ÖZYEĞİN UNIVERSITY

AI IN SPACE & CYBERSECURITY & LAW FOR AI-BASED LEO SATELLITES

Exploring the Role of Artificial Intelligence, Cybersecurity, and Legal Frameworks and Law Aspects in Securing the Future of Low Earth Orbit Satellite Systems

PREPARED BY

- Belinay Kuru
- Cengiz Onat Yapanel
- Defne Nur Yılmaz
- Defne Su Birlik
- Ece Bahar
- Gökçe Kaan Aslan
- Medine Yaren Güneysu

UNIVERSITY
Özyeğin University

PROGRAM
AI in Space : Cybersecurity and Law for AI-based Leo Satellites

PROGRAM DURATION
1st July to 14th July

MENTOR
Assistant Professor
Dr. Başak Ozan Özparlak

Foreword

Türkiye's increasing activities in space, coupled with the Cybersecurity Board's designation of space as a critical sector, necessitate collaboration among individuals from diverse disciplines. The fundamental transformation in space is driven by the growing involvement of the private sector alongside governments, and the increasing prevalence of satellite constellations like Starlink in low earth orbit (LEO), making them critical for broadband connectivity. Furthermore, artificial intelligence (AI) is becoming a significant enabler for some tasks in space. For these reasons, space has become a crucial domain for IT law also. Therefore, when launching a summer research program for high school students supported by Özyeğin University, I chose a topic that addresses the increasing importance of AI and cybersecurity in space, especially for satellite communication from a legal perspective. By creating an application process that was as unconditional as possible (the only requirement was a genuine curiosity about this field), I didn't expect such qualified young people to apply. I initially considered two students, but as applications came in, I increased the number to five, then to seven. From our first meeting at the campus, I met these brilliant high school students Belinay, Cengizhan, Ece, Defne Nur, Defne Su, Gökçe Kaan, and Medine Yaren. Their future plans vary like studying aerospace engineering, law, and electric and electronic engineering. Witnessing their achievements, their curiosity, dedication and interdisciplinary teamwork skills increased my hopes for the future! This report was written in just 12 days in a two-week programme. Any shortcomings or errors are solely my responsibility as I was their mentor. I wholeheartedly congratulate and thank them for their dedication to the program.

I would like to thank Özyeğin University for creating such a programme for high school students. Also, as you will see at the end of the report, this program was enriched not only by my mentorship but also by the voluntary support of students, researchers, entrepreneurs, and academics from various research laboratories and faculties of Özyeğin University. The doors of the laboratories were opened to these bright young people, and presentations were given from different fields. We would also like to thank everyone from outside the university who enriched the program with their presentations, especially Turkish Space Agency (TUA).

I believe we will reshape the future again and again (!) through such interdisciplinary dedicated collaborations.

"The future is in the skies!"

Başak Ozan Özparlak
Assistant Professor of IT Law
Özyeğin University Faculty of Law

Table of Contents

AI in Space: Cybersecurity and Law for AI-Based LEO Satellites

Project Report: AI In Space Summer Research Programme for High School Students, Ozyegin University, Istanbul, July 2026

Authors (in alphabetical order): Belinay Kuru · Cengiz Onat Yapanel · Defne Nur Yılmaz · Defne Su Birlik · Ece Bahar · Gökçe Kaan Aslan · Medine Yaren Güneysu

"Space assets, including both ground systems and satellites, are fundamental, underlying components of most critical infrastructure" [1]

Gregory Falco

"As Arthur C. Clarke observed in 1970, satellite communication promised to do for a connected world what the telegraph had done for a unified nation a century earlier; the hope was only that the transition would be less turbulent this time." [2]

1. Purpose of This Report

Space is now a vital domain that underpins modern society thanks to the explosive growth of commercial satellite constellations in low earth orbit (LEO). Satellite networks are essential today for many services, including telecommunications, navigation, financial transactions, emergency response, and national security. But as these systems become more connected with terrestrial digital infrastructure and involve use of artificial intelligence (AI), they become more vulnerable to cyber threats. Recent events, like Viasat attack, have shown that even if there is no AI integration, attacks on a single vulnerability of the ground segment can lead to disruption of satellite services in several countries and sectors. On the other hand, AI plays a dual role regarding cybersecurity; it both increases vulnerability and at the same time, it is a useful tool for mitigating cyber threats for space assets like satellites.

This report firstly focuses on the 2022 Viasat KA-SAT cyberattack, as one of the first major cyber incidents to demonstrate the strategic consequences of compromising commercial satellite infrastructure during an armed conflict. But while attacks typically focus on the spacecraft, this operation exploited a vulnerability in the ground segment, leading to widespread disruption for both military and civilian users across Europe. The incident also raised important questions about international law, protecting dual-use infrastructure, and the future of space cybersecurity.

This report aims to analyze the Viasat KA-SAT cyberattack from a technical, legal and strategic perspective. By combining these perspectives it also aims to demonstrate how cybersecurity has become a crucial part of modern space security even without AI integration, and why strengthening the resilience of satellite systems will become increasingly essential in the New

Space era of massive commercialization in LEO and increasing use of AI in satellite communication.

2. LEO, MEO, and GEO Satellite Systems

Satellite communication systems mainly operate in Geostationary Earth Orbit (GEO), Middle Earth Orbit (MEO) and Low Earth Orbit (LEO). These orbits differ in altitude, coverage, latency, and operational characteristics, making each suitable for different applications. Understanding these differences is important not only for satellite communications but also for evaluating cybersecurity risks, as demonstrated by the 2022 Viasat KA-SAT cyberattack.[3]

Geostationary Earth Orbit (GEO) is located 35,786 km above the Earth's equator. Satellites in GEO orbit at the same speed as the Earth's rotation, allowing them to remain fixed over one location. This enables continuous coverage of large geographic areas by using only a few satellites. As a result, GEO systems are widely used for television broadcasting, weather monitoring, government communications, and internet services.[4] The KA-SAT satellite targeted in the 2022 cyberattack is also a GEO satellite providing broadband connectivity across Europe, North Africa, and parts of the Middle East.[5]

Although the incident involved a satellite in orbit, the satellite itself was never attacked. Instead, the attackers exploited a vulnerability in the ground segment, gained access to the network management system, and deployed the AcidRain malware to thousands of satellite modems. While the satellite continued operating normally, users across several European countries lost connectivity because the supporting ground infrastructure had been compromised. The incident demonstrated that satellite cybersecurity depends on securing the entire communication system, not only the satellite itself.[5,6]

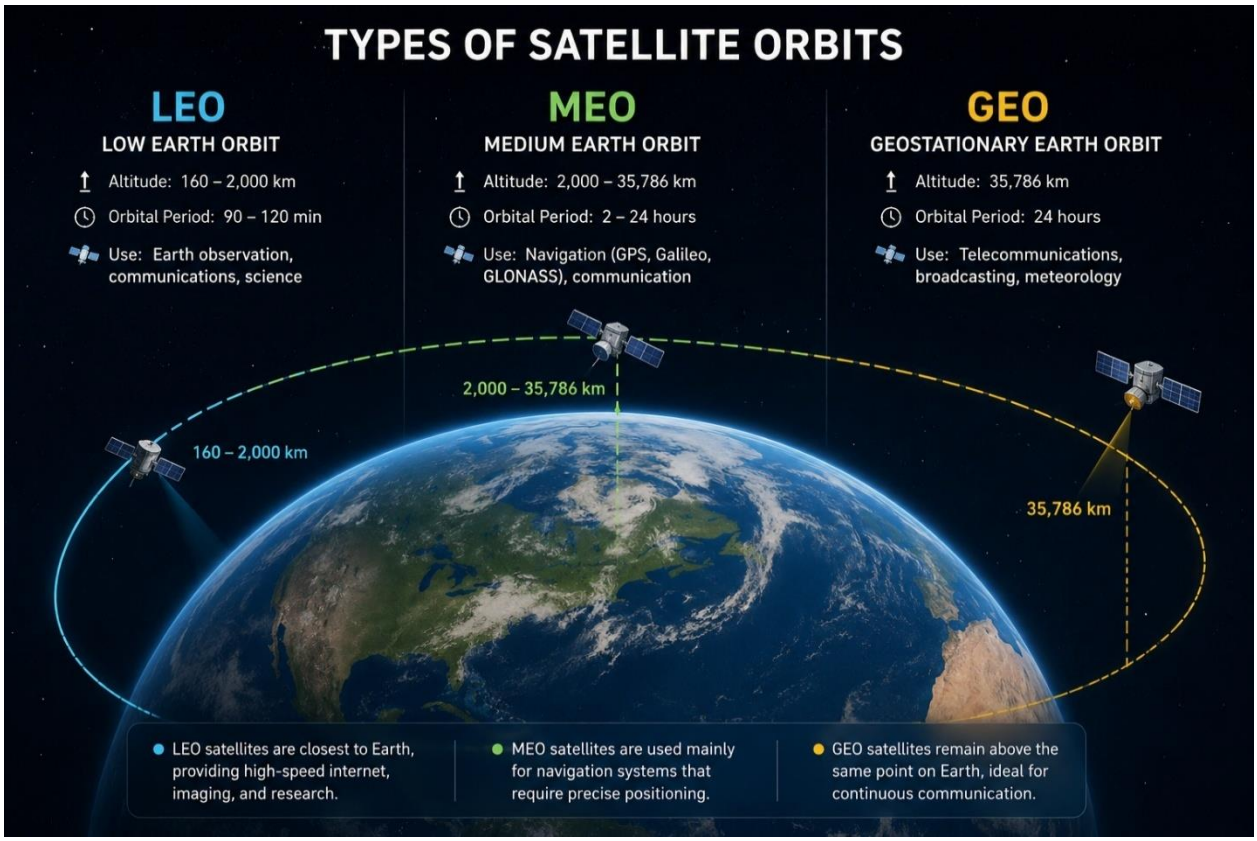


Figure 1. Orbital Classifications of Commercial Satellite Systems. Generated by ChatGPT.

Unlike GEO satellites, LEO satellites, like SpaceX's Starlink constellation satellites, operate between approximately 160 and 2,000 km above the Earth's surface and complete one orbit in about 90 to 120 minutes. Their lower altitude significantly reduces communication latency, making them well suited for broadband internet, emergency communications, remote healthcare, and future 5G and 6G services. However, because each LEO satellite covers a relatively small area, continuous global coverage requires large constellations consisting of hundreds or thousands of interconnected satellites.[7]

Beyond their technical advantages, LEO constellations have become strategically important because they provide resilient communication during natural disasters, military conflicts, and in regions where terrestrial infrastructure is unavailable or has been damaged. Their distributed architecture also reduces dependence on a small number of satellites, improving network resilience and supporting critical services for governments, businesses, and emergency responders.[7,8]

The rapid growth of LEO constellations is expanding both the capabilities and the cyber risks of modern space infrastructure. As more satellites, ground stations, and communication links become interconnected, the potential attack surface also grows. ENISA emphasizes that effective satellite cybersecurity requires protecting the entire ecosystem, including ground stations, user terminals, network management systems, and communication links.[7] The KA-SAT cyberattack remains a landmark example of this principle, demonstrating that vulnerabilities in the ground segment can disrupt satellite services on a continental scale, regardless of whether the system operates in GEO, MEO or LEO.[9]

3. The Growing Importance of Cybersecurity in Space

Modern space infrastructure has expanded far beyond the geostationary communications satellites of the twentieth century. Today's space systems include not only traditional GEO broadcast and broadband satellites like KA-SAT, but also sprawling LEO constellations and, as projects like Starmind illustrate, orbital platforms that may in the near future function as AI computing infrastructure in their own right.[10] This expansion means space systems now underpin sectors far outside aerospace itself: banking relies on satellite timing signals, agriculture depends on satellite-based monitoring, emergency responders use satellite links when terrestrial networks fail, and militaries treat satellite connectivity as core operational infrastructure.[11,12]

As these systems multiply and interconnect, so does their exposure to cyber risks. A single intrusion into ground infrastructure, the network management systems, gateway stations, and control links that keep satellites operational, can cause disruption on a continental scale, regardless of whether the underlying satellite operates in GEO, MEO or LEO. The February 2022 Viasat KA-SAT cyberattack remains the clearest illustration of this dynamic: attackers never touched the satellite itself, yet the consequences reached across Europe within hours.[11,12]

Moreover, the emergence of AI-supported satellite systems adds a further dimension. As onboard artificial intelligence takes on a larger share of satellite operations (from autonomous navigation/routing, collision avoidance to, in proposals like Starmind, large-scale data processing), the attack surface extends beyond communications disruption to include the integrity of AI-driven decision-making itself.[10] The incident showed that protecting satellites alone is not enough; cybersecurity has become a core element of space security, and increasingly, of the legal and regulatory frameworks now being built around both LEO constellations and AI in orbit.[11,12]

4. Background: Viasat and the KA-SAT Network

Viasat is a satellite communications company founded in 1986 and headquartered in Carlsbad, California. Through its fleet of geostationary satellites and ground infrastructure, it provides broadband, in-flight, maritime, enterprise, and government connectivity in more than seventy countries.[13]

KA-SAT itself is a high-throughput satellite using Ka-band frequencies and a multi-spot-beam architecture to provide broadband across Europe, North Africa, and parts of the Middle East. Like any satellite communication system, it comprises a space segment (the satellite in orbit) and a ground segment: gateway stations, network management systems, and user terminals that keep the system operational.[14]

Figure 2. A Ka-band satellite gateway antenna used in Viasat's government/military SATCOM systems. Source: Viasat.[16]

The network's ownership reflects the layered, multi-operator structure typical of commercial satellite infrastructure. KA-SAT began as a joint venture between Viasat and Eutelsat. In October 2021, Viasat acquired the remaining stake and became the full owner of the satellite and its associated ground infrastructure. However, Eutelsat's subsidiary Skylogic continued to operate parts of the ground segment on Viasat's behalf.[15]

This structure gave KA-SAT a dual-use character, as the same network carried residential, enterprise, government, and military traffic. As a result, an intrusion into its management plane affected far more than its intended target.[5]

5. What Happened: Anatomy of the Viasat Attack

Reconnaissance and initial access attempts against KA-SAT's ground network began as early as 23 February 2022, a day before the destructive payload was triggered roughly one hour ahead of Russia's invasion of Ukraine.[17] The attackers gained access through a misconfigured VPN appliance connected to the trusted management network. Later reports identified it as a Fortinet FortiGate device. From there, they moved laterally into the network segment used to manage residential broadband modems.[5,18] Rather than attacking the satellite itself, they pushed destructive commands to tens of thousands of modems at once. SentinelLabs' analysis of the malware, named AcidRain, found that it targeted embedded Linux-based modems and routers by deleting files and corrupting flash memory. As a result, affected devices could no longer boot and had to be either reflashed or replaced.[6,19] Investigators also found that AcidRain shared code with VPNFilter, a 2018 tool previously claimed to be linked to Russian military intelligence.[6,19]

The disruption reached far beyond Ukraine: while several thousand Ukrainian customers lost connectivity, tens of thousands of additional subscribers across Germany, France, Poland, Italy, Hungary, and Greece were also affected.[20] Viasat and NSA officials later concluded that the campaign involved two related incidents: the initial intrusion and a second wave in which compromised modems were used to launch denial-of-service traffic against Viasat's own systems. This complicated efforts to restore the network.[17]

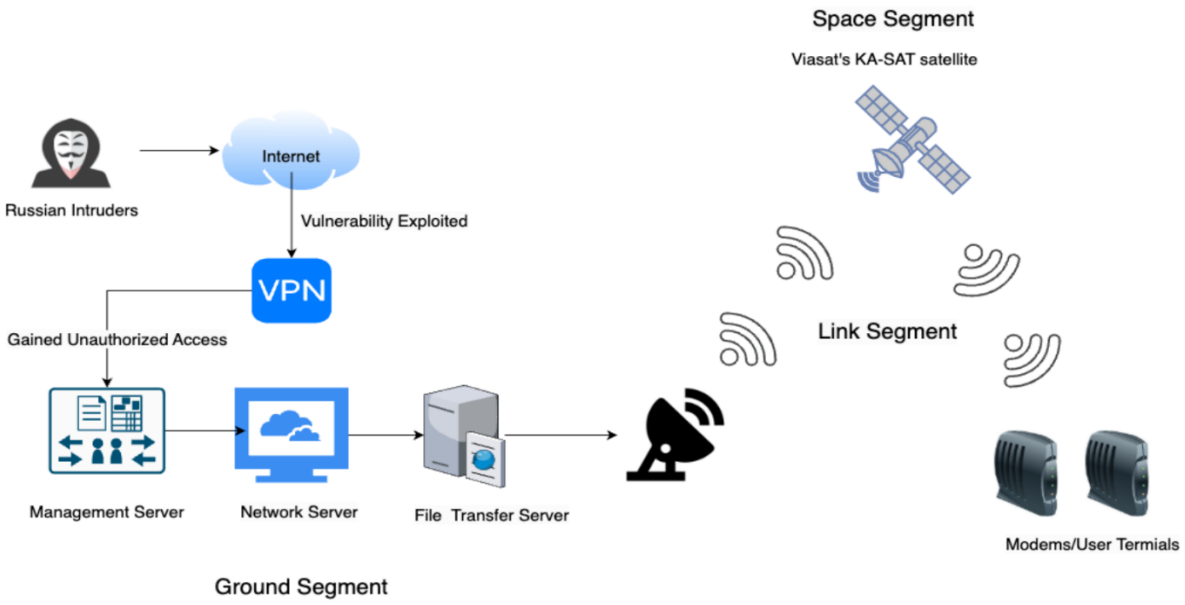


Figure 3. Viasat's Network Infrastructure Diagram. Source: Kazi, Kazi, and Bhosale 2025, 62 [21]

6. Operational, Legal, and Strategic Implications of the Attack

One of the most significant examples of cross-border collateral damage involved approximately 5,800 Enercon wind turbines in Germany, which temporarily lost remote monitoring capability after their satellite-linked control modems went offline. The incident showed how a cyberattack targeting military communications in one country could also disrupt civilian energy infrastructure in another.[20] The attack soon attracted international attention not only because of its operational consequences, but also because of the legal and political questions it raised.

On 10 May 2022, the European Union (EU), the United States (US), the United Kingdom (UK), and allied governments formally attributed the attack to Russia, describing it as a deliberate act carried out roughly an hour before the invasion to disrupt Ukrainian military and government communications.[22,23,24] This sequence reflects a broader pattern in how states handle cyber incidents. Technical attribution often comes first, followed by corporate confirmation and, only later, formal state attribution. Because technical evidence alone rarely provides complete certainty, governments increasingly combine it with intelligence and diplomatic assessments before assigning responsibility.[25] Russia did not directly address the allegations and declined to participate in any investigation. Consistent with its broader position on cyber incidents, Moscow has repeatedly denied conducting offensive cyber operations of this kind.[26] The attribution nonetheless triggered a fresh round of sanctions against Russia days later.[17]

Beyond the question of attribution, the incident also renewed discussions on how international law applies to commercial satellite infrastructure used for both civilian and military purposes during armed conflict. Because KA-SAT served both civilian and military users through the same network, the attack raised important questions about how international law applies to dual-use infrastructure during armed conflict. As a result, the incident became an important case for examining how existing international legal frameworks apply to cyber operations affecting commercial space infrastructure. These legal questions become particularly complex when the same infrastructure serves both civilian and military functions.[27]

Under Article 52(2) of Additional Protocol I to the Geneva Conventions, military operations must be confined to objects that make an effective contribution to military action and whose neutralization offers a definite military advantage. The Principle of Proportionality, set out separately in Article 51(5)(b) of the same Protocol, prohibits attacks expected to cause civilian harm that is excessive relative to the military advantage anticipated.[28] The KA-SAT operation can be assessed under both provisions: its primary objective was plausibly military, but its indiscriminate, borderless effects on European civilian users raise a genuine proportionality question. Because the malware could not confine its effects to military-linked terminals, the attack also affected civilian users across Europe. This has led legal scholars associated with the Tallinn Manual 2.0 project to support a more effects-based interpretation of what constitutes an "attack" under international law. The International Committee of the Red Cross similarly argues that permanently disabling infrastructure during an armed conflict may amount to a kinetic-equivalent attack, even without physical destruction.[25,27]

The legal and operational challenges exposed by the KA-SAT incident have also influenced policy developments within the digital legislative framework in the EU. Space infrastructure is now treated as critical infrastructure under the EU's NIS2 Directive, and ESA has expanded cybersecurity programs.[11,12,29] Building on this, the European Commission proposed the EU Space Act in June 2025, aiming to harmonize the fragmented, country-by-country regulatory landscape that currently governs European space activities. The Space Act proposal rests on three pillars: safety (rules for tracking space objects and mitigating debris), resilience (cybersecurity requirements tailored specifically to space operators), and environmental sustainability. Unlike the NIS2 Directive, which covers ground-segment operators and electronic communications providers but does not extend to Union-owned space assets or space-specific risks, the EU Space Act is designed to close that gap by applying cybersecurity obligations directly to satellite operators and other space-service providers operating in or serving the Union.[30] If adopted, the regulation is expected to apply from January 2030, a timeline that itself signals how recently space cybersecurity has been treated as a distinct regulatory priority rather than an extension of general critical-infrastructure rules. 2030 is also the planned deployment time for 6G wireless communication with the aims of terrestrial and non-terrestrial networks.

7. Project Starmind

Project Starmind is a planned space-based AI megaconstellation consisting of up to one million satellites designed to operate as a distributed orbital data center. According to SpaceX's proposal, the project aims to relocate a significant portion of AI processing from terrestrial data centers to Low Earth Orbit (LEO), taking advantage of continuous solar energy and the natural cooling environment of space to support large-scale AI computation.[10,31]

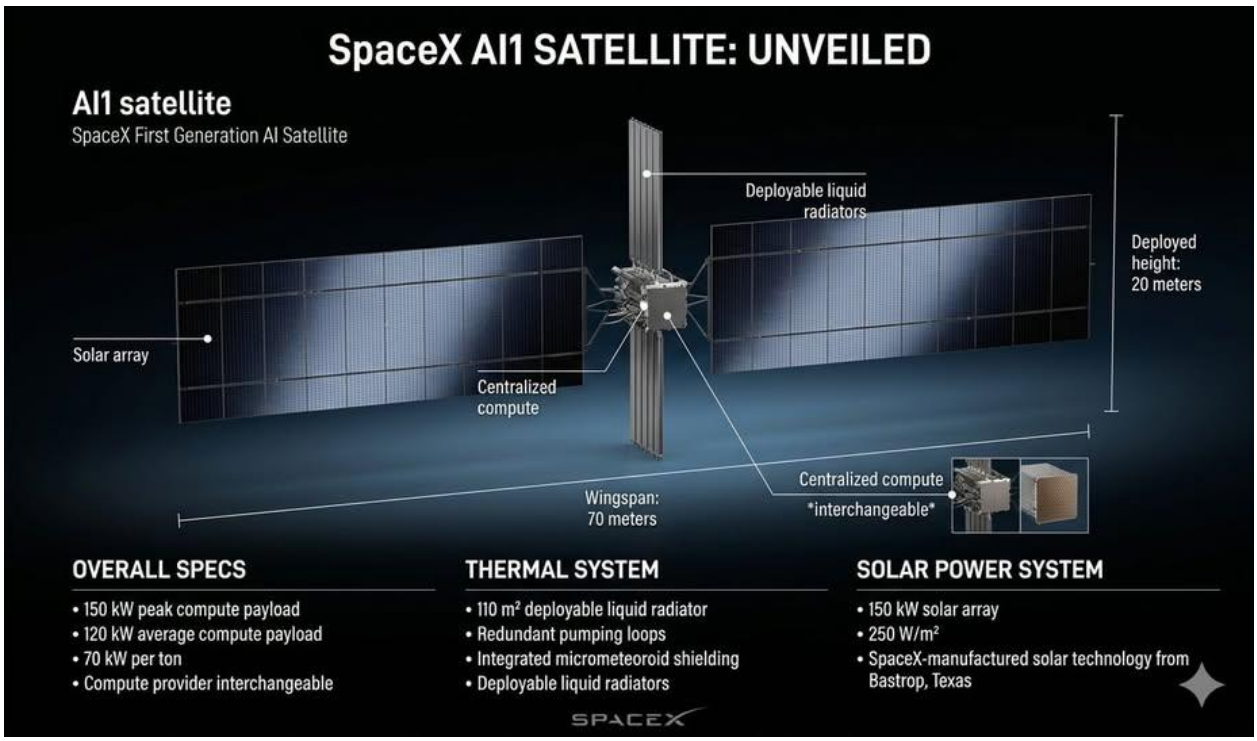


Figure 4. Illustrative rendering of SpaceX's AI1 satellite. Source: TechiExpert.[32]

The Starmind infrastructure is expected to be engineered, manufactured, and launched primarily by SpaceX. Its core technical architecture is planned to rely on xAI (Elon Musk's artificial intelligence company), which is being integrated into the broader SpaceX ecosystem under the SpaceXAI initiative.[10] Hardware engineering, testing, manufacturing, and launch operations are expected to take place across SpaceX's major aerospace facilities in the US.

The project first appeared in public records following a preliminary FCC application submitted on January 30, 2026. On June 8, 2026, SpaceX publicly introduced the first AI1 satellite hardware nodes, while the initial prototype launch campaign is currently planned to begin in early 2027.[30,33] Since the project is still under development, many of its technical capabilities remain conceptual and will require further testing and validation.

7.1 AI In Satellites

AI is a key component of Project Starmind and is expected to support the operation of its large satellite constellation. Unlike conventional satellite systems that depend heavily on ground operators, Starmind will be designed to use onboard AI to perform many routine operations

autonomously. By processing data directly on the satellite through edge AI, the system can reduce the amount of information sent back to Earth, lower communication delays, and improve operational efficiency.

However, even before the Starmind project, today AI is being used in satellite operations. Besides running Large Language Model (LLM) inference, onboard AI can assist with navigation, orbit and attitude control, collision avoidance, communication routing, bandwidth management, health monitoring, predictive maintenance, power distribution, thermal control, fault detection, and resource management. AI can also help satellites coordinate with one another, making the constellation more efficient and resilient. Although these capabilities could improve the performance of the system, they also introduce new challenges related to cybersecurity, reliability, and the verification of autonomous decision-making.

Project Starmind has the potential to change how AI infrastructure and satellite networks operate, but it also raises several technical, environmental, and security concerns. Deploying up to one million satellites would greatly increase the number of objects in Low Earth Orbit, creating additional challenges for traffic management, collision avoidance, and space debris mitigation.

Another concern is the size of the satellites' solar arrays. Large reflective surfaces may interfere with ground-based astronomical observations and contribute to light pollution, an issue that has already attracted attention from the scientific community.

Environmental impacts should also be considered. As satellites reach the end of their operational lives and re-enter Earth's atmosphere, the materials released during atmospheric burn-up may contribute to pollution in the upper atmosphere. As the constellation grows, managing these long-term environmental effects will become increasingly important.

The extensive use of onboard AI also expands the cybersecurity threat surface. AI models, satellite software, communication links, and onboard control systems could become targets for cyberattacks. Ensuring the security and resilience of these systems will therefore be essential for the safe and reliable operation of future orbital AI infrastructure.

7.2 How It Will Be Produced and Engineered

Project Starmind relies on large-scale aerospace manufacturing and SpaceX's vertically integrated production model. Rather than developing an entirely new industrial infrastructure, the project aims to utilize existing SpaceX manufacturing facilities together with the reusable Starship launch system.

Because Starship is designed to maximize orbital payload capacity while significantly reducing launch costs, SpaceX proposes to mass-produce computational satellites and deploy them in large orbital clusters. According to the company's long-term vision, the constellation could eventually provide up to one terawatt of orbital AI computing capacity annually. Musk has linked this figure to a related SpaceX/Tesla/xAI initiative called Terafab, a chip-manufacturing venture announced in March 2026 that targets one terawatt of AI compute capacity per year,

with roughly 80 percent of that output intended for deployment via orbital satellites like Starmind.[34,35,36] This figure therefore describes Terafab's chip-production target rather than a confirmed specification of the Starmind constellation on its own. If successfully implemented, this approach could reduce some of the energy, cooling, land-use, and infrastructure constraints associated with conventional terrestrial AI data centers.

Instead of continuously transmitting raw sensor data or user requests to Earth, the satellites are expected to perform localized AI computation onboard. Large Language Model (LLM) inference and edge AI processing could be executed directly on the satellites, allowing only processed outputs to be transmitted back to Earth through high-speed communication networks. This distributed computing architecture aims to reduce communication latency and optimize bandwidth usage while improving overall operational efficiency.[31]

The proposed infrastructure is expected to support global technology companies, defense organizations, cloud service providers, research institutions, and other users requiring large-scale AI processing, continuous data analysis, and high-performance digital infrastructure. However, the commercial viability and operational scalability of this concept remain dependent on future technological development and successful deployment.

7.3 Powering Orbital Compute: The Electrical Engineering Challenge

Beyond its AI architecture, Starmind's AI1 prototype illustrates the electrical engineering problem at the heart of orbital computing: generating and dissipating enormous amounts of power without access to a terrestrial grid or atmosphere. According to SpaceX's June 2026 specifications, each AI1 satellite is built around a 70-meter deployable solar array rated at roughly 250 watts per square meter, targeting approximately 150 kW of peak electrical output and 120 kW sustained.[37,38] Because a vacuum offers no air or water to carry away waste heat, all of that power must ultimately be radiated as infrared energy; AI1's design includes a 110-square-meter deployable liquid radiator, oriented edge-on to the sun and radiating from both faces, with redundant pumping loops and micrometeoroid shielding.

This radiator design is also where the electrical engineering claims become most contested. SpaceX's target of roughly 70 kW of compute per metric ton would require an areal heat-rejection rate several times higher than any thermal control system previously flown, including the International Space Station's own system, which rejects approximately 70 kW across 422 square meters, an order of magnitude more radiator area for a comparable heat load.[37,38] Independent technical analysis published shortly after the announcement argued that reaching SpaceX's stated power-to-mass target would require every design variable, solar efficiency, radiator performance, and structural mass, to land simultaneously at its most optimistic plausible value, with no realistic margin for error.[39]

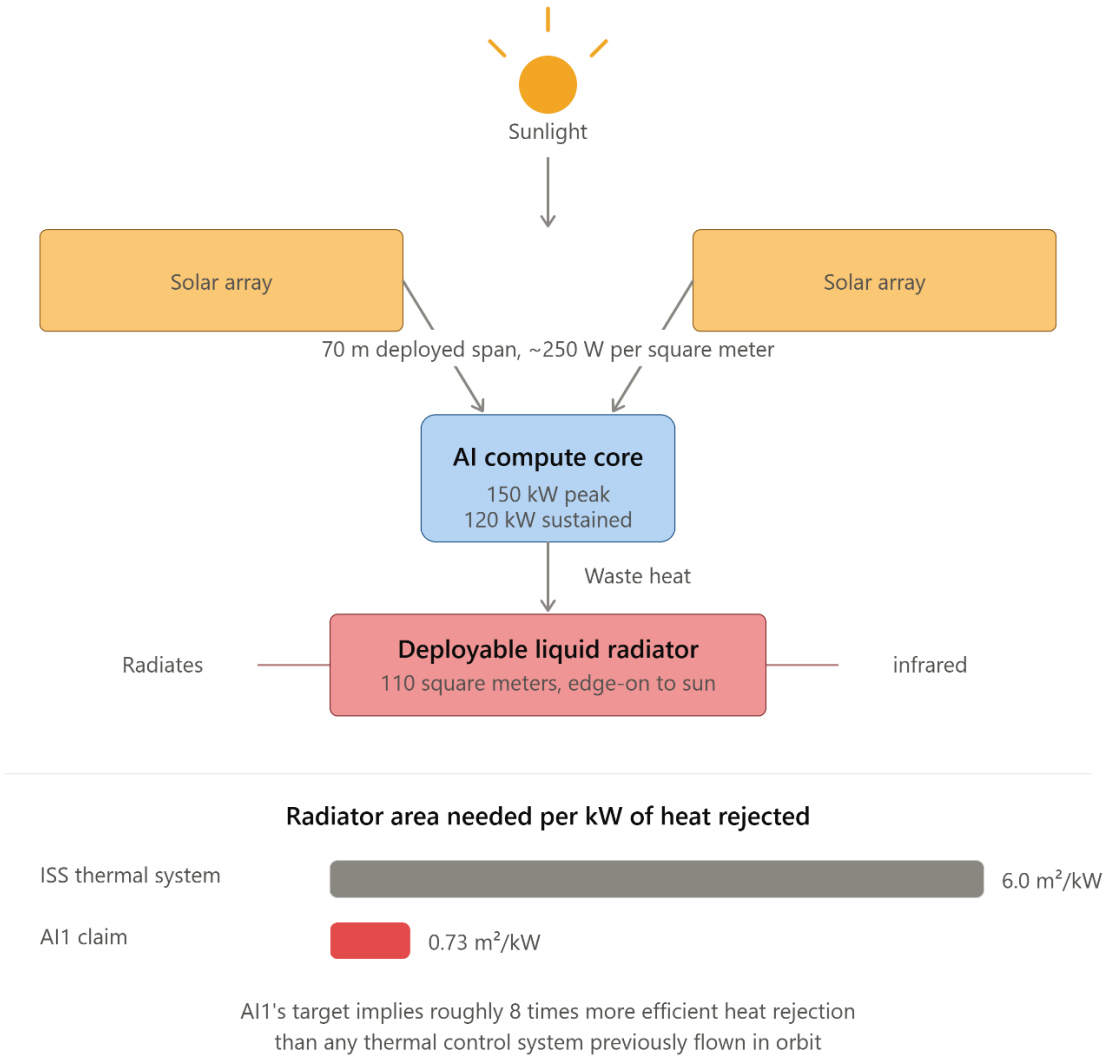


Figure 5. Power thermal system diagram for AI1 Satellite. Generated by Claude.

8. Why the Case Matters: Academic Perspectives on Cybersecurity for AI in Space

Integrating AI, especially rapidly developing agentic AI in every sector, increases cyber vulnerabilities since it renders human oversight increasingly difficult. Academic analysis of the incident has emphasized that the KA-SAT attack succeeded not by defeating some space-specific defense but by exploiting a terrestrial vulnerability: a poorly secured VPN. Boschetti, Gordon, and Falco argue that this reflects the main risk of dual-use space infrastructure.[9] Systems serving both civilian and military users become attractive targets, while weaknesses in ground-based IT security can affect space-dependent services worldwide.

These same dual-use vulnerabilities apply with even greater force to AI-supported satellite services. Where the KA-SAT attack disrupted communications by compromising a ground management system, an equivalent intrusion into a satellite that also makes autonomous decisions, whether navigating, allocating bandwidth, or, in proposals like Starmind, performing AI computation itself, raises the stakes considerably. The concern is no longer only that a

service goes offline, but that a compromised system could act on false or manipulated inputs while continuing to appear functional, a failure mode with little precedent in traditional satellite communications.[40] This is precisely why the lessons of the Viasat case are being carried forward into the design of next-generation systems: cybersecurity that once focused on protecting connectivity now has to account for protecting the integrity of onboard decision-making as well.

Later studies have highlighted the broader strategic implications of the attack. NATO's Secretary General has since stated that, in principle, a cyberattack could trigger the Alliance's Article 5 collective-defense clause.[41] A separate 2024 study identified 124 cyber operations targeting the space sector during the Russia–Ukraine war. This suggests that the KA-SAT incident was not an isolated case, but part of a broader pattern.[42] Reporting from late 2025 confirms this: a Chinese state-sponsored group that had already breached major U.S. telecom providers went on to target the satellite communications sector, with Viasat again among the companies affected.[43] The growing importance of satellite cybersecurity is also reflected in Türkiye's space initiatives. In 2026, Türksat announced that production of the Türksat 7A communication satellite would begin, representing another step toward strengthening Türkiye's independent satellite capabilities. As national satellite programs expand, integrating cybersecurity into both satellite and ground infrastructure will become increasingly important.[44]

9. Cybersecurity Lessons Learned

The Viasat incident highlights five operational lessons for critical infrastructure operators. First, management networks should be separated from operational systems. Second, privileged remote access requires strong authentication and continuous monitoring. Third, operators should maintain tested recovery plans and spare equipment for destructive attacks. Fourth, satellite services should be designed with resilience in mind, not only normal availability. Finally, cybersecurity strategies must protect the ground segment as carefully as the space segment.[5,45]

10. The Growing Importance of Space and Cybersecurity in Türkiye

The lessons learned from the Viasat KA-SAT cyberattack are increasingly relevant as Türkiye continues to expand its national satellite capabilities and next-generation communication infrastructure. The Turkish Space Agency (TUA), established in 2018, is the national authority responsible for coordinating Türkiye's national space policy, supporting the development of space technologies, and promoting international cooperation in space activities.[46] Through the implementation of the National Space Program and collaboration with domestic and international stakeholders, TUA plays a central role in strengthening the country's space ecosystem. The growing importance of Türkiye's space sector will also be reflected by the 77th International Astronautical Congress (IAC 2026), which will be held in Antalya, Türkiye, on 5–9 October 2026, marking the first time the congress is hosted in Türkiye.[47]

Türkiye is also investing in future communication technologies beyond satellite development. Following the national frequency auction in October 2025, Turkcell officially launched its commercial 5G network infrastructure across Türkiye on April 1, 2026.[48] In parallel with this

deployment, the operator has advanced a next-generation research center focusing on the integration of terrestrial and non-terrestrial communication to accelerate 6G development in Türkiye, with a strategic emphasis on autonomous networks, AI, and digital twins. These innovations are expected to integrate terrestrial and non-terrestrial networks more closely, making secure communication architectures increasingly important.[49]

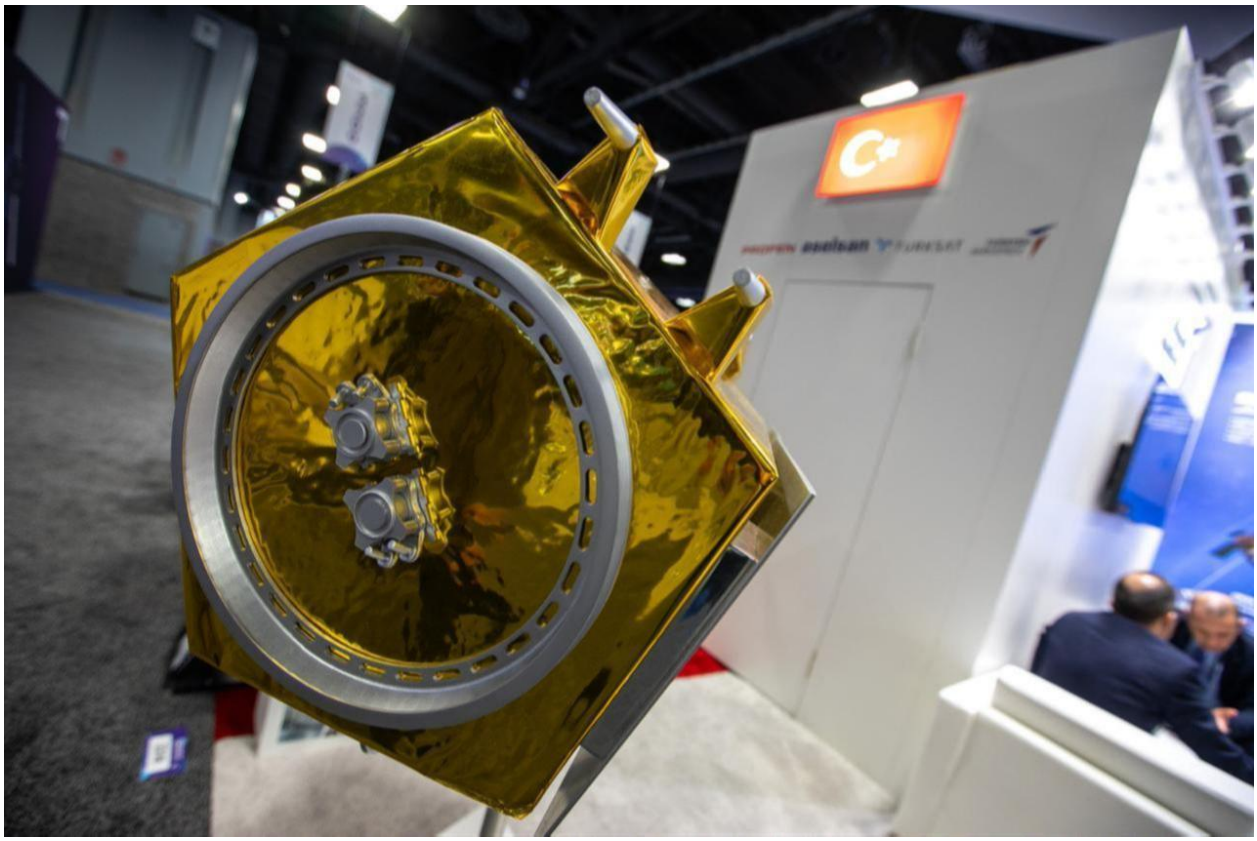


Figure 6. Representatives of Türksat, TAI, Aselsan, PROFEN, and Fergani Space at Satellite 2025, Washington, D.C. Photo: Anadolu Agency (AA).[50]

Recently, on May 5th, 2026, the Turkish Cyber Security Board categorized space as one of the 15 critical infrastructures under Act No.7545. Also, on June 13th, the Turkish AI Action Plan was announced, which also highlights the inevitable intersection of AI and cybersecurity.[51]

Together, these developments demonstrate that cybersecurity is becoming a strategic component of Türkiye's digital and space policies. As satellite systems, AI-driven network management, and future AI-enabled 6G infrastructures become more interconnected, protecting both space-based and ground-based assets will be essential for ensuring resilient and secure communications. The Viasat KA-SAT cyberattack provides an important reminder that vulnerabilities in ground infrastructure can have consequences extending far beyond a single satellite system.[5,12]

11. Conclusion

The Viasat KA-SAT cyberattack demonstrated that the security of modern space systems depends as much on ground infrastructure as on the satellites themselves. By exploiting a

vulnerability in the ground segment, the attackers disrupted military communications, civilian broadband services, and critical infrastructure across Europe, highlighting the interconnected nature of today's space ecosystem.

Beyond its immediate operational impact, the incident raised important legal and strategic questions related to dual-use satellite infrastructure, state responsibility, and the application of international humanitarian law to cyber operations. As commercial satellite networks continue to expand, and AI is becoming a major enabler for satellite operations, cybersecurity must be recognized as a fundamental component of space security. The Viasat case therefore represents not only a landmark cyberattack, but also a defining example of why technical resilience, legal frameworks, and international cooperation must evolve together to protect future space infrastructure. Today with the fast developing AI capabilities in satellites, these lessons are much more crucial than ever.

Acknowledgements

This work was supported by the Özyeğin University Summer Research Programme for High School Students, 2026, and was carried out under the mentorship of Assistant Prof. Başak Ozan Özparlak. The authors and the mentor would like to thank Özyeğin University, all academicians, researchers, PhD and undergraduate students of Özyeğin University from different faculties, administrative staff of Özyeğin University who generously shared their time, expertise, and work at their labs throughout this Summer Research Programme. In particular, the authors are grateful to those who delivered presentations, hosted laboratory visits, and offered guidance during the programme, including Turkish Spave Agency (TUA). Their openness and enthusiasm made this work possible.

Notes

1. Gregory Falco, "Cybersecurity Principles for Space Systems," Journal of Aerospace Information Systems 16, no. 2 (2019): 61–70.
2. Arthur C. Clarke, First on the Moon (New York: Harcourt Brace Jovanovich, 1970).
3. European Space Agency, ESA Report on the Space Economy 2025 (Paris: European Space Agency, 2025).
4. European Space Agency, Telecommunication Systems and Techniques, accessed July 2026.
5. Viasat, "KA-SAT Network Cyber Attack Overview," Viasat News, March 30, 2022.
6. Juan Andres Guerrero-Saade and Max van Amerongen, "AcidRain | A Modem Wiper Rains Down on Europe," SentinelOne (SentinelLabs), March 31, 2022.
7. European Union Agency for Cybersecurity (ENISA), Low Earth Orbit (LEO) SATCOM Cybersecurity Assessment, February 2024.
8. Türkiye Uzay Ajansı (Turkish Space Agency, TUA), Karasal Olmayan Şebekeler (NTN) Kapsamında LEO Haberleşme Uydu Sistemleri Raporu, November 14, 2022.
9. Nicolò Boschetti, Nathaniel G. Gordon, and Gregory Falco, "Space Cybersecurity Lessons Learned from the ViaSat Cyberattack" (paper presented at ASCEND 2022, Las Vegas, NV, October 24–26, 2022).
10. SpaceX, "SpaceX AI — Starmind," accessed July 2026.
11. European Space Agency, "Strengthening Space Cybersecurity through ESA's GSTP," accessed July 2026.

12. European Union Agency for Cybersecurity (ENISA), Space Threat Landscape (Heraklion: ENISA, 2022).
13. Viasat, "About Viasat," accessed July 3, 2026.
14. SatBeams, "KA-SAT Satellite Details," accessed July 3, 2026.
15. Viasat, "Viasat Completes Acquisition of Remaining Stake in Its European Broadband Joint Venture," October 1, 2021.
16. Viasat, "Satellite Communications Antenna Systems," accessed July 2026.
17. Jonathan Greig, "NSA, Viasat Say 2022 Hack Was Two Incidents; Russian Sanctions Resulted from Investigation," The Record from Recorded Future News, August 11, 2023.
18. Kevin Poireault, "Five Takeaways From the Russian Cyber-Attack on Viasat's Satellites," Infosecurity Magazine, May 9, 2023.
19. MITRE ATT&CK, "AcidRain (S1125)," accessed July 2026.
20. Via Satellite, "Viasat Details KA-SAT Cyberattack That Affected Thousands of Modems in Ukraine," March 30, 2022.
21. Arsheen Kazi, Samreen Kazi, and Saloni Bhosale, "Invisible Battlefields: Analyzing the Viasat Attack and Its Broader Implications," *Scientific Bulletin* XXX, no. 1 (2025): 62, fig. 2.
22. Council of the European Union, "Russian Cyber Operations against Ukraine: Declaration by the High Representative on Behalf of the European Union," May 10, 2022.
23. U.S. Department of State, "Attribution of Russia's Malicious Cyber Activity Against Ukraine," May 10, 2022.
24. UK Foreign, Commonwealth & Development Office, "Russia Behind Cyber Attack with Europe-Wide Impact an Hour Before Ukraine Invasion," May 10, 2022.
25. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, ed. Michael N. Schmitt (Cambridge University Press, 2017).
26. RFE/RL, "Western Allies Say Moscow Behind Cyberattack Ahead Of Ukraine Invasion," Radio Free Europe/Radio Liberty, May 10, 2022.
27. International Committee of the Red Cross, International Humanitarian Law and Cyber Operations during Armed Conflicts (Geneva: ICRC, 2019).
28. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, 1125 U.N.T.S. 3.
29. European Parliament and Council of the European Union, Directive (EU) 2022/2555 of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive), Official Journal of the European Union, December 27, 2022.
30. European Commission, Proposal for a Regulation of the European Parliament and of the Council on the Safety, Resilience and Sustainability of Space Activities in the Union, COM(2025) 335 final, June 25, 2025.
31. Teslarati, "SpaceX's Newest Starmind Will Make Earth Data Centers Obsolete," June 2026.
32. TechiExpert, "SpaceX Released AI1 Satellite Architecture to Launch Megawatt-Scale Orbital AI Data Centers," June 2026.
33. Space.com, "Another 'Star' Is Born: SpaceX Names AI Megaconstellation 'Starmind,'" June 2026.
34. Tom's Hardware, "Elon Musk Unveils $20 Billion 'TeraFab' Chip Project to Make Chips, Memory, and Package Processors All Under One Roof, Targets a Terawatt of Annual Compute," March 22, 2026.
35. Teslarati, "Elon Musk Launches TERAFAB: The $25B Tesla-SpaceXAI Chip Factory That Will Rewire the AI Industry," March 22, 2026.
36. Euronews, "What Is Elon Musk's New Chip-Making Facility, Terafab, and Why Is He Building It Now?," May 6, 2026.
37. Data Center Dynamics, "SpaceX Details AI1 Satellite 'Data Center,' Claims 150kW Peak Compute," June 2026.
38. Tom's Hardware, "Elon Musk's First-Gen Orbital Data Center Craft Spans Wider Than a Boeing 747," June 9, 2026.
39. Graham Wallington, "Why SpaceX's AI1 Orbital Data Centre Doesn't Add Up," Medium, June 9, 2026.

40. Rajiv Thummala, Shristi Sharma, Matteo Calabrese, and Gregory Falco, "Adversarial Machine Learning Threats to Spacecraft," arXiv:2405.08834, May 14, 2024.
41. Rajiv Thummala and Gregory Falco, "Space Hacktivism and the Russo–Ukrainian War: An Open Source Space Security Analysis," Journal of Cybersecurity 12, no. 1 (2026): tyag013.
42. Clémence Poirier, Hacking the Cosmos: Cyber Operations against the Space Sector: A Case Study from the War in Ukraine (Zürich: Center for Security Studies, ETH Zürich, 2024).
43. Sandra Erwin, "The Race to Defend Satellites from Cyberattacks," SpaceNews, November 2025.
44. TÜRKSAT A.Ş., "Türksat Genel Müdürü Atalay: 'Türksat 7A'nın Üretimi Bu Yıl Başlayacak,'" March 26, 2026.
45. CyberPeace Institute, "Case Study: Viasat Attack," accessed 2026.
46. Turkish Space Agency, "National Space Program," accessed July 13, 2026.
47. International Astronautical Federation, "IAC 2026 Antalya," accessed July 13, 2026.
48. T.C. Ulaştırma ve Altyapı Bakanlığı, "5G Yetkilendirme İhalesi ve Mobil Altyapı Stratejisi," October 16, 2025.
49. Ericsson, "Turkcell and Ericsson Partner on 6G Research in Türkiye," March 4, 2026.
50. Türkiye Today, "Türksat to Launch 7A Satellite Project in First Quarter of 2026," September 21, 2025.
51. Cumhurbaşkanlığı Siber Güvenlik Başkanlığı, Siber Güvenlik Kurulu, "Kritik Altyapıların Korunması," accessed July 2026.

Authors

Belinay KURU is a high school student at İrfan Bileydi Vocational and Technical Anatolian High School (Antalya) specializing in cybersecurity with a strong passion for artificial intelligence, space technologies, and interdisciplinary research. She enjoys exploring how emerging technologies can be applied to solve real-world challenges, particularly in secure and intelligent systems. As a participant in the Özyeğin University High School Summer Research Program, she contributed to the technical cybersecurity aspects of AI-enabled LEO satellite systems, further strengthening her interest in the intersection of AI, cybersecurity, and space. Through competitions, research projects, and hands-on technical experiences, she continues to develop her skills while pursuing opportunities to contribute to innovative technologies.

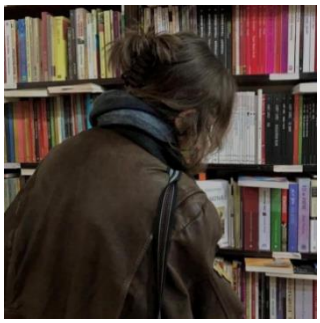
Cengiz Onat YAPANEL is an IB Diploma student at Kabataş Erkek High School (İstanbul) with a strong passion for aerospace engineering, artificial intelligence, and scientific research. He has conducted multiple research projects in satellite technologies and AI, with papers accepted to international conferences such as the International Astronautical Congress (IAC) and the Recent Davanca in Space Technologies (RAST) Conference. He has also completed internships at Turkish Aerospace Industries (TUSAŞ), Istanbul Technical University, Özyeğin University, and CERN. Beyond academics, he founded his school's AI Club, leads environmental initiatives, and actively volunteers as a tutor. His experiences have strengthened his research, leadership, and problem-solving skills, and he aspires to develop innovative engineering solutions that create a positive impact on society.

Defne Nur YILMAZ is a student at MatBilim Koleji (Ankara). She is a high-achieving student with a deep focus on aerospace engineering and artificial intelligence. Consistently demonstrating academic excellence, she has earned full scholarships and graduated as the top-ranked student in her previous institutions. Her technical foundation is complemented by her discipline and resilience as a national-level fencing athlete—a balance that allows her to thrive in high-pressure environments. Committed to innovation and social responsibility, she has actively pursued specialized technical training in aeronautics and AI through international institutions like the Technical University of Munich and the University of Pennsylvania. Defne Nur specializes in the technical development of her projects, consistently taking the lead on the engineering and implementation aspects of her work. She is now leveraging this technical rigor and strong academic background as she prepares to advance her studies in international higher education.

Defne Su BİRLİK is a student at İstek Acıbadem Anatolian High School (İstanbul) with a strong interest in artificial intelligence, technology law, and international relations. She has a strong academic background and has improved her research, public speaking, teamwork, and problem-solving skills through Model United Nations conferences, where she has received three Outstanding Delegate Awards and one Honorable Mention Award. Outside of academics, she played volleyball for Fenerbahçe Volleyball Club and Beşiktaş Volleyball Youth Team, has been playing the piano for ten years, and is an active member of her school's dance club. Defne recently has worked as a research assistant on a project about the use of AI in satellite technologies and the legal issues related to this field. Through this research, she developed her interest in the relationship between technology and law. In the future, she hopes to study law and build a career in international corporate law. She is committed to improving herself through research, leadership, and international academic opportunities.

Ece BAHAR is an AP student at TEV İnanç High School (Kocaeli) and a participant in the BİLSEM Gifted and Talented Education Program. She is the founder and president of her school's Law Club and has represented Turkey in three Erasmus+ international mobility programs in Romania, the Czech Republic, and Hungary, participating in international projects focused on intercultural collaboration and global citizenship. With a growing interest in electronics and hands-on technology projects such as Arduino, alongside her academic focus on socio-legal research, she is drawn to the intersection of technology, sociology, and psychology. Outside of academics, she is an accomplished guitar player, actively engages in vocal performance, pursues creative arts, and is a devoted animal lover.

Gökçe Kaan ASLAN is a student at Zafer High School (Ankara) with a strong interest in mathematics, computer science, and artificial intelligence. He has participated in various academic competitions, technology programs, and research projects, gaining experience in problem-solving, programming, and teamwork. Motivated by curiosity and continuous learning, he enjoys applying his knowledge to practical challenges and further developing his technical and analytical skills.



Medine Yaren GÜNEYSU is a high school student. Her experience includes working as a team member in the Research & Opportunities Team for the international student-led Next Idea Club, where she helps prepare academic resources and guides. Additionally, she has experience organizing and leading a student workshop, and participates in her school's Radio Club, contributing to visual design, and the Philosophy Club, where she has proposed organized debates. Her academic and personal interests include law, biology, literature, visual arts & character design, and ballet. She speaks native Turkish, advanced English, and is self-studying French.

Bibliography

- Boschetti, Nicolò, Nathaniel G. Gordon, and Gregory Falco. "Space Cybersecurity Lessons Learned from the ViaSat Cyberattack." Paper presented at ASCEND 2022, Las Vegas, NV, October 24–26, 2022.
- Clarke, Arthur C. First on the Moon. New York: Harcourt Brace Jovanovich, 1970.
- Council of the European Union. "Russian Cyber Operations against Ukraine: Declaration by the High Representative on Behalf of the European Union." May 10, 2022.
- Cumhurbaşkanlığı Siber Güvenlik Başkanlığı, Siber Güvenlik Kurulu. "Kritik Altyapıların Korunması." Accessed July 2026.
- CyberPeace Institute. "Case Study: Viasat Attack." Accessed 2026.
- Data Center Dynamics. "SpaceX Details AI1 Satellite 'Data Center,' Claims 150kW Peak Compute." June 2026.
- Ericsson. "Turkcell and Ericsson Partner on 6G Research in Türkiye." March 4, 2026.
- Erwin, Sandra. "The Race to Defend Satellites from Cyberattacks." SpaceNews, November 2025.
- Euronews. "What Is Elon Musk's New Chip-Making Facility, Terafab, and Why Is He Building It Now?" May 6, 2026.
- European Commission. Proposal for a Regulation of the European Parliament and of the Council on the Safety, Resilience and Sustainability of Space Activities in the Union. COM(2025) 335 final, June 25, 2025.
- European Parliament and Council of the European Union. Directive (EU) 2022/2555 of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, December 27, 2022.
- European Space Agency. ESA Report on the Space Economy 2025. Paris: European Space Agency, 2025.
- European Space Agency. "Strengthening Space Cybersecurity through ESA's GSTP." Accessed July 2026.
- European Space Agency. Telecommunication Systems and Techniques. Accessed July 2026.
- European Union Agency for Cybersecurity (ENISA). Low Earth Orbit (LEO) SATCOM Cybersecurity Assessment. February 2024.
- European Union Agency for Cybersecurity (ENISA). Space Threat Landscape. Heraklion: ENISA, 2022.
- Falco, Gregory. "Cybersecurity Principles for Space Systems." Journal of Aerospace Information Systems 16, no. 2 (2019): 61–70.
- Greig, Jonathan. "NSA, Viasat Say 2022 Hack Was Two Incidents; Russian Sanctions Resulted from Investigation." The Record from Recorded Future News, August 11, 2023.
- Guerrero-Saade, Juan Andres, and Max van Amerongen. "AcidRain | A Modem Wiper Rains Down on Europe." SentinelOne (SentinelLabs), March 31, 2022.
- International Astronautical Federation. 2026. "IAC 2026 Antalya." Accessed July 13, 2026.
- International Committee of the Red Cross. International Humanitarian Law and Cyber Operations during Armed Conflicts. Geneva: ICRC, 2019.
- Kazi, Arsheen, Samreen Kazi, and Saloni Bhosale. "Invisible Battlefields: Analyzing the Viasat Attack and Its Broader Implications." *Scientific Bulletin* XXX, no. 1 (2025): 59–67.
- MITRE ATT&CK. "AcidRain (S1125)." Accessed July 2026.
- Poireault, Kevin. "Five Takeaways From the Russian Cyber-Attack on Viasat's Satellites." Infosecurity Magazine, May 9, 2023.
- Poirier, Clémence. Hacking the Cosmos: Cyber Operations against the Space Sector: A Case Study from the War in Ukraine. Zürich: Center for Security Studies, ETH Zürich, 2024.
- Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I). June 8, 1977. 1125 U.N.T.S. 3.
- RFE/RL. "Western Allies Say Moscow Behind Cyberattack Ahead Of Ukraine Invasion." Radio Free Europe/Radio Liberty, May 10, 2022.

- SatBeams. "KA-SAT Satellite Details." Accessed July 3, 2026.
- Space.com. "Another 'Star' Is Born: SpaceX Names AI Megaconstellation 'Starmind.'" June 2026.
- SpaceX. "SpaceX AI — Starmind." Accessed July 2026.
- Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Edited by Michael N. Schmitt. Cambridge: Cambridge University Press, 2017.
- T.C. Ulaştırma ve Altyapı Bakanlığı. "5G Yetkilendirme İhalesi ve Mobil Altyapı Stratejisi." October 16, 2025.
- Teslarati. "Elon Musk Launches TERAFAB: The $25B Tesla-SpaceXAI Chip Factory That Will Rewire the AI Industry." March 22, 2026.
- Teslarati. "SpaceX's Newest Starmind Will Make Earth Data Centers Obsolete." June 2026.
- Thummala, Rajiv, and Gregory Falco. "Space Hacktivism and the Russo–Ukrainian War: An Open Source Space Security Analysis." Journal of Cybersecurity 12, no. 1 (2026): tyag013.
- Thummala, Rajiv, Shristi Sharma, Matteo Calabrese, and Gregory Falco. "Adversarial Machine Learning Threats to Spacecraft." arXiv:2405.08834, May 14, 2024.
- Tom's Hardware. "Elon Musk's First-Gen Orbital Data Center Craft Spans Wider Than a Boeing 747." June 9, 2026.
- Tom's Hardware. "Elon Musk Unveils $20 Billion 'TeraFab' Chip Project to Make Chips, Memory, and Package Processors All Under One Roof, Targets a Terawatt of Annual Compute." March 22, 2026.
- Turkish Space Agency. 2026. "National Space Program." Accessed July 13, 2026.
- Türkiye Today. "Türksat to Launch 7A Satellite Project in First Quarter of 2026." September 21, 2025.
- Türkiye Uzay Ajansı (Turkish Space Agency, TUA). Karasal Olmayan Şebekeler (NTN) Kapsamında LEO Haberleşme Uydu Sistemleri Raporu. November 14, 2022.
- TÜRKSAT A.Ş. "Türksat Genel Müdürü Atalay: 'Türksat 7A'nın Üretimi Bu Yıl Başlayacak.'" March 26, 2026.
- UK Foreign, Commonwealth & Development Office. "Russia Behind Cyber Attack with Europe-Wide Impact an Hour Before Ukraine Invasion." May 10, 2022.
- U.S. Department of State. "Attribution of Russia's Malicious Cyber Activity Against Ukraine." May 10, 2022.
- Via Satellite. "Viasat Details KA-SAT Cyberattack That Affected Thousands of Modems in Ukraine." March 30, 2022.
- Viasat. "About Viasat." Accessed July 3, 2026.
- Viasat. "KA-SAT Network Cyber Attack Overview." Viasat News, March 30, 2022.
- Viasat. "Satellite Communications Antenna Systems." Accessed July 2026.
- Viasat. "Viasat Completes Acquisition of Remaining Stake in Its European Broadband Joint Venture." October 1, 2021.
- Wallington, Graham. "Why SpaceX's AI1 Orbital Data Centre Doesn't Add Up." Medium, June 9, 2026.