OVERVIEW OF THE THREAT OF CYBER INCIDENTS IN THE SPACE DOMAIN

Dimitar Dimitrov, Evgeni Andreev

Nikola Vaptsarov Naval Academy, Department of Information Technology
e-mail: dimitar@nvna.eu; e.andreev@naval-acad.bg

Keywords: *cyber incidents, space domain, spacecraft, KA-SAT*

Abstract: *The report examines the threat of cyber incidents related to the space domain. It reviews the main techniques, tactics, and procedures that hackers can use to compromise the security of spacecraft and missions. Some of the most high-profile and high-risk attacks on the space sector, both on the ground and in space, are discussed. Focus is placed on the hacking attack on Viasat's KA-SAT network in 2022.*

ОБЗОР НА ЗАПЛАХИТЕ ОТ КИБЕР ИНЦИДЕНТИ В КОСМИЧЕСКАТА ОБЛАСТ

Димитър Димитров, Евгени Андреев

Висше военноморско училище „Н. Й. Вапцаров“, Катедра „Информационни технологии“
e-mail: dimitar@nvna.eu; e.andreev@naval-acad.bg

Ключови думи: *киберинциденти, космическата област, космически апарати, KA-SAT*

Резюме: *Докладът разглежда заплахата от киберинциденти, свързани с космическата област. В него се прави преглед на основните техники, тактики и процедури, които хакерите могат да използват, за да компрометират сигурността на космически апарати и мисии. Обсъждат се някои от най-значимите и високорискови атаки срещу космическия сектор – както на наземните сегменти, така и в орбита. Акцентът е поставен върху хакерската атака срещу мрежата KA-SAT на Viasat през 2022 година.*

Introduction

As the post-digital era takes hold, cyberspace and outer space are no longer separable technical realms but a fused, interdependent infrastructure. Satellites, ground stations, cloud-enabled mission control and user terminals now operate as a single cyber-physical system that underpins communications, navigation, finance, logistics and defense. This digitalization of space expands the attack surface from the spacecraft itself to the entire lifecycle and supply chain, binding orbital assets to terrestrial networks and making cyber risk inseparable from space operations. In policy and doctrine alike, space and cyber are increasingly treated as mutually enabling operational environments, in practical terms, modern space capabilities ride on the same networks, protocols and software stacks that shape cyberspace.

Within this integrated system, cyber incidents against space infrastructure now constitute national-security concerns rather than narrow technical anomalies. The February 2022 cyber operation against Viasat's KA-SAT [1] network illustrates the point: Russian military intelligence (GRU) first used DDoS to disrupt terminals, then exploited a misconfigured VPN in the management segment to push the AcidRain wiper to thousands of SurfBeam 2 modems, degrading Ukrainian military connectivity and producing cascading civilian effects across Europe. Beyond the immediate loss of service, the KA-SAT incident exposed cross-sector dependencies, for example, German wind farms SCADA connectivity, where a single disruption in satellite internet propagated risk to power and emergency services, highlighting how commercial, dual-use systems can become strategic targets in conflict. Compiled evidence from the Russo-Ukrainian war further shows a marked uptick in cyber

activity directed at the space sector. This operational reality is situated within the broader context of strategic competition. Commercial mega constellations and private ground infrastructure have become critical factors for military C2 and national resilience, driving adversaries to use cost-effective, deniable cyber means against space systems rather than kinetic attacks that produce fallout. Non-state hackers operate as ecosystems of proxies, often represented or supported by state interests and are more active against space targets, while threats openly discuss space systems as ultimate challenges, indicating both heightened intent and a learning curve that accelerates with each widely publicized incident. Although many attacks remain unsophisticated, the overall pace, the variety of targets, such as national agencies to manufacturers and service providers, and the timing around political events indicate that cyber operations against space assets are becoming normalized tools of influence and disruption in crises that do not reach the level of war.

At the same time, governance and standards have struggled to keep pace with this convergence. ENISA's 2025 Space Threat Landscape [2] emphasizes the need for sector-specific, lifecycle-aware controls and notes gaps despite recent advances such as NASA's Space Security: Best Practices Guide (2024), ECSS's Security in Space Systems Lifecycles (2024), and longstanding US policy direction in Space Policy Directive-5 (SPD-5) [3]. Technically, defense-in-depth architectures and threat-informed requirements remain the cornerstone of spacecraft and ground-segment protection, but their translation into consistently engineered baselines across civil and commercial programs is uneven an asymmetry that adversaries can and do exploit.

Overview of the attack surface of the space domain

The digitization of space infrastructure has transformed satellites from isolated orbital artifacts into nodes of a vast, software-defined, cyber-physical system. Mission planning, tasks, telemetry, and data usage increasingly depend on ground networks, cloud services and automated update channels. In this configuration, the space domain is inseparable from the cyber substrate that brings it to life. The ENISA report on space threats highlights this very link between the life cycle [4] (design, manufacturing, launch, operation and decommissioning), arguing that risk now accumulates across all phases and actors, rather than at a single technical boundary. The CSS analysis [5] also notes that cyberspace and outer space share open, cross-border, and immaterial characteristics that encourage exploitation, especially as satellites adopt internet connectivity and software-defined control.

A practical way to think about this unified domain is through the classic segmentation of ground, space, and user segments, each supported by the connection itself. The ground segment encompasses mission control systems, electrical ground equipment, satellite control centers, and business IT environments (email, ERP), all connected via wide area networks and Space Link Extension for data exchange with telemetry, tracking, and command stations. The space segment covers the bus, payload, onboard software, attitude and data control, and interfaces between satellites or between space and ground. The user segment covers terminals and end devices through which services are used and commands can be relayed indirectly. ENISA's asset taxonomy maps these segments to life cycle phases and actors, clarifying where third-party dependencies and supply chain risks arise. This scaling of the system of systems expands the attack surface. In the ground segment, adversaries can exploit misconfigurations in remote access, such as VPNs, weaknesses in identity and access management or insufficient segregation between business IT and operational networks. Once footholds are established, the control planes that coordinate fleets of terminals or modems become attractive targets, enabling broad, synchronized effects.

Within the space domain, vulnerabilities stem from design choices as well as inherent physical limitations. Space vehicles operate as interconnected computing systems linked through unstable wireless channels and the notion that outer defenses alone suffice has resulted in inadequate internal partitioning and unprotected operations that falter when perimeters are violated. Aerospace sector standards, grounded in threat analysis, highlight dangers such as vulnerable or unverified control pathways, overrides of encryption in protected configurations, inadequate foundational security and verification for operational software and the possibility of mission loads causing power exhaustion that leaves the craft in a compromised condition. These standards advocate for secure boot processes with extensive safeguards, verification of directives, isolation of communication lines, improved fault handling and resilient security states that sustain verification and data protection amid adversity.

The data link layer serves as a prime target for threats. While jamming and spoofing are still prevalent, the protection of data confidentiality and integrity at this layer relies heavily on secure protocols and rigorous cryptographic practices. Guidelines from the CCSDS on securing space data offer protections at the link level for confidentiality, integrity and authentication, yet adoption varies widely, particularly in commercial areas where encryption is sometimes viewed as optional. Flaws in protocols, inadequate key handling and restricted algorithm adaptability create exploitable weaknesses in both uplink and downlink communications, amplified by the use of software-defined

radios and adaptable payloads that expand the system's adaptability and potential entry points for attacks. Within the consumer market, diversity and volume heighten vulnerabilities. Terminals used by individuals or businesses are frequently situated beyond secure operational settings, with their software origins, update routines, and setup standards often falling short of ideal security measures. The KA-SAT incident illustrated this, where a system intended for overseeing a network of modems was hijacked to distribute harmful updates once compromised, revealing how user-end devices can escalate broader system failures. Across multiple areas, the supply chain and development processes reveal widespread vulnerabilities. Spacecraft and ground systems depend on commercial off-the-shelf (COTS) parts and firmware sourced globally, which can lead to risks such as tainted hardware, counterfeit components or software supply chain attacks. Research by Bailey [6] supports the certification of trusted suppliers (DMEA accreditation for critical microelectronics), rigorous evaluation before silicon fabrication, and strict control of development environments to prevent insertion of malicious code and to ensure traceability and uniformity in production. Protecting design resources like command dictionaries, FMEA/FMECA reports, and system blueprints is equally important because their exposure speeds up adversaries' ability to find system vulnerabilities.

Recent conflict data emphasize that these vulnerabilities are actively targeted. The CSS/ETH Zürich dataset documenting the Russo-Ukrainian conflict since 2022 shows over 100 cyber incidents mostly aimed at ground infrastructure [7] such as web services, corporate networks, and user devices, while major destructive attacks like the KA-SAT incident are rare but severe. The threat actors tend to be generalists exploring the space sector rather than specialists, sometimes mistakenly hitting unintended targets, reflecting limited current expertise but fast-changing threats. Hacktivist groups with varying state ties have attacked space-related targets, and state-sponsored cyber activities are likely underreported, only appearing publicly in high-profile or officially recognized cases.

In this developing threat landscape, embedding security by design is an essential engineering priority. ENISA stresses integrating security by design and default across the satellite lifecycle, supported by asset classification and interoperable safeguards, aligning with EU initiatives such as NIS2 and the Cyber Resilience Act. Standards efforts like ECSS lifecycle security and IEEE P3349 and secure development lifecycle strategies for link-layer defense are also important. In the U.S., Space Policy Directive-5 promotes risk-based cybersecurity principles and collaboration with commercial partners to set baseline standards [8]. Aerospace guidelines translate these principles into practice by advocating a threat-informed, layered defense that anticipates breaches, ensuring authenticated and encrypted operations even under compromise.

TTPs in space cyber operations

At the radio level, electronic warfare tactics like jamming and spoofing are fundamental techniques because they provide immediate denial or deception without needing deep system infiltration. Jamming disrupts telemetry [9], tracking, command links, or mission data channels, causing traditional availability issues and forcing devices or spacecraft to enter limited operational modes. Spoofing exploits weaknesses in authentication or anti-replay mechanisms, causing system misbehavior. According to Bailey’s research, these are top risks: jamming is specifically coded under SV-AV-1, while spoofing and replay attacks align with command-link intrusions under access control threats (SV-IT-1, SV-AC-2) [10]. The protective measures focus on authenticated, encrypted communications, anti-replay protections, and disciplined key management so spacecraft never accept unauthorized commands or weaken cryptographic safeguards during recovery.

The KA-SAT attack demonstrates related ground-based tactics, where attackers exploited poorly managed remote access to move laterally into privileged control domains and execute objectives using operators’ own tools [11]. This operation was made more resilient by using the management network, which controls customer terminals, as a distribution channel for destructive payloads, allowing targeted, synchronized effects on the fleet. Also, attackers combined destructive malware with denial-of-service attacks on KA-SAT’s DHCP services, overwhelming recovery attempts and prolonging disruption. Open-source analyses highlight common initial access methods such as VPN misconfigurations and credential reuse in enterprise contexts. When malware targets space operations, it generally prioritizes rapid spread and impact over stealth [12]. AcidRain malware exemplifies this by leveraging trusted channels to degrade endpoints below recoverable software states, imposing costly physical remediation burdens. ENISA’s analysis highlights the severe consequences of firmware corruption and destructive updates, especially given satellite networks’ large scale, where operator errors can cause mass device failures.

While focus often lies on terminals and ground IT assets, attackers also target spacecraft onboard software and fault management, trying to exploit recovery modes. Bailey emphasizes the risk of safe modes that disable cryptographic protections or relax command authentication, which could

enable injection or replay attacks. Therefore, cyber-safe modes maintaining encryption and authentication, secure boot chains, and strict inter-bus segregation on spacecraft are vital safeguards.

Adversaries increasingly employ a combination of technical tactics, techniques, and procedures (TTPs) alongside obfuscation and narrative manipulation strategies. Concurrent distributed denial-of-service (DDoS) or electronic warfare (EW) activities [13] often serve as distractions that conceal more covert intrusions into management planes. Additionally, adversaries' self-attribution tactics obfuscate public understanding and complicate communication efforts among operators. Reflections by Viasat's security leadership underscore the importance of detecting recurring attack patterns early to fortify defenses proactively, while cautioning that false-flag operations and cloud data leakages may inadvertently accelerate adversaries' learning processes [14]. The growing prevalence of cyberattacks targeting space-related entities signals a shift from a niche, low-volume threat landscape to one characterized by political signaling. Consequently, rudimentary techniques such as DDoS, basic intrusions, and opportunistic spamming persist alongside sophisticated state-level operations [15].

The predominant chain of TTPs in the space sector is pragmatic and multi-layered, typically involving terrestrial entry points created by misconfigurations or partner vulnerabilities, lateral movements targeting orchestration or update infrastructures, and synchronized attacks executed at population scale [16], including malicious configurations and destructive updates, augmented by denial-of-service campaigns at the link layer or DHCP flooding. Where possible, attackers also exploit recovery processes or safe-mode functionalities within spacecraft. Effective defense-in-depth strategies reflect this complexity and are well-documented across authoritative sources. These include the implementation of authenticated, anti-replay command links that maintain continuous cryptographic protections; robust root-of-trust and verified boot processes; stringent segmentation of buses and enclaves; rigorously managed, signed, and monitored update channels with rollback capabilities; and lifecycle-aware ground control systems that treat management planes as critical assets. The KA-SAT incident exemplifies how commonplace IT tradecraft, when magnified by the scale and centralization inherent to satellite networks, constitutes a significant threat vector, highlighting that cyber adversaries extend traditional cyber tactics to the unique operational context of space infrastructure [17, 18].

Conclusion

The cybersecurity threat landscape in the space domain has become increasingly complex, dynamic, and critical, reflecting the deep integration of cyberspace and outer space into a unified cyber-physical ecosystem. Satellites and their supporting ground infrastructures now underpin vital global functions in telecommunications, navigation, finance, defense, and emergency services, making them essential yet vulnerable assets with a broad attack surface spanning design, manufacturing, launch, operation, and decommissioning phases. High-profile incidents such as the 2022 Viasat KA-SAT attack illustrate how adversaries exploit common IT weaknesses, like misconfigurations, poor access controls and supply chain risks, to achieve disruptive outcomes at scale, revealing how traditional cyber tactics are adapted and amplified in space contexts.

The threats originate from a diverse set of actors, including state-affiliated groups, proxies, hacktivists, and cyber criminals, who increasingly apply layered tactics, techniques and procedures involving jamming, spoofing, lateral network movement, destructive malware deployment, and obfuscation through concurrent electronic warfare or denial-of-service activities. These methods mask sophisticated intrusions targeting management and command planes and recovery mechanisms, significantly complicating detection and mitigation efforts. Moreover, the hybridization of threat narratives and false-flag operations reflects the strategic role cyberattacks on space assets play in political signaling and influence operations, underscoring the importance of threat intelligence and attribution in shaping defense postures.

Significantly, the space cybersecurity challenge demands holistic risk management that integrates ground IT security with space hardware and software assurance throughout the satellite lifecycle. Operators must recognize that vulnerabilities often originate on human error, insecure engineering or supply chain compromises and that exploiting these can enable cascading disruptions affecting entire satellite constellations and the critical services they deliver. Enhanced data sharing, regulatory frameworks, and collaborative information-sharing centers contribute toward a stronger collective defense, but proactive engagement and continual adaptation by all stakeholders remain imperative.

References:

1. Kazi, A., et al. Invisible battlefields: analyzing the Viasat attack and its broader implications. Scientific Bulletin (Nicolae Balcescu Land Forces Academy) 30(1), 59–67, 2025. https://doi.org/10.2478/bsaft-2025-0007
2. ENISA. ENISA Space Threat Landscape 2025. European Union Agency for Cybersecurity, 2025. Available online at: https://www.enisa.europa.eu/sites/default/files/2025-03/Space_Threat_Landscape_Report_fin.pdf
3. Anjum, N., and T. Farheen. SoK: Securing the final frontier for cybersecurity in space-based infrastructure. Available online at: https://doi.org/10.48550/arXiv.2507.17064
4. Cucinschi, A. Cyber and space domains – Impact on the development of the multi-domain operations. Bulletin of "Carol I" National Defence University (BNDU) 12(1), 80–91, 2023. Available online at: https://revista.unap.ro/index.php/bulletin/article/view/1677
5. Poirier, C. Understanding cybersecurity in outer space. Center for Security Studies, ETH Zurich, 2024. Available online at: https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse343-EN.pdf
6. Bailey, B. Cybersecurity protections for spacecraft: a threat-based approach. The Aerospace Corporation, 2021-04-29. Available online at: https://aerospace.org/sites/default/files/2022-07/DistroA-TOR-2021-01333-Cybersecurity%20Protections%20for%20Spacecraft--A%20Threat%20Based%20Approach.pdf
7. Poirier, C. Hacking the cosmos: Cyber operations against the space sector. Cyber defense Report, Center for Security Studies, ETH Zurich, October 2024. Available online at: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/cyber-reports-2024-10-hacking-the-cosmos.pdf
8. Fleming, C., et al. Securing commercial satellites for military operations: a cybersecurity supply chain framework. International Conference on Cyber Warfare and Security 18(1), 85–92, 2023. https://doi.org/10.34190/iccws.18.1.1062
9. Atanasov, V. E. and I. Iliev. Electrocardiogram signal processing: integrating filter fusion techniques. Diagnostyka 26(4), art. no. 2025402, 2025. https://doi.org/10.29354/diag/211623. Available online at: https://doi.org/10.29354/diag/211623
10. Waterman, S. Hackers attacked satellite terminals through management network, Viasat officials say. Air & Space Forces Magazine, 2022. Available online at: https://www.airandspaceforces.com/hackers-attacked-satellite-terminals-through-management-network-viasat-officials-say/
11. Sharmin, A., et al. Cyber attacks on space information networks: vulnerabilities, threats, and countermeasures for satellite security. Journal of Cybersecurity and Privacy 5 (3), article 76, 2025. https://doi.org/10.3390/jcp5030076
12. Barrett, T. Looking to the skies: the importance of satellite cybersecurity. United States Studies Centre, 2024. Available online at: https://www.ussc.edu.au/the-importance-of-satellite-cybersecurity
13. Mura, A. An analysis of the cyberattack against ViaSat of February 2022, 2022. Available online at: https://centri.unibo.it/computational-social-science/it/cosa-facciamo/our-students-papers/mura_cs-cw2024_final.pdf/@@download/file/Mura_CS&CW2024_FINAL.pdf
14. Klein, J.. Space and cyber warfare as one. CSIS, 2024. Available online at: https://www.csis.org/analysis/space-and-cyber-warfare-one
15. Poirier, C. Cyber operations against the space sector in the Russo-Ukrainian War. Russian Analytical Digest 328, p. 20, 2025. https://doi.org/10.3929/ethz-b-000738640
16. Nikolov, D. Концептуален подход за създаване на сценарии за киберучения, базиран на основни модели за анализ на кибератаки и пробиви в сигурността. SiT Review 2, 10–24, 2025. ISSN 2738-7593
17. Bitic, A. G. The supply chain vulnerability in EU space infrastructure. VOYCE. Available online at: https://voycecommunity.eu/our-work/f/the-supply-chain-vulnerability-in-eu-space-infrastructure
18. Leventopoulos, S., and N. Benias. Cyber warfare affecting land, sea, air and space operations. Journal of Computations and Modelling no. 7, 29–34.