutorials*. 24(2), 1047-1068.

Cybersecurity and Infrastructure Security Agency (CISA) (2022) *APT Cyber Tools Targeting Space and Satellite Operations*. CISA Alert AA22-113A.

Consultative Committee for Space Data Systems (CCSDS) (2020) *Security Threats Against Space Mission Operations*. CCSDS 350.0-G-1.

Consultative Committee for Space Data Systems (CCSDS) (2022) *Security Threats Against Space Missions*. CCSDS 350.1-G-3. Green Book. Washington, DC, USA.

U.S. Department of Homeland Security (DHS) (2019) *GPS Signal Jamming: An Evolving Threat*. DHS Report. https://www.dhs.gov/archive/science-and-technology/first-responder-electronic-jamming-exercise [Accessed 6th Novenber 2024]

Egli, D. (2023) Space Cybersecurity: Challenges and Strategies. *Space Policy*. 69, 101503.

European Union Agency for Cybersecurity (ENISA) (2022) *Cybersecurity Threats to Space Systems and Their Potential Impact*. ENISA Report.

Ewert, M. (2023) The Human Factor in Space Cybersecurity: Training and Awareness. *Space Policy*. 70, 101512.

Harrison, J. & Pearson, G. (2022) *The Role of AI in Offensive and Defensive Cybersecurity for Space Systems*. AI & Society. 37, 1221-1235.

Hui, M. (2022) Supply Chain Security in Space Systems: Assessing the Risks. *Journal of Space Safety Engineering*. 9(4), 315-323.

Humphreys, T. E. (2019) *The Effects of GPS Jamming and Spoofing on Civilian and Military Systems. International Journal of Critical Infrastructure Protection*. 27, 24-33.

Johnson, R. (2022) Satellite Cybersecurity: Understanding and Mitigating Emerging Threats. *Space Policy*. 58, 101472.

Kaspersky (2020) *Cybersecurity Threats to Space Operations: Insider Risks and Prevention Strategies*. Kaspersky Security Reports. https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security [Accessed 2nd November 2024]

Satellite Today (2022) *Cyberattack on Viasat's KA-SAT Network Disrupts Communications Across Europe*.

Sinha, A. & Banerjee, S. (2021) Cybersecurity for Space-Based Systems: Addressing Legacy Vulnerabilities. *Journal of Aerospace Information Systems*. 18(6), 421-433.

Space Information Sharing and Analysis Center (Space ISAC) (2021) *Building a Community of Resilience in Space Cybersecurity*. Space ISAC Report.

Stiennon, R. (2020) *There Will Be Cyberwar: How the Move to Network-Centric War Fighting Has Set the Stage for Cyberwar*. IT-Harvest Press.

Wang, S., Xu, Y., Liu, Q., & Zhang, Y. (2023) *Cybersecurity Threats and Protection Strategies for Satellite Systems: A Comprehensive Review*. IEEE Access, 11, 25332-25345.

Zhou, Q., Huang, S., & Wang, L. (2023). *AI-Driven Cybersecurity for Space Operations: Capabilities and Risks*. IEEE Transactions on Aerospace and Electronic Systems, 59(3), 1140-1153.