Cybersecurity and Law

2026 Nr 1(15)

DOI: 10.35467/cal/221060

Cyber and Signal Threats to Space Infrastructure

Zagrożenia cybernetyczne i łączności dla infrastruktury kosmicznej

Marcin MAZUR
Polish Space Agency
ORCID: 0009-0002-5681-4807
E-mail: marcin.mazur@polsa.gov.pl

Abstract

This article describes the growing importance of space for the functioning of states, economies, and everyday life. Satellite systems are now crucial for communications, navigation, and financial services, among other things, making their loss or disruption a serious threat. With the development of space technologies, the number of cyberthreats is growing. From simple signal interception incidents in the 20th century, we have moved to advanced attacks such as jamming, spoofing, DDoS and APT cyberattacks, and satellite eavesdropping. A particular increase in threats occurred after 2022 (the war in Ukraine), demonstrating the strategic importance of space infrastructure in conflicts. Satellite systems are vulnerable to attacks primarily due to their commercial nature – companies often limit security investments due to cost. Furthermore, many systems are outdated and unsuited to modern threats, and the lack of uniform standards complicates protection. The article indicates that artificial intelligence can help improve security, for example, by detecting anomalies, identifying interference, and automatically responding to attacks. At the strategic level, the role of the European Union was emphasized, as it is beginning to regulate the sector (e.g., the NIS2 Directive), although legal loopholes and the need for better cooperation between industries remain. Conclusion: space infrastructure is critical today, but increasingly vulnerable to cyberattacks. Ensuring its security requires investment, new technologies (including AI), regulation, and international cooperation.

Keywords

space safety, cyberthreats, cyberspace, signal threats, in-orbit eavesdropping, AI in space

Streszczenie

Niniejszy artykuł opisuje rosnące znaczenie przestrzeni kosmicznej dla funkcjonowania państw, gospodarek i życia codziennego. Systemy satelitarne mają obecnie kluczowe znaczenie między innymi dla komunikacji, nawigacji i usług finansowych, co sprawia, że ich utrata lub zakłócenie stanowi poważne zagrożenie. Wraz z rozwojem technologii kosmicznych rośnie liczba cyberzagrożeń. Od prostych incydentów przechwytywania

sygnałów w XX wieku, przeszliśmy do zaawansowanych ataków, takich jak zakłócanie, spoofing, cyberataki DDoS i APT oraz podsłuch satelitarny. Szczególny wzrost liczby zagrożeń nastąpił po 2022 roku (wojna na Ukrainie), co pokazuje strategiczne znaczenie infrastruktury kosmicznej w konfliktach. Systemy satelitarne są podatne na ataki przede wszystkim ze względu na swój komercyjny charakter – firmy często ograniczają inwestycje w bezpieczeństwo ze względu na koszty. Ponadto wiele systemów jest przestarzałych i nieprzystosowanych do współczesnych zagrożeń, a brak jednolitych standardów komplikuje ochronę. W artykule wskazano, że sztuczna inteligencja może pomóc w poprawie bezpieczeństwa, na przykład poprzez wykrywanie anomalii, identyfikację zakłóceń i automatyczne reagowanie na ataki. Na poziomie strategicznym podkreślono rolę Unii Europejskiej, która zaczyna regulować sektor (np. dyrektywa NIS2), choć wciąż istnieją luki prawne i potrzeba lepszej współpracy między branżami. Wniosek: infrastruktura kosmiczna ma dziś kluczowe znaczenie, ale jest coraz bardziej podatna na cyberataki. Zapewnienie jej bezpieczeństwa wymaga inwestycji, nowych technologii (w tym sztucznej inteligencji), regulacji i współpracy międzynarodowej.

Słowa kluczowe

bezpieczeństwo kosmiczne, cyberzagrożenia, cyberprzestrzeń, zagrożenia sygnałowe, podsłuch na orbicie, sztuczna inteligencja w kosmosie.

Introduction

The development of space technologies and their widespread use for civilian and military purposes have significantly increased the importance of space for the functioning of our economies. It should be noted that production, trade in goods and services, and industrial development rely heavily on satellite resources. Limiting access or completely eliminating these capabilities would threaten the pursuit of national interests. The rapid growth in the number of satellite systems has led to increasing dependence of society, the economy, and public administration on data, products, and services (DPS) originating from space. Activities such as checking the weather forecast, obtaining up-to-date information on a train's location, or making an international transfer all require the use of space-based resources[1].

A key aspect of space utilisation, forming the foundation of the state's security system, is both the capability to operate in space and assured access to satellite resources. At the same time, the expanding role of space activities has resulted in a growing number of potential threats, both natural and human-induced. Any restriction or disruption of access to space resources may therefore pose a serious risk to national interests. Given the increasing reliance on space assets and the evolving threat landscape, cybersecurity in the space domain has become a critical issue. Cyberattacks, jamming, interference, spoofing of satellite services, eavesdropping, and data interception are becoming increasingly common due to the commercial nature of services and the rapid development of cyber tools.

The main objective of this article is to examine the nature and scale of cyber threats directed against space infrastructure, which plays a critical role in national security systems. Furthermore, the article analyses the causes of these risks and explores the potential application of new technologies, as well as the instruments implemented at the European Union level. Accordingly, the article

[1] M. Mazur, Logistics Security in Transport and Decision-making Problems in the Management of European Satellite Resources in Space, “Rocznik Ochrona Środowiska” 2025, vol. 27, pp. 788-798. Website: https://doi.org/10.54740/ros.2025.063.

addresses the following issues: threat developments and examples, the causes of space infrastructure vulnerability, examples of resilience solutions, strategic aspects of cybersecurity.

The article is structured into four parts. The first outlines the evolution of threats since the early 1970s, highlighting a marked increase since 2022, i.e., the Russian invasion of Ukraine. The second part examines the vulnerability of satellite systems, largely resulting from the commercial nature of the services provided. The third part discusses the potential application of artificial intelligence as a tool supporting advanced security mechanisms such as encryption. The final part presents the strategic dimension of cybersecurity at the European Union level.

Despite the growing number of studies and policy reports addressing cybersecurity challenges in space systems, a significant research gap remains in the integrated analysis of cyber, signal, and organizational vulnerabilities of space infrastructure, particularly in the context of increasing reliance on commercial satellite services. Existing publications often focus on selected technical aspects or legal frameworks, without sufficiently capturing the systemic nature of threats affecting space-based services as critical enablers of modern security and defence systems.

The research problem addressed in this article concerns the increasing exposure of space infrastructure to cyber and signal threats, combined with insufficient technological, organizational, and regulatory mechanisms to ensure system resilience in the current security environment.

To solve the above mentioned problem, the article seeks to answer the following research questions: What types of cyber and signal threats currently pose the greatest risk to space infrastructure? What structural and organizational factors contribute to the vulnerability of satellite systems, particularly those operated by commercial entities? To what extent can artificial intelligence–based solutions support the detection, mitigation, and response to cyber threats in the space domain?

The aim of this article is to identify and systematize contemporary cyber and signal threats to space infrastructure, analyse their underlying causes, and assess selected technological and strategic approaches – particularly those based on artificial intelligence – aimed at strengthening system resilience.

This study is based on qualitative research methods, including document analysis of open-source intelligence materials, strategic policy documents, and industry reports published between 2020 and 2025, as well as peer-reviewed articles in academic journals. Comparative analysis was applied to identify recurring threat patterns and systemic vulnerabilities affecting space infrastructure. Additionally, selected case studies of cyber and signal incidents involving satellite systems were used to illustrate practical implications of the identified threats.

Development of threats

With the development of space technologies and the widespread use of satellite resources in our lives, attacks on the space sector, particularly SATCOM systems and infrastructure, have increased. In the 1980s and 1990s, alongside the expansion of satellite communications and broadcasting, incidents of signal interception began to occur.

An example of this type of activity was the April 27, 1986, hijacking and jamming of the satellite signal of the commercial broadcaster HBO by American engineer John R. MacDougall (using the pseudonym "Captain Midnight"), using the Galaxy 1 satellite. In protest against rising subscription fees, he interrupted the broadcast and transmitted his own message, which was received by viewers across the eastern United States (which then constituted over half of HBO's 14.6 million subscribers) [2]. Figure 1 shows an image of the HBO signal being jammed and intercepted by an American engineer nicknamed "Captain Midnight":

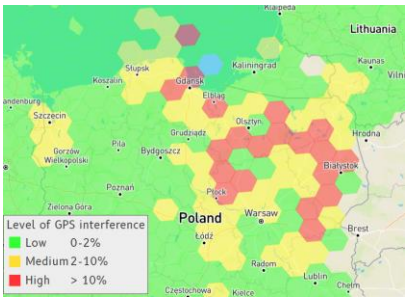
Fig. 1. *The image of a jammed HBO signal from April 27, 1986.*

Source: CBS News website: https://www.cbsnews.com/news/flashback-hacker-interrupts-hbos-film-in-1986/ (date: 04 Dec 2025).

Then, at the beginning of the 21st century, jamming activities began to emerge, although initially they were more frequently used in areas where military operations were underway. However, with the growing importance of data and services provided by space assets, satellite jamming shifted to areas where there were no theaters of operations, and the activities had a predominant impact on civilian users, daily life, and economic stability.

An example of GNSS signal jamming activity is north-eastern Poland, where interference affects the degradation of the navigation signal delivered to receivers, both for civilian and military recipients. Figure 2 shows the signal degradation percentage octanes available in open sources:

Fig. 2. *The GPS signal disruption example from February 2024.*



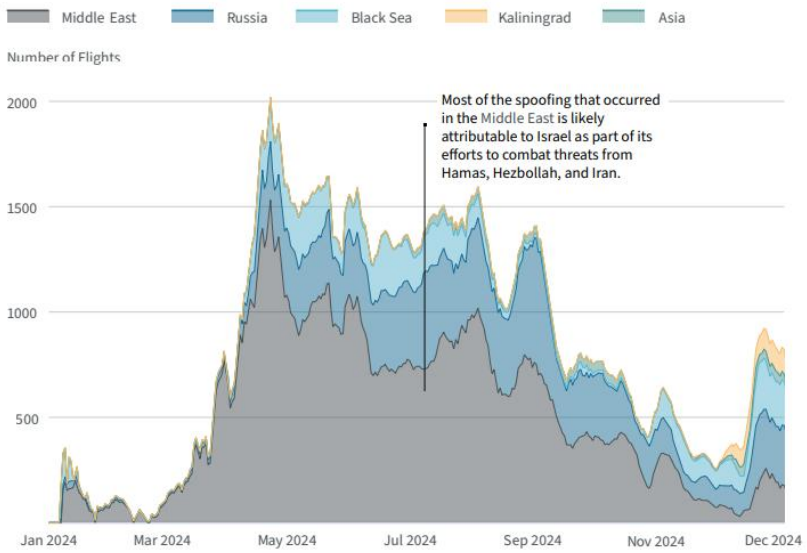
Source: https://gpsjam.org/ (date: 04 Dec 2025).

[2] CBS News website: https://www.cbsnews.com/news/flashback-hacker-interrupts-hbos-film-in-1986/ (date: 04.12.2025).

Unfortunately, both the disruption and spoofing of navigation signals[3] significantly affect widely used services in today's global economies, the trade of goods, and the protection of national interests. They also negatively impact commercial aviation by interfering with navigation systems used in transport operations.

The chart below, Figure 3, created by the US *Center for Strategic and International Studies* in 2025 as part of the *Space Threat Assessment*, shows the frequency of these activities throughout 2024, broken down by region. The greatest activity can be observed in the Middle East, where Israel is fighting its neighbours. However, these fighting impacts civilian assets.

Fig. 3. *Number of disrupted commercial flights, by world region, in 2024.*



Source: Center for Strategic and International Studies. *Space Threat Assessment* (2025).

As a result of technological development, the world's largest space powers have increasingly begun to build their capabilities in the IOE (In-orbit Eavesdropping), in order to intercept a sample of the signal transmitted to Earth and prepare for the need to decrypt the transmitted information.

An example of such activity is the Russian Luch (Olymp) satellite constellation, which primarily performs SIGINT tasks. The first satellite launched its mission in September 2014 in the geostationary orbit (GEO) zone. Over the past 11 years, it has approached and "parked" for periods ranging from several weeks to several months near more than 25 non-Russian telecommunications satellites, primarily those of *Intelsat* and *Eutelsat*.

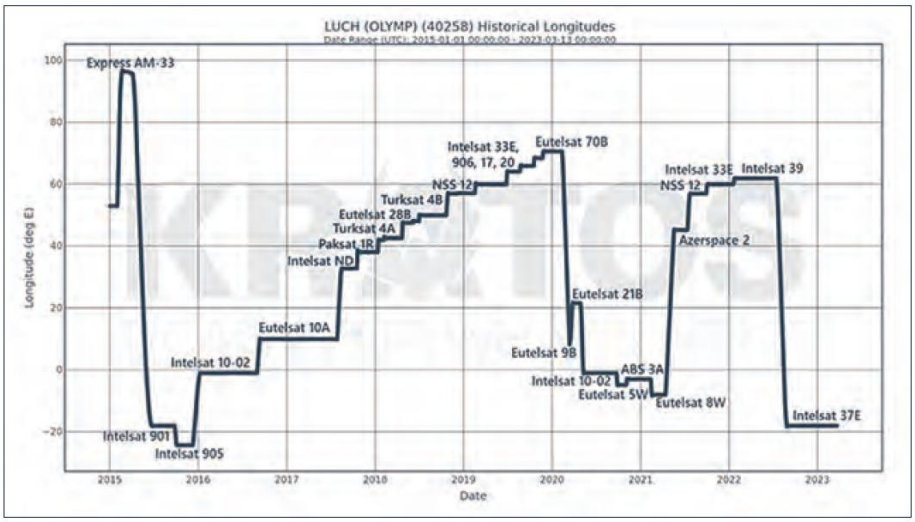
The chart below in Figure 4, prepared by the American company *Kratos Defense* and presented in the report *Global Counterspace Capabilities, An Open-Source Assessment* by the *Secure World Foundation*, shows the historical profile of Luch satellites approaching other telecommunications satellites:

[3] G. Kavallieratos, S. Katsikas, An exploratory analysis of the last frontier: A systematic literature review of cybersecurity in space, “International Journal of Critical Infrastructure Protection” 2023, vol. 43, pp. 3. Website: https://doi.org/10.1016/j.ijcip.2023.100640.

At the same time, cyber threats began to evolve, with DDoS (Distributed Denial-of-Service) and APT (Advanced Persistent Threat) attacks becoming increasingly common.

DDoS cyberattacks involve flooding a server, website, or network service with a massive number of fraudulent requests originating from multiple infected devices (such as a botnet). Their goal is to exhaust the attacked website's resources and prevent legitimate users from accessing the service. An example is the paralysis of government websites, public administration bodies, or service providers. This is a form of "distributed denial of service" attack, resulting in slowdowns, outages, or complete service shutdowns, often with the aim of extorting ransom, harming competitors, or as a form of protest.

Fig. 4. *The historical approach profile of Luch satellites to other telecommunications satellites.*



Source: Secure World Foundation. *Global Counterspace Capabilities, An Open-Source Assessment* (2025).

APTs are advanced and stealthy cyberattacks conducted by sophisticated groups (often state-sponsored) that aim to silently infiltrate networks, gain unauthorized access, and engage in sustained espionage, data theft, or sabotage, bypassing standard defences. These attacks are multi-stage, encompassing reconnaissance, intrusion (e.g., through a backdoor), maintaining a presence, and systematic intelligence gathering, lasting for months or even years.

Unfortunately, the frequency of cyberattacks on space systems is doubling annually, a trend that will likely continue in the coming years amid rising geopolitical tensions. The main threat trends from 2022 onward include the diversification of targets and the increasing complexity of attacks.

The turning point came in 2022 with the start of Russia's invasion of Ukraine, demonstrating the critical role of satellite systems in modern conflict, and cyber threats in space, targeting satellite infrastructure, are becoming as common as those affecting regular ICT infrastructure.

On February 14, 2022, the Russian invasion began with a cyberattack on the Ka-Sat civilian satellite, operated by the American company *VIASAT*, with the aim of cutting off government and military users from data transmission services.

Outside Ukraine, the issue affected approximately 9,000 French subscribers to *NordNet* broadband, which relied on a satellite internet connection provided by *VIASAT*. A third of the 40,000 subscribers of British broadband provider *BigBlu* were affected in Germany, France, Hungary, Greece, Italy, and Poland. Furthermore, German energy company *Enercon* reported an inability to remotely monitor and control access to 5,800 wind turbines. Some satellite modems became unusable and could not be repaired or updated remotely.

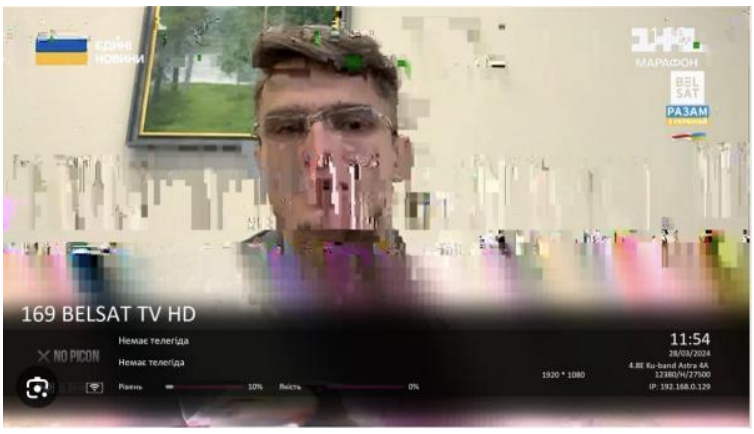
As a result of the Ukrainian government's disconnection from the geostationary satellites telecommunications resource, the Ukrainian side began using the resources of another commercial provider, *Starlink*, *SpaceX*, which relies on satellites located in low Earth orbit (LEO). In consequence, the Russian side began jamming this resource and its signal over Ukrainian territory.

Unfortunately, according to the US report *Global Counterspace Capabilities, An Open-Source Assessment*, prepared by the *Secure World Foundation* and published in April 2025, *Starlink* has become a prime target for the development of jamming systems and attacks on satellite infrastructure. The report highlights two key Russian systems: *Tobol* and *Kalinka*. The *Tobol* system was originally designed to protect Russian satellites from interference but was subsequently transformed and is now used to disrupt satellite communications and navigation systems. The *Kalinka* system, nicknamed the "*Starlink Killer*", is an electronic warfare platform capable of detecting and jamming signals to and from Starlink-type satellites in low Earth orbit[4].

Since March 2024, the Russian Federation has also been actively jamming the satellite signals of Ukrainian television channels on the *Astra4A* and *Hotbird13E* satellites, owned by European telecommunications companies *SES* and *Eutelsat*. The aim of jamming and signal interception is to confuse the public and spread hostile narratives, especially in areas near temporarily occupied territories.

Figure 5 below shows the attack of March 29, 2024, on *BELSAT* television, broadcast from the territory of Poland:

Fig. 5. *The image of the jammed and intercepted BELSAT TV signal.*

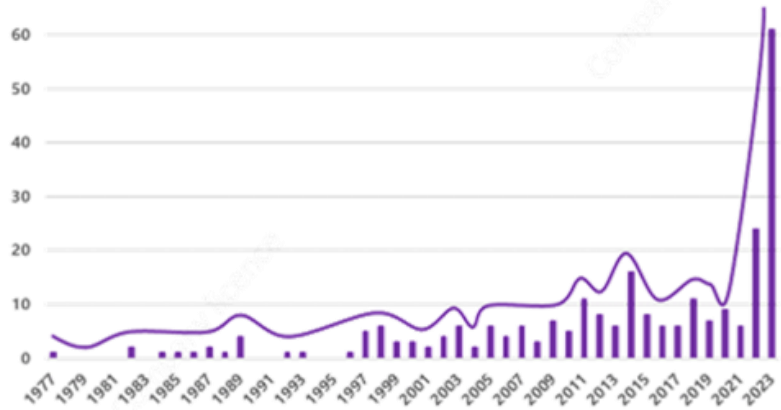


Source: https://belsat.eu/en/news/29-03-2024-ukrainian-broadcaster-reports-severe-russian-disruption-of-the-astra-satellite-which-led-to-the-jamming-of-the-belsat-tv-signal (date: 04 Dec 2025).

[4] Website: https://spacenews.com/russia-china-target-spacexs-starlink-in-escalating-space-electronic-warfare/ (date: 04.12.2025).

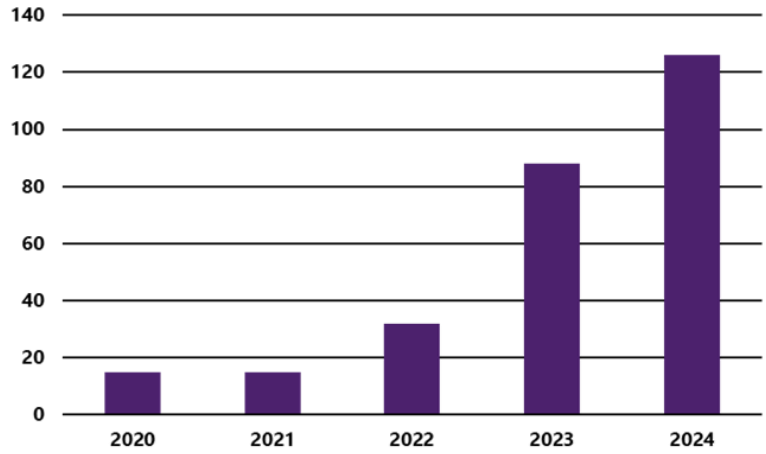
If we look at the table in Figure 6, prepared by the French company *CyberInFlight*, on the number of cyber-attacks on satellite infrastructure since the 1970s, there is a noticeable increase from a few per year in the 20th century, through a dozen or so at the beginning of the 21st century, and then an increase from 2022 to several dozen per year[5]:

Fig. 6. *The summary of the growth of cyberattacks on the space sector (1977 to 2023).*



Source: CyberInFlight. *Space Cybersecurity Market Intelligence Report* (2025). Extract available on the website: https://www.cyberinflight.com/?page_id=4004 (date: 27 Nov 2025).

Fig. 7. *The summary of the growth of cyberattacks on the space sector (2020 to 2024).*



Source: CyberInFlight. *Space Cybersecurity Market Intelligence Report* (2025). Extract available on the website: https://www.cyberinflight.com/?page_id=4004 (date: 27 Nov 2025).

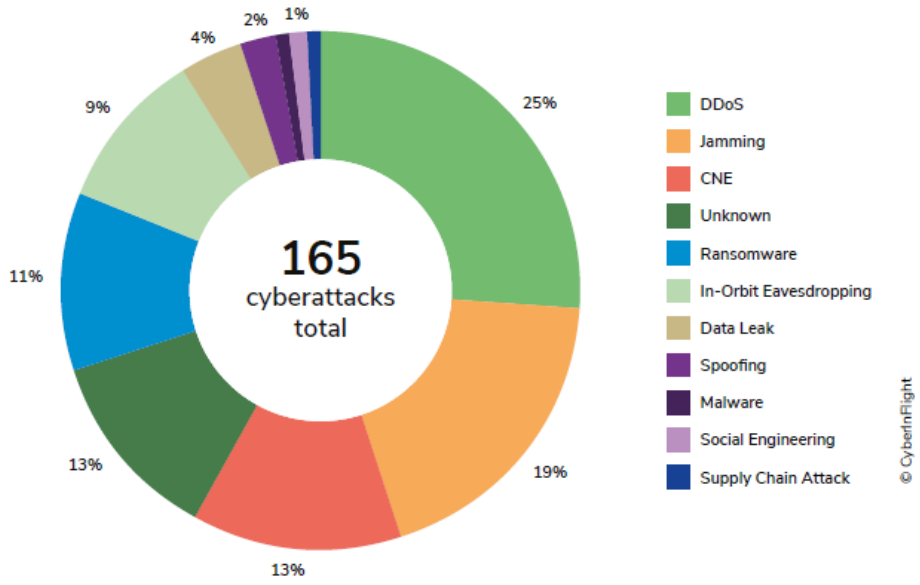
However, if we look only at the last five years, from 2020, a clear increase in cyberattacks occurred in 2022[6]. This is shown in Figure 7 also prepared by the French company *CyberInFlight* as part of the *Space Cybersecurity Market Intelligence Report*.

Looking specifically at the types of cyberattacks, the following table from Figure 8 shows the diversity of 165 different forms of attacks and threats to space

[5] CyberInFlight. Space Cybersecurity Market Intelligence Report (2025). Extract available on the website: https://www.cyberinflight.com/?page_id=4004 (date: 27.11.2025).
[6] Ibidem.

infrastructure, over a period of 2.5 years, from January 2022 to July 2024, prepared by *CyberInFlight* and presented in a study by the EUSPA (European Union Agency for the Space Programme)[7]:

Fig. 8. *The summary of types of attacks on the space sector (Jan 2022 to Jul 2024).*



Source: European Union Agency for the Space Programme (EUSPA). *GNSS and Secure SATCOM, User Technology Report* (2025).

The above list of attack types includes attempts to disrupt the functioning of computer systems or networks by attacking the systems, disrupting the link itself, or, of course, stealing transmitted data. Cyber threats target software across all segments: user, ground, and space.

The above list includes typical advanced cyber threats, APTs (*Advanced Persistent Threats*), CNEs *(Computer Network Exploitation)*, DDoS (*Distributed Denial-of-Service*) attacks, data leaks, phishing attempts, malware, ransomware, but also supply chain attacks.

Attacks also target radio links – the data transfer between Earth and orbit, as well as between space assets (orbit-to-orbit). These activities include eavesdropping, interception, in-orbit eavesdropping[8] (IOE), jamming, and spoofing.

The most common effect of these attacks is a complete loss of service, data access, or at least a reduction in its quality. In the case of eavesdropping or data interception by a third party, the user may be unaware of the data loss, and as a result, the data or information may be exploited by an opposing party.

Cause of infrastructure vulnerability

Due to technological advancements, the miniaturization of hardware devices and electronics, the market for commercial services has expanded

[7] European Union Agency for the Space Programme (EUSPA). GNSS and Secure SATCOM, User Technology Report (2025).

[8] Y. Zhang, Y. Zhao, X. Yan, W. Wang, J. Zhang, VLEO Eavesdropping Modeling and Prevention in Multi-Constellation Satellite Networks. ICC 2025 - IEEE International Conference on Communications. Website: 10.1109/ICC52391.2025.11161189.

significantly. With increasing competition and competition for consumers, cybersecurity has become a secondary issue due to the high entry costs. Commercial operators viewed this part of the business as cost-intensive and difficult to monetize[9]. The only way to generate a return on this investment was to find a limited number of customers in the government sector, through government or military contracts.

As a result of the emergence of new players in the satellite services market and the widespread development of New Space, using cloud solutions, the attack surface has expanded to include more potential systems than before.

Therefore, the division between satellite systems and the services provided, dedicated to either commercial or government clients, is very clear. Government clients define security requirements in the event of a crisis or war, which increases the costs of building secure satellite systems, while commercial clients seek the most affordable service that meets their needs.

The cost of encryption technology and the acquisition of expensive cryptographic devices is a significant barrier for many companies, a cost that will not be recouped in the market for the services provided. Furthermore, many satellite systems providing services, such as large (communications) satellite systems, and their architectures were designed 10-15 years ago and are not immune to today's cybersecurity threats and challenges. Today's systems are increasingly interconnected, forming an interconnected network, and cyberthreats are becoming increasingly sophisticated and sophisticated.

While encryption protects data transmitted to Earth, it's only part of the network architecture, designed to ensure security. A significant aspect is the transmission of information and telemetry over the uplink, known as TTC (*Telemtry, Tracking, and Command*). If the uplink is compromised by a hostile party, it means the satellite is lost. Furthermore, as in standard networks, authentication and key management are essential to ensure security and prevent hostile takeovers[10].

To combat a wide variety of threats, secure SATCOM systems must develop and implement anti-jamming and anti-spoofing technologies such as power limiters, automatic level control loops, frequency hopping, null antennas, spread spectrum techniques, and tactical modulation methods[11].

Of course, the commercial market is responding to growing threats by implementing cheaper software solutions, based on software that can be deployed on dedicated hardware to ensure physical separation.

Ensuring cybersecurity is hampered by the lack of formal, accepted standards, which leads to a variety of solutions.

Potential uses of AI

Artificial Intelligence (AI) has become one of the crucial enabling technologies shaping contemporary security environments, including cyber, information, and space-related domains. Its applications extend from operational support and decision-making processes to strategic-level planning and risk

[9] G. Kavallieratos, S. Katsikas, op.cit., 5.
[10] M. Anwar, Cybersecurity for Space Systems: Securing Satellites and Communications Against Threats. Authorea, 2025. Website: 10.22541/au.173809572.25947135/v1.
[11] European Union Agency for the Space Programme (EUSPA). GNSS and Secure SATCOM, User Technology Report (2025).

assessment[12]. In recent years, AI has transitioned from experimental use to practical deployment in both civilian and military contexts, significantly influencing the effectiveness and resilience of complex systems[13].

AI is widely applied in areas related to data processing, anomaly detection, automation, and decision support[14]. Another important application involves space-related systems and satellite operations. AI is increasingly used for satellite image analysis, object detection, and change detection in Earth observation data. Algorithms based on deep learning enable faster and more accurate interpretation of optical and radar imagery, supporting intelligence, surveillance, and reconnaissance (ISR) tasks. In addition, AI assists in space situational awareness (SSA) by predicting orbital behavior, identifying potential collisions, and monitoring anomalous satellite maneuvers[15].

In the longer term, AI may play a role in strategic-level modeling and simulation, supporting scenario analysis, risk assessment, and policy development. Such applications could assist decision-makers in evaluating the consequences of technological, organizational, or geopolitical changes, particularly in contested and multi-domain operational environments[16].

The development of new technologies, including the possibility of using artificial intelligence (AI), can help secure space infrastructure and optimize the use of resources, including transmitted data[17].

To optimize bandwidth, it is possible to use AI in operational techniques by using Beam Hopping or Beam Forming, as well as channel modeling to ensure reliable and fast communication.

Artificial intelligence and machine learning (ML) can help detect anomalies in telemetry, tracking, and control (TTC) data that may fall outside acceptable ranges, detect and classify interference, and develop methods and techniques to counteract interference. Artificial intelligence (AI) can enable more efficient, effective, and precise monitoring of satellite system health.

Furthermore, using machine learning (ML) methods, it is possible to identify data transmission disruptions and automatically respond to the system by using frequency hopping, power limiters or level control loops to protect the payload and ensure a secure link[18].

Finally, excessive reliance on AI may lead to organizational and cognitive dependency, reducing human situational awareness and decision-making skills.

---

[12] A. Carlo, N. Manti, B. Semesta, F. Casamassima, N. Boschetti, P. Breda, T. Rahloff, The importance of cybersecurity frameworks to regulate emergent AI technologies for space applications, “Journal of Space Safety Engineering” 2023, Vol. 10, Website: https://doi.org/10.1016/j.jsse.2023.08.002.

[13] OECD (2023). Artificial Intelligence, Data and Trust in the Digital Society. https://www.oecd.org/digital/artificial-intelligence/ (date: 26.11.2025).

[14] NATO (2021). NATO Artificial Intelligence Strategy. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy?selectedLocale= (date: 26.11.2025).

[15] ESA / Applications / Observing the Earth / Φsat-2, New satellite demonstrates the power of AI for Earth observation. https://www.esa.int/Applications/Observing_the_Earth/Copernicus/Sentinel1/AI_maps_icebergs_10_000_times_faster_than_humans (date: 26.11.2025).

[16] Defence24.com. AI in multi-domain operations: Capabilities and challenges. Defence24.com website: https://defence24.com/technology/ai-in-multi-domain-operations-capabilities-and-challenges (date: 5.12.2025).

[17] A. Bécue, I. Praça, J. Gama, Artificial intelligence, cyber-threats and Industry 4.0: challenges and opportunities, “Artificial Intelligence Review” 2021, Vol. 54. Website: https://doi.org/10.1007/s10462-020-09942-2.

[18] European Union Agency for the Space Programme (EUSPA). GNSS and Secure SATCOM, User Technology Report (2025).

This highlights the importance of maintaining human oversight and ensuring that AI systems function as decision-support tools rather than fully autonomous decision-makers[19].

Strategic Aspects of Cybersecurity

With the growing importance of space resources and the growing threats in space, cybersecurity in space has become increasingly important. A key aspect of utilizing space, which forms the foundation of a state's security system, is the ability to utilize space and secure access to satellite resources.

The increase in cyberattacks following the outbreak of the war in Ukraine has raised the need to consider the cybersecurity of space infrastructure not only from an industrial perspective, but also from a political and strategic perspective.

There is currently no legal framework dedicated to the cybersecurity of commercial space systems, nor are there any cybersecurity obligations or requirements for space companies providing space services on the European market.

In 2016, the *EU Network and Information Systems (NIS) Directive* was established, which specifies security and protection measures, including cybersecurity, that operators of critical infrastructure and essential services must comply with. However, this directive did not cover space infrastructure or SATCOM operators as part of the digital infrastructure. As a result, the NIS Directive did not directly apply to the space sector, even though many of these essential services rely on satellites.

As a result of existing legal loopholes and the evolving threat environment, in 2020 the European Commission proposed a new NIS2 Directive, repealing the previous directive, which defined space as an essential entity and will apply to terrestrial infrastructure operators. Furthermore, the Commission proposed the adoption of a directive on the resilience of critical entities CER (*Critical Entity Resilience*).

In March 2023, the European Union published a strategic document on the use of space for security and defense purposes (*The EU Space Strategy for Security and Defense*) [20] as a response to the threats, challenges, and risks arising from the use of space. Because space currently plays a crucial role in both security and economic interests, it is also an arena where the interests of states vying for dominance compete[21]. However, this document is not specifically dedicated to the cybersecurity of space systems.

As a result of this publication, the *EU Space ISAC* (*Information Sharing and Analysis Centre*) was established in April 2024. It facilitates the exchange of information on space security, aims to raise awareness of threats and promote best practices among private entities. The mission of the EU Space ISAC is to contribute to the security and resilience of space systems and their supply chains.

In practice, the space sector is expected to implement the NIS2 and ECI directives in practice, but also to actively participate in promoting best practices

[19] IEEE (2022). Ethically Aligned Design: A Vision for Prioritizing Human Well-being with AI. https://standards.ieee.org/industry-connections/ec/autonomous-systems/ (date: 26 Nov 2025).

[20] European External Action Service website: https://www.eeas.europa.eu/eeas/eu-space-strategy-security-and-defence-0_en (date: 26.11.2025).

[21] M. Mazur, Logistics Security in Transport and Decision-making Problems in the Management of European Satellite Resources in Space, “Rocznik Ochrona Środowiska” 2025, vol. 27, pp. 788-798. Website: https://doi.org/ 10.54740/ros.2025.063

among private entities within the EU Space ISAC. A challenge is the lack of practical cooperation between the cybersecurity and IT communities, and the space engineering, astrophysics, and satellite systems communities, to better understand cyber threats to space systems.

Conclusions and summary

The development of space technology and its widespread use for civilian and military purposes are increasing the importance of space for the functioning of modern states. Economic functioning, production, trade in goods and services, and industrial development all rely on space resources.

At the same time, the growing importance of space exploration has led to an increase in potential threats, both natural and human induced. Restricting access to or completely eliminating space resources could pose a threat to national interests.

With the growing importance of space assets and the growing threats in space, cybersecurity in space has become increasingly important. Cyberattacks, jamming, interference, spoofing, eavesdropping, and data interception have become commonplace due to the commercial nature of the services provided[22].

Asset protection, along with the use of new technologies, including artificial intelligence, is becoming a necessity to ensure security. Furthermore, the implementation of European Union directives by all EU operators will increase awareness and require the use of agreed standards.

It's understandable that, on the one hand, the digitalization and digitization of space systems make them more vulnerable to traditional cyber threats, which encourages the use of traditional cybersecurity measures. However, on the other hand, the unique environment of satellite systems renders traditional cybersecurity insufficient.

The analysis conducted confirms that cyber and signal threats to space infrastructure have become systemic in nature, affecting not only technical components but also organizational and regulatory dimensions of security. The findings indicate that the growing dependence on commercial satellite services significantly increases the attack surface, while existing governance mechanisms remain only partially adapted to space-specific risks.

The article contributes to the academic discussion by integrating technological, organizational, and strategic perspectives on space cybersecurity. At the same time, the study is subject to limitations resulting from reliance on open-source data, which may restrict access to classified operational details. This limitation points to directions for future research, including empirical studies and simulations of cyber incidents in space systems. The presented results provide a foundation for further interdisciplinary research on cybersecurity and resilience in the space domain.

Confirming the safety of satellite resources during operation requires investing in software solutions, both AI-based and hardware-based, to minimize risks. Ensuring standards and applying limited trust in the selection of subcontractors are crucial to ensuring the reliability of components and subsystems used. Collaboration in the space sector is certainly necessary, but it must be done with risk minimization in mind.

[22] R. Thummala, P. Liu, Exploring the Applications of Frequency Modulation to Secure CubeSats from Eavesdropping, “Jamming, and Interference. American Institute of Aeronautics and Astronautics” 2022. Website: https://doi. org/10.2514/6.2022-4381.

References

Anwar M., Cybersecurity for Space Systems: Securing Satellites and Communications Against Threats. Authorea, 2025.

Bécue A., Praça I., Gama J., Artificial intelligence, cyber-threats and Industry 4.0: challenges and opportunities, “Artificial Intelligence Review” 2021, Vol. 54. Website: https://doi.org/10. 1007/s10462-020-09942-2.

Carlo A., Manti N., Semesta B., Casamassima F., Boschetti N., Breda P., Rahloff T., The importance of cybersecurity frameworks to regulate emergent AI technologies for space applications, “Journal of Space Safety Engineering” 2023, Vol. 10, Website: https://doi.org/10.1016/ j.jsse.2023.08.002.

Kavallieratos G., Katsikas S., An exploratory analysis of the last frontier: A systematic literature review of cybersecurity in space. “International Journal of Critical Infrastructure Protection” 2023, vol. 43. Website: https://doi.org/_10.1016/j.ijcip. 2023.100640.

Mazur M., Logistics Security in Transport and Decision-making Problems in the Management of European Satellite Resources in Space, “Rocznik Ochrona Środowiska” 2025, vol. 27.

Thummala R., Liu P., Exploring the Applications of Frequency Modulation to Secure CubeSats from Eavesdropping, Jamming, and Interference. American Institute of Aeronautics and Astronautics 2022. Website: https://doi.org/_10.2514/6.2022-4381.

Zhang Y., Zhao Y., Yan X., Wang W., Zhang J., VLEO Eavesdropping Modeling and Prevention in Multi-Constellation Satellite Networks. ICC 2025 - IEEE International Conference on Communications 2025. Website: 10.1109/ICC52391._2025. 11161189.