

Headline

Countermeasures against security threats arise with development of space industry

Hyun-joo Kim / OT/ICS Consulting Team Leader

■ Overview



In 2001, American billionaire entrepreneur Dennis Tito paid \$200 million (about KRW 280 billion) for a trip to the International Space Station (ISS) and became the first person to travel into space at his own expense. Since then, Amazon founder Jeff Bezos, SpaceX CEO Elon Musk, and Japanese billionaire entrepreneur Yusaku Maezawa have paid huge amounts of money to experience space.

Today, space tourism cost went down to \$450,000 (about KRW 600 million). And you could orbit the moon aboard a Russian Soyuz (Союз) spacecraft for \$100 million (about KRW 140 billion). We are at the beginning of a full-fledged 'new space' era in which the private sector leads space travel around the world.

In line with this, the scope of security is also expanding into space. This article will discuss security trends in the 'new space' era, as well as space security threats and response measures.

■ Growth of the space industry

In the past, the prevailing perception was that the space industry was only possible at a national level. It cost an astronomical amount of money, so no private sector company could even think of getting involved. However, recently, low-cost launch vehicle and satellite manufacturing technologies have been developed and private companies such as SpaceX, Blue Origin and Virgin Galactic, have emerged that can invest huge amounts of money in the space industry. Since then, the space industry has begun to grow rapidly.

The size of the global space industry has grown from \$339.1 billion (about KRW 475 trillion) in 2016 to \$386 billion (about KRW 540 trillion) in 2021 and is expected to reach \$1 trillion (about KRW 1,400 trillion) by 2040. One of the most notable reasons for the expansion of the space industry is the sharp decrease in the cost of sending satellites into space. With the advent of private companies and reusable rockets, launch costs fell to \$1,500 (about KRW 2.1 million) per kg in 2022, more than 30 times cheaper than in the past, and are expected to drop further to \$100 (about KRW 140 thousand) per kg by 2040.

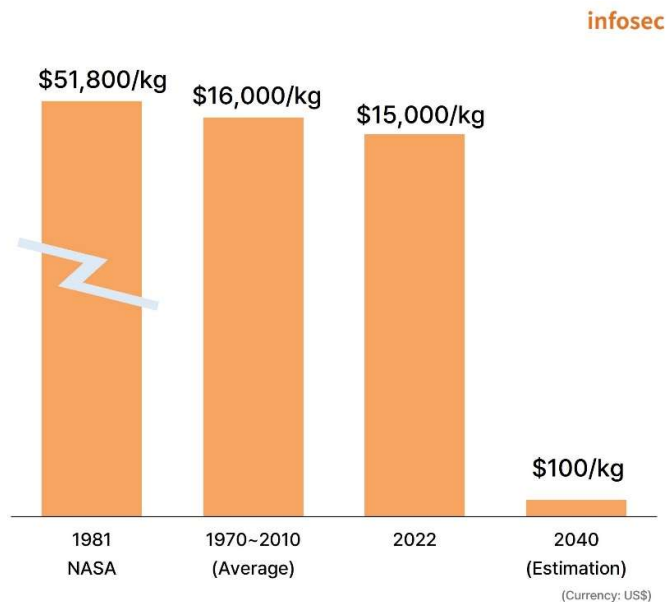


Figure 1. Launch cost trends for space launch vehicles

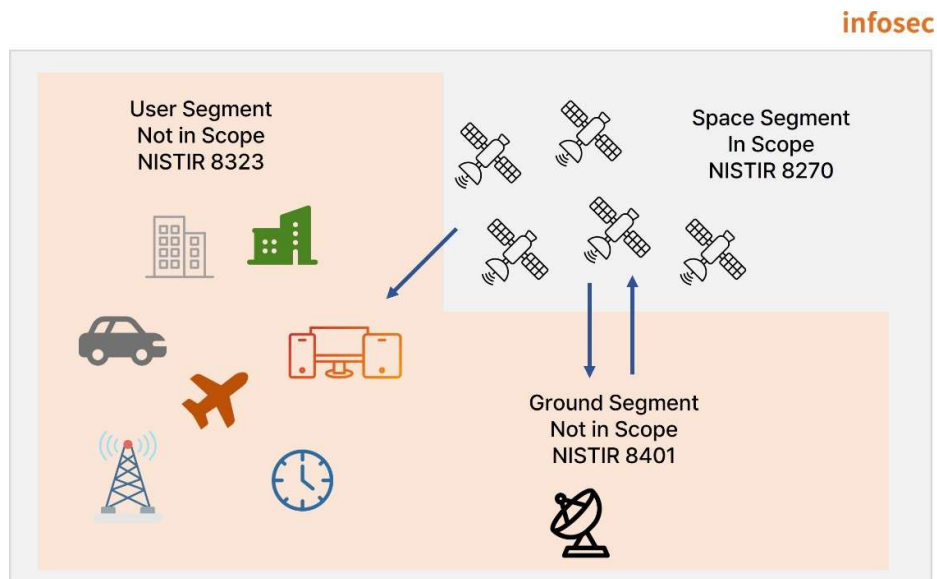
The United States, known as a space industry powerhouse, has developed a national strategy for in-space servicing, assembly, and production as part of its efforts to secure and maintain leadership in the global space market. Japan also operates a space industry strategy fund and is actively investing in nurturing space-related startups. Competition in space services is intensifying as global space companies prepare various services, such as the global satellite communication network based on low-orbit small satellites being built by SpaceX building.

In line with the global trend, the Korean government is also working to create a private space enterprise ecosystem, such as by establishing a plan to strengthen support for the creation of a private-sector-led space industry ecosystem. The government selected

aerospace technology as one of 12 national strategic technologies to scale up in the public-private collaboration market and secure irreplaceable source technologies for. The Korean government allocated KRW 839.2 billion to its space budget in 2023, and plans to increase the budget to KRW 1.5 trillion by 2027 and operate various programs to foster space experts.

■ Components of the space operation architecture

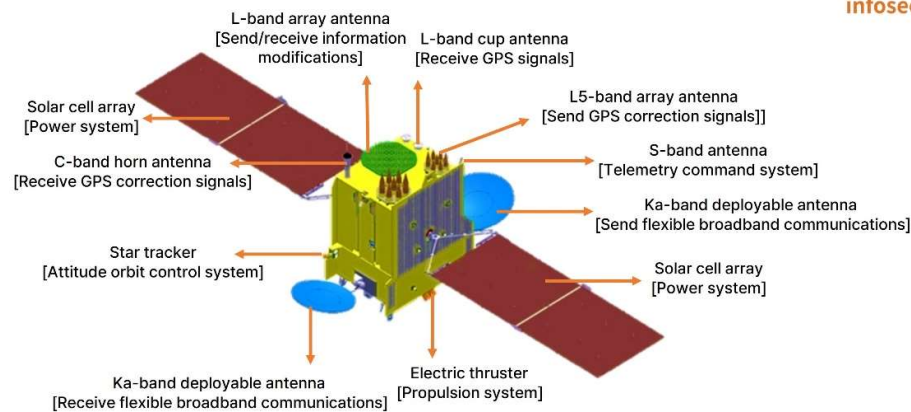
Under the National Institute of Standards and Technology (NIST) Interagency Report (IR) 8270 (Introduction to Cybersecurity for Commercial Satellite Operations), the space operations architecture is divided into the space segment, the ground station segment, and the user segment.



* Source: NIST IR 8270

Figure 2. Segments of the space operation architecture

The space segment is outer space where spacecraft and satellites are located, and the ground segment is the area where satellites are operated and controlled. The user segment is a service area where satellites are utilized for smart ships, airplanes, autonomous cars, buses, etc.



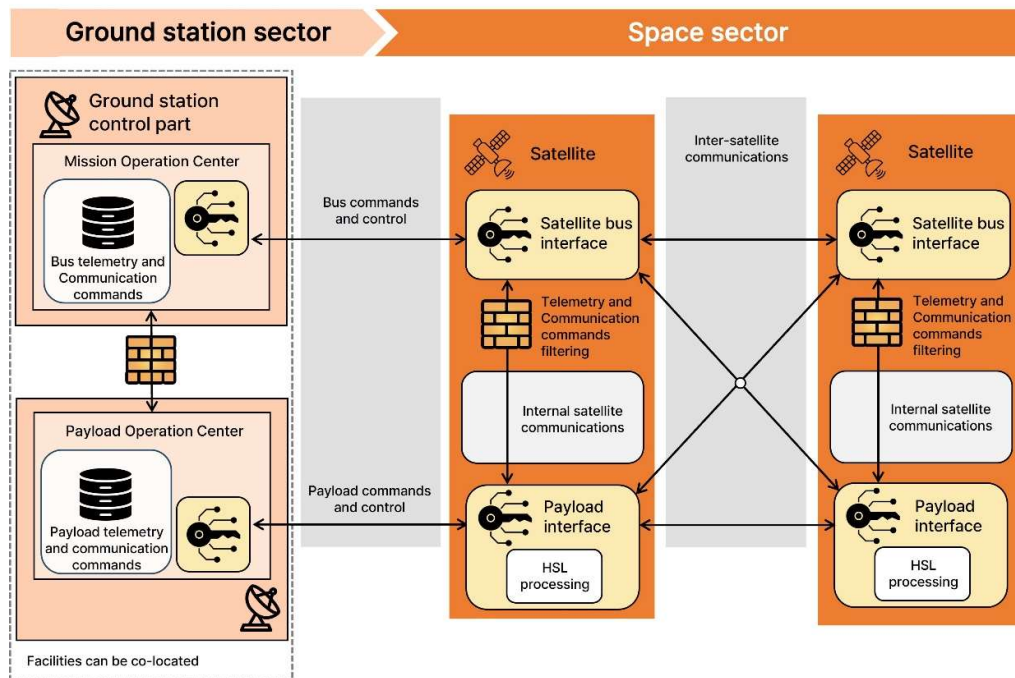
* Source: Outside view of the Chollian-3 satellite (Ministry of Science and Technology Information and Communication]

Figure 3. Outside view of a satellite

Satellites belonging to the space segment are composed of a bus that operates the satellite and payloads that perform missions for communication, observation, exploration, etc. Satellites are divided into communication satellites, meteorological satellites, ocean observation satellites, broadcast satellites, etc., depending on their functions. The payloads perform satellite services, and the bus carries the payloads and enables them to perform their functions.

The Chollian-3, a public communications satellite for disaster/safety responses scheduled to be launched in 2027, is composed of multiple antennas and subsystems, as shown in the figure above. As can be seen, the bus, which is the satellite body, is composed of several subsystems. These include the structural system, which forms the skeleton of the satellite; the power system, which supplies electricity; the attitude orbit control system, which controls the attitude and orbit to prevent the satellite from deorbiting; the propulsion system, which includes the fuel and thrusters; the telemetry and command system, which exchanges commands with the ground station; and the thermal control system, which maintains the satellite at an appropriate temperature. The type of satellite (communication satellite, observation satellite, broadcasting satellite, etc.) is determined based on the payload configuration, and the structure and shape of the satellites may vary.

The ground station consists of a mission operation center and a payload operation center. The mission operations center issues commands to the satellite and receives telemetry data. The payload operation center communicates with the satellite's payloads to provide satellite services. NIST IR 8270 (Introduction to Cybersecurity for Commercial Satellite Operations) comprehensively describes the communication link between ground stations and satellites.



* Source: NIST IR 8270 (Introduction to Cybersecurity for Commercial Satellite Operations)

Figure 4. Architecture of the space segment and ground station segment

In the space segment, satellites communicate with each other using lasers, and ground stations and satellites communicate with each other by sending and receiving radio waves through large antennas. The ground station mission operation center operates and controls the satellites by issuing remote commands to the bus, and the payload operations center receives and processes payload data from the satellite. For communications between the ground segment and the satellite, the frequency is selected according to the purpose and use. For satellite communications, the L-band (1–2 GHz), S-band (2–4 GHz), C-band (4–8 GHz), X-band (8–12 GHz), Ku-band (12–18 GHz), and Ka-band (26–40 GHz) are used.

■ Space Security Incident Cases

In February 2022, just before invading Ukraine, Russia attacked a satellite Internet network, disabling tens of thousands of Viasat modems and disrupting the Ukrainian military's direction and command system. This is a representative example of a space security incident. The space industry is currently growing rapidly and satellite utilization services are increasing, so the number of space-related security incidents is expected to increase in the future.

Year	Space Security Incident	Impact of the security incident
2008	A jamming attack on NASA's Terra satellite left the satellite uncontrollable.	Satellite became uncontrollable
2014	An internet cyberattack occurred on the weather observation satellite network of the National Oceanic and Atmospheric Administration's (NOAA).	Satellite data not received
2015	There was an announcement that it was possible to interpret, decode, and convert phasor communication data from an Iridium communication satellite into clear text information (plain text) using commercially available antennas (International Conference Chaos Communication Camp 2015).	Communication content exposed
2018	An employee illegally infiltrated the network of NASA's Jet Propulsion Laboratory (JPL) using a Raspberry Pi installed without permission, and leaked 23 files and 50 MB of data.	Mission data leaked
2020	Radio analysis using commercially available antennas demonstrated that communications to geostationary communications satellites were not encrypted (International Conference BlackHat). - Information about hazardous materials, wind power plant administrator privileges, and personal information (passport numbers, credit card data, etc.) were found to be in plaintext.	Communications intercepted
2022	A specific communication modem using Viasat's communication satellite KA-SAT service was infected with wiper malware, making it impossible to access the satellite.	Impossible to access satellite
2022	A cyberattack on the computer system of the Alma Observatory in Chile disrupted scientific observations and shut down the website of the Chilean Joint ALMA Observatory.	Observation of satellites disrupted

* Source: Japan, 'Guidelines for Cyber Security Measures for Private Sector Space Systems'

Table 1. Space security incident cases

■ Space Security Threats

Satellites are used for academic, military, and business purposes, and provide a wide range of services to a variety of users, including ships, automobiles, airplanes, businesses, and homes. Any space-related components carried onboard satellites for these purposes, as well as control software, communications links between satellites and ground stations, and ground station networks and systems, can be very attractive targets for hackers.

From an IT (information technology)/OT (operational technology) perspective, satellite and ground station components comprise systems with security vulnerabilities and often transmit signals in an unencrypted state, exposing them to various IT/OT security threats. The motivations of hackers attacking space systems are no different from those of hackers attacking IT/OT systems (financial, social, and political reasons). In June 2023, the U.S. Air Force held a satellite hacking contest after launching a test satellite, as it believed that the level of security in the aerospace field was insufficient. The aerospace field is considered vulnerable to hacking because it is highly dependent on information and communication networks such as satellite communication networks, ground station control infrastructure, and GPS systems.

NIST IR 8270 (Introduction to Cybersecurity for Commercial Satellite Operations) identifies eight types of potential space cybersecurity threats. The security threats presented in this report include jamming, spoofing and hijacking of communications links between satellites and ground stations, as well as system compromise, denial of service attacks and malware injection that could affect satellite control.

- A. Intentional jamming and spoofing of sensor data
- B. Interception and theft of sensor data
- C. Intentional corruption of sensor systems
- D. Denial-of-service attacks on sensors
- E. Intentional jamming or spoofing of guidance control
- F. Hijacking of or unauthorized commands to guidance control
- G. Malicious code injection
- H. Denial-of-service attacks on guidance

Japan's 'Guidelines for Cyber Security Measures for Private Sector Space Systems (Mar. 2023)' presented seven risk scenarios that could cause serious damage to space systems.

No.	Space Hazard Scenarios (Cases)	
1	Loss of satellite orbit control due to a targeted mail attack	<ul style="list-style-type: none"> ① An employee's terminal is infected with malware via email ② A hacker gains unauthorized access over the Internet. ③ The hacker intercepts uplink data and manipulates attitude control information and mission equipment control information, and sends it to the satellite. ④ Satellite control is temporarily lost.
2	Loss of satellite/mission device control due to a malware infection of a development/manufacturing terminal	<ul style="list-style-type: none"> ① A development/manufacturing terminal used to update satellite body software via mail is infected with malware. ② A hacker gains unauthorized access over the Internet (a backdoor is inserted into the update program infected with malware). ③ The hacker uses the backdoor of the update program to remotely operate the satellite from the ground station (satellite operating facility). ④ Satellite control is temporarily lost.
3	Loss of satellite control due to a cyberattack on satellite data utilization equipment	<ul style="list-style-type: none"> ① An unauthorized terminal is installed in the ground station (satellite data utilization facility). ② A hacker gains unauthorized access over the Internet. ③ The hacker travels across unseparated networks and illegally accesses multiple servers. ④ Various servers at the ground station (satellite operation facility) go down and the satellite control capability is lost.
4	Inability to provide service due to illegal access to an observation reception server	<ul style="list-style-type: none"> ① A hacker gains unauthorized access to the observation reception server over the Internet and infects it with ransomware. ② All servers and terminals within the ground station (satellite data use facility) are infected with ransomware due to insufficient security settings of the cloud-built ground station. ③ System data (boot files, etc.) in the satellite data provision server is deleted, making it impossible to reboot or provide service.
5	Leakage of corporate secrets through an email attack in a remote work environment	<ul style="list-style-type: none"> ① A server is infected with malware by email from a hacker posing as a worker while working remotely. ② The hacker gains unauthorized access over the Internet. ③ The satellite manufacturing company's confidential information is leaked.

No.	Space Hazard Scenarios (Cases)	
6	Suspension of operations due to unauthorized use of a USB memory device	<ul style="list-style-type: none"> ① A hacker creates a USB infected with malware and delivers it to a manufacturing facility manager, disguising it as a configuration USB for a controller. ② The server is infected with malware when the manufacturing facility manager changes controller settings using the USB provided by the hacker. ③ The controller settings and manufacturing program are falsified, causing equipment control problems and stopping manufacturing operations.
7	Disintegration of satellite constellations due to the introduction of an illegal satellite-borne device	<ul style="list-style-type: none"> ① The hacker installs logic bombs on circuit boards used in the attitude control controller and sells the boards at a low price to a satellite developer planning to build constellations of dozens of satellites. ② The circuit boards pass the acceptance inspection and system inspection of the manufacturing manager and are installed in the mass-produced satellites. ③ After launch, the logic bomb is executed when specific conditions are met. ④ Satellite control is lost and there is a risk of cluster collapse.

Table 2. Space hazard scenario cases





Satellites provide services in various fields such as smart ships, autonomous vehicles, urban air mobility (UAM), and smartphones. However, a disruption of the Global Navigation Satellite System (GNSS) or the manipulation of position information provided by the GNSS could cause significant social unrest. Accidents may occur, such as smart ships deviating from their routes or UAM crashing due to driving errors. Therefore, it is necessary to closely analyze space-related security threats and establish security measures.

■ Space Security Trends

As awareness of space security threats grows, interest in space cybersecurity is growing in many countries. In 2020, the Trump administration issued Space Policy Directive (SPD)-5, declaring its commitment to adherence to principles and guidelines for space cybersecurity. In addition, considering that space systems such as satellites provide essential services across the socioeconomic spectrum, discussions have been ongoing for several years as to whether space systems should be designated as the 17th type of infrastructure facility. The Japanese government has announced space system security guidelines and is pushing forward with full-scale cybersecurity enhancement projects. The Korean government announced a strategy to secure global competitiveness in the information security industry to improve the level of security in the private sector aerospace industry (Sep. 2023, Ministry of Science and ICT) and launched the Space Asset Cybersecurity Council. The council is currently working with the National Intelligence

Service, the Ministry of National Defense, and the Korea AeroSpace Administration to develop an integrated roadmap for responding to satellite cyber threats.

The table below shows policies and strategies related to space and space security of major countries.

Country	Description	
USA 	Policies and guidelines	<ul style="list-style-type: none"> · National Security Strategies (Dec. 2017) · National Cyber Strategies (Sep. 2018) · Space Priority Framework (Dec. 2021) · Cybersecurity Framework for Hybrid Satellite Networks_NIST IR 8441 (Jun. 2023)
	Laws and systems	<ul style="list-style-type: none"> · Space Policy Guidelines (SPD 1–7) · US House introduced a space infrastructure bill (Jun. 2021) <ul style="list-style-type: none"> - Promoted the addition of space systems to 16 critical infrastructures classified by the Department of Homeland Security. · U.S. Senate reissued a bill on commercial satellite cybersecurity (May 2023) <ul style="list-style-type: none"> - Mandated the CISA to protect commercial satellite operators - Required the Director of National Cybersecurity and the Space Council to develop strategies to enhance coordination across the federal government regarding the cybersecurity of satellite systems.
EU 	Policies and guidelines	<ul style="list-style-type: none"> · EU Space Strategies for Security and Defense (Mar. 2023) · Cybersecurity Assessment Report for LEO SATCOM (Feb. 2024)
	Laws and systems	<ul style="list-style-type: none"> · EU Space Act (to be pursued)
Japan 	Policies and guidelines	<ul style="list-style-type: none"> · 2023 Space Policy Basic Plan (Jun. 2023, revised) · Guidelines for Cybersecurity Measures for Private Sector Space Systems (Mar. 2023)
	Laws and systems	<ul style="list-style-type: none"> · Space Basic Act (2008)
Germany 	Policies and guidelines	<ul style="list-style-type: none"> · National Space Strategies (Sep. 2023, revised)
	Technical development / infrastructure	<ul style="list-style-type: none"> · IT Basic Protection Profile for Space Infrastructure (Jul. 2022)
	Laws and systems	<ul style="list-style-type: none"> · Space Agency Establishment Act (1998) · Remote Exploration Act (2007) · National Space Act (under preparation)
China 	Policies and guidelines	<ul style="list-style-type: none"> · 2030 Science and Technology Innovation Plan, 'Space-Ground Integrated Information Network' Construction Project · 2021 Space White Paper (published every five years)
	Technical development / infrastructure	<ul style="list-style-type: none"> · Announced the Zero Trust System Technical Specifications (2021)

* Source: Korea Internet & Security Agency, 'Survey and Analysis of the Space Cyber Security Policy Trends of Major Countries'

Table 3. Global policies and strategies for space and space security

■ Space Security Response Plan

Until recently, satellites have been considered safe because they are located in space, far from the ground. However, as explained above in terms of space security incidents and security threats, satellites are no longer in a safe zone. To strengthen space security, it is necessary to internalize and apply cybersecurity throughout the space system life cycle, from the development/manufacturing stage of space products to the operation stage and the disposal stage. For this purpose, the following security measures are required.

1) Space product development security and supply chain security

The top priority is to consider security at the design/development stage of software installed in space products and to internalize security from the manufacturing stage of parts. Software installed on satellites and applications developed for satellite services must have security requirements defined and secure coding applied from the design/development stage. In addition, supply chain security vulnerability checks, including the confirmation of open source vulnerabilities, must be performed, and a security review process that reviews security applications must be followed at the testing stage.

2) Risk analysis by segment and application of security technologies

Security technologies must be applied to identify and respond to risks that may arise in the space segment (satellite), ground segment (satellite control equipment, payload data operation equipment), and satellite utilization service areas (smart ships, autonomous vehicles, urban air mobility, etc.).

- A. Satellite: Security verification for onboard software and devices, and countermeasures against vulnerabilities
- B. Communication section between satellites and ground stations: Application of communication section tunneling, encryption of transmitted data, message authentication to respond to data tampering, anti-jamming technology (such as frequency hopping), etc.
- C. Ground segment (satellite control equipment, payload data operation equipment): Network security against unauthorized persons (intrusion blocking, intrusion prevention, network access control, etc.), satellite control and payload data security (data encryption, information leakage prevention), authentication and authority control (multi-authentication, account management), malware response (vaccine, abnormal symptom detection), physical access control (antenna, access control to important facilities, monitoring, etc.)
- D. Satellite utilization service segment: Preparation of measures to identify and manage risks for each service

■ Conclusion

In order to implement the same space security measures mentioned above, it is necessary to establish national space cybersecurity guidelines. It is important for both governments and businesses to take a continuous interest in leading space-related companies and applying security to the accelerating space industry.

Following this trend, SK Shieldus provides cyber security services and consulting suitable for space industry security.

SK Shieldus can provide security consulting, diagnosis/simulated hacking, SI business (encryption solutions, network security, authentication/access control systems, etc.), and physical security services to companies operating ground stations to enhance security. Satellite service provision applications are often implemented primarily on the web, so it is necessary to undergo source code diagnosis, mock hacking, and supply chain security diagnosis (open source inspection, etc.).

Since it is difficult to update and modify the S/W of a satellite once it has been launched, a diagnosis of the S/W loaded on the satellite, such as an IoT security diagnosis before launch, is necessary. Companies that manufacture satellite components can receive OT/ICS security consulting and security solution services for safer management.

Please visit the [SK Shieldus website](#) for details.