kaspersky

Space systems as targets and tools for cyberattacks

Semen Kort, Alexander Nikolaev, Ekaterina Rudina

06.08.2026 Version 1.0

Contents

Introduction

In November 2019 in Brussels, NATO leaders officially recognized space as a "new operational domain" (alongside land, sea, air, and cyberspace).

This article explores issues related to information security and attacks in space. Its focus is not limited to targeted attacks on the digital infrastructure of space systems; it also encompasses a broader spectrum of incidents, including software glitches, system failures, and unintentional human errors. A retrospective analysis of these events provides valuable information for identifying hidden vulnerabilities and improving the resilience of space infrastructure. It is impossible to build an effective space cybersecurity strategy without factoring in errors and failures – this assertion lies at the core of the present research.

A space system is an extremely remote and hard-to-control automated system. To describe various attacks on space systems, let us present a diagram that includes the primary subsystems and communication links.

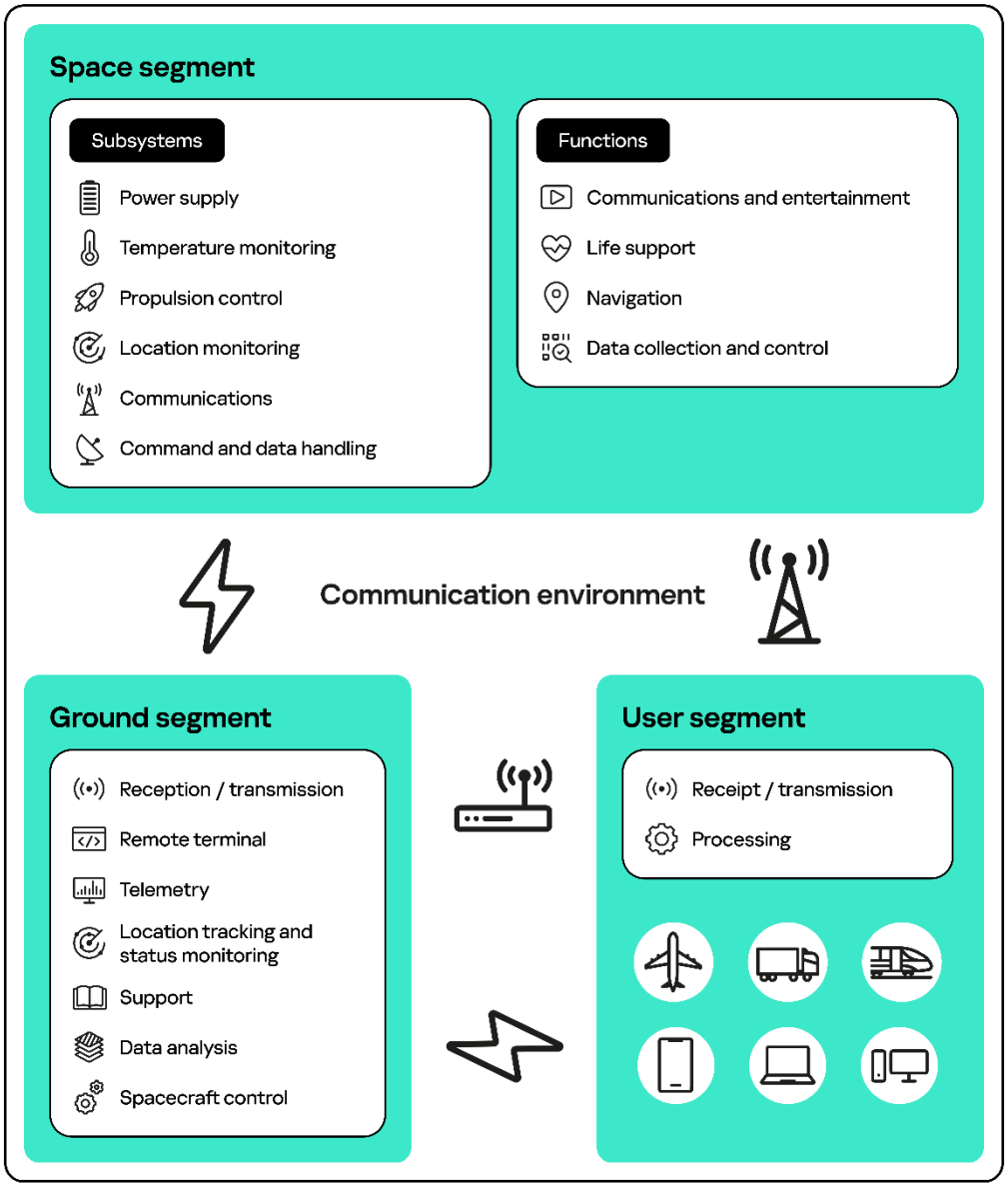

Figure 1. Space system

The space segment consists of spacecraft in orbit, with the system's positioning accuracy and operational stability depending on the relative positions of these spacecraft and the parameters of the signals transmitted by them. The ground (control) segment includes a network of ground stations used to control spacecraft and update information. The user (subscriber) segment comprises the receiving equipment of all system users, whether military services, commercial organizations, or individuals. In some cases (for

example, direct-to-home broadcasting), there is no ground segment, and the signal is transmitted directly to the user segment.

Below we outline the consequences of a security breach in a space system.

- Gain of control by a threat actor over a spacecraft, the ground segment, or a user device.
- Device denial of service.
- Theft of technology.
- Interception and planting of information, including the dissemination of messages to the broader public.
- Reputational damage for the vendor of the attacked system, and the public compromise of organizations using the system.

Modern space systems, primarily satellite systems, are part of critical infrastructure: many processes that directly affect everyday life depend on their operation. Below we list the potential consequences of a complete shutdown of satellite systems.

- Communication disruptions. Satellites are a key component of global communication systems. The failure of satellite system components leads to severe disruptions across all types of communications, including telephone, internet, and television networks. Communication degradation results in massive operational disruptions for businesses, power outages, the inability of emergency services to function, and ultimately, a negative impact on public safety and the well-being of the population.
- Navigation issues. Global Navigation Satellite System (GNSS) receivers provide accurate location information. Obviously, airplanes could fly, and ships could sail long before the advent of satellite navigation. Maritime vessels are still equipped with charts and navigation instruments, and aircraft can reach their destinations under the guidance of air traffic controllers. However, crews have grown accustomed to modern navigation tools; operating without GNSS is significantly more difficult, and safety suffers as a result. Road transport faces problems as well – today, it is difficult to imagine a trip without a GPS navigator. In addition, tracking and moving cargo becomes problematic, because logistics companies and customs services rely on navigation beacons.
- Difficulties with weather forecasting. Satellites play a critical role in monitoring weather conditions and collecting data used for meteorological forecasts. Without satellites, the ability to forecast severe weather events, such as hurricanes, tornadoes, and typhoons, and prepare for them on time, would be significantly diminished.

- Limited capabilities for scientific research. Satellites are widely used in research projects to monitor environmental conditions, study climate change, and track ocean currents. Without them, scientists would be limited in their ability to obtain data and expand scientific knowledge.
- Threats to national security. Many countries use satellites for military purposes, particularly for surveillance and reconnaissance. The loss of satellites could have severe consequences for national and global security: it could negatively impact intelligence gathering, disrupt the strategic balance of power, and lead to or exacerbate military conflicts.

All of this explains why space systems – and satellite systems in particular – are a significant target for attacks and attract the attention of threat actors.

Attacks on space systems

According to open-source information, slightly more than a hundred attacks on space systems were recorded between 1957 and the early 2020s. Researchers disagree on what exactly constitutes a cyberattack on a space system – whether to include jamming or spoofing signals from a ground station, traffic eavesdropping, or the use of user segment infrastructure by threat actors to conceal malicious activity. According to various sources, the number of incidents has lately reached thousands or tens of thousands of attacks per year; however, this figure directly depends on how the concepts of "space system" and "cyberattack" are interpreted.

The transparency of information on space incidents (those that were successfully detected) has increased over time – from rumors of attacks in the early days of space technology to detailed descriptions of some incidents today.

With this in mind, we will examine examples of incidents and trace the evolution of attacks on space systems. The dates in the timeline are approximate: they correspond to the developmental stages of the systems, with each stage featuring different incident causes, consequences, and actor motivations. These factors have evolved over time, and these very changes are the subject of our research.

1957–1979. Early stages of space system automation

When the USSR launched the world's first artificial Earth satellite, Sputnik 1, in 1957, no one knew of or even considered the concept of cybersecurity. The systems were analog. The most that could be done to protect data was to

ensure physical security. This involved using restricted "military" frequencies, encryption, and restricting personnel access to project data. The "threat model" included reconnaissance, surveillance, or attempts to interfere with radio communications, but no suspicion of such interference was ever confirmed. However, declassified CIA documents mention, among other things, US monitoring of the first automated docking of the uncrewed Cosmos 186 and Cosmos 188 spacecraft in 1967, as well as the activity of NATO radio intelligence stations in Norway.

Until the mid-1970s, all spacecraft were entirely analog, but errors in computerized calculations sometimes led to problems. In 1965, during the Gemini 3 and Gemini 5 missions, there were errors in landing point calculations. In both cases, the deviation amounted to about 100 kilometers: in the former, due to an error in calculating the capsule's aerodynamic characteristics, and in the latter, because a programmer set the Earth's daily rotation to 360° instead of the actual 360.98°. In both instances, the crew corrected the course as much as possible, but for uncrewed spacecraft, correcting such errors requires remote control (which is also helpful for crewed missions).

In the second half of the 1970s, gradual integration of digital systems into spacecraft began. Although intentional attacks on these systems were still a long way off, potential problems could be inferred from incidents involving operational failures. Software and control system issues, software update errors, and insufficient personnel competence plagued both NASA missions and the Soviet space program. The role of human error is particularly notable. During the Apollo 8 mission, an astronaut inadvertently entered a command that erased the computer's memory, causing the computer to determine that the inertial measurement unit was indicating an incorrect spacecraft orientation. The situation was corrected manually. During the Apollo 10 mission (described as a "dress rehearsal" for the lunar landing), the lunar module's abort guidance system was mistakenly switched from attitude hold to automatic control, triggering an unexpected roll of the module that also required human intervention to stabilize.

There were also irreversible errors, especially in later years, when the objectives of space exploration became more distant and diverse, and the fail-safe mechanisms were still not flawless. For this reason, we include the following examples in this chapter. In 1982, while updating the software of the Mars surface lander portion of the American Viking 1 spacecraft, an operator made an error in the command sequence, causing the spacecraft to lower its antenna and resulting in a permanent loss of communication.

On September 1, 1988, the Soviet uncrewed interplanetary station Phobos 1 failed to respond during a scheduled communication session. It was later

discovered that three days prior, an operator at the Mission Control Center in Yevpatoria had inadvertently omitted a single hyphen in one of the commands. All commands were supposed to undergo verification on a computer prior to transmission, but that day the computer was out of order. The operator bypassed protocol and sent the command without waiting for the malfunction to be resolved. This minor alteration in the command code activated an unused test sequence and disabled the attitude control thrusters, leading to a loss of solar tracking and, consequently, battery depletion. The spacecraft was lost.

Just the following week, on September 5, 1988, the crewed spacecraft Soyuz TM-5 narrowly avoided disaster. The cause was an outdated version of the Mir space station docking software loaded into the onboard computer: it had been intended for a previous mission. Following undocking from the station, the retrofire engines ignited seven minutes later than scheduled due to a software malfunction involving the infrared horizon sensor, forcing the cosmonauts to shut them down. A second attempt to ignite the engines, undertaken three hours later, lasted only six seconds. Computerized control prevented manual deorbiting of the spacecraft due to the initial engine shutdown. The engines were successfully restarted only after the spacecraft commander reprogrammed the control module mid-flight to ignore the first unsuccessful retrofire impulse. The program execution was then manually interrupted to prevent the jettisoning of the instrument-assembly module: without it, the cosmonauts would not have survived, as the descent would have been prolonged and they would have run out of air and electricity. Redocking with the station was also impossible, as the docking system had already been jettisoned. After essentially hacking the spacecraft's computer system and forcing it to switch to manual control, the cosmonauts spent an additional day in orbit and successfully deorbited and landed on September 7, on their third attempt.

Thus, the majority of known incidents were caused by the human factor: a lack of verification, a lack of redundancy, or the circumvention of procedures. However, there were also issues directly caused by software bugs. In 1981, the first test flight of the reusable transport spacecraft – the STS-1 Space Shuttle – was scrubbed just minutes before liftoff. This occurred in the presence of US President Ronald Reagan and on live television. The cause was a loss of synchronization during data exchange between the primary and backup computers. The issue lay in a bug that was difficult to detect in the later stages of development. The programs had been written and debugged; however, during the development of the complex Shuttle control software, which included redundancy and recovery capabilities, modifications were made to the standard onboard computer platform regarding the use of the primary computer's operating system queue timer. Because of these changes – specifically, the initialization of certain subroutines prior to the primary

computer's first process – the scheduled initialization of the first process occasionally fell in the past and was postponed by the operating system by one cycle in accordance with the scheduler algorithm. With a probability of 1 in 67, this led to a loss of synchronization between the primary and backup computers: the primary computer's queue timer was used to clock all processes on all computers, while processes on different computers executed at varying times relative to this timer. The issue was not detected during integration testing, and it occurred on the day of the Shuttle launch.

Thus, the early stage of space system automation is characterized by the following takeaways:

- Even a minor error in a digital control system can lead to disastrous consequences.
- Incidents are more frequently linked to the human factor (the absence, circumvention, or overriding of verification procedures) rather than to code errors – and the consequences of such incidents are more severe.
- Incidents demonstrated that redundancy and automatic recovery capabilities are essential for autonomous systems.
- The capability for flexible configuration, as well as the emergency and reliable updating of both crewed and uncrewed assets, is critical when responding to unforeseen circumstances.

1980–1989. Commercialization of space technologies

In the 1980s, personal computers and satellite television became part of everyday life, and satellites began to be used for the benefit of the civil sector. The consumer base for space technologies expanded. By that time, space systems had become predominantly automated and computerized, making them accessible targets for information security threats, while the inevitable commercialization of the technologies provided a motive for attacks.

In this section, we will examine attacks on the ground and user segments of US space systems. These attacks were driven, among other factors, by a conflict of interest between commercial companies and technology users. The primary goal of these attacks was to publicize the hack itself and broadcast a public message. They are similar, for example, to the website defacement attacks that emerged later on the internet, and were provoked by the fact that US legislation was evolving alongside technological developments to protect the interests of commercial companies – a shift that consumers viewed as unfair.

At the same time, the attacks described above were not the only type of incidents in the 1980s. Attacks aimed at intercepting, jamming, and spoofing

information appeared at the same time as satellite data transmission. According to open-source data, in 1986 Indonesia became the first state accused of violating satellite eavesdropping rules, and in 1996, it was the first to intentionally use a satellite to jam the signal of another satellite. However, incidents related to state signals intelligence (SIGINT), electronic warfare (EW), and the space race fall outside the scope of this article, as it is often impossible to distinguish reliable facts from assumptions and speculation in publicly available materials on these topics. Therefore, we will limit our discussion strictly to attacks on commercial systems intended for civil applications.

The Captain Midnight attack on the Home Box Office (HBO) satellite broadcast is likely one of the first widely known acts of hacktivism. To understand the motive behind this attack, we must look at the history of the development of satellite television technology in the 1970s and 1980s. In the late 1960s and early 1970s, satellite television broadcasting systems were designed so that the satellite signal could only be received by receiving stations of cable operators, which in turn sold channel subscriptions to their customers. However, in 1976, former NASA employee Henry Taylor Howard, out of personal interest, assembled an equipment kit in his garage that allowed him to directly receive the satellite signal intended for television operators' receiving stations (this technology was later called Direct-to-Home, or DTH). He tested the new method and even sent HBO a check for the content he received; however, neither the check nor the invention itself attracted the company's interest. In 1980, Henry Taylor Howard and Robert Taggart founded Chaparral Communications to manufacture and sell equipment for viewing satellite television. The equipment allowed users to watch multiple channels from several providers without subscription fees, with image quality superior to that of cable network transmissions. Furthermore, it could be used in remote areas where cable operators' services were unavailable. Consequently, despite the high cost of the equipment, the company's business took off rapidly. In the early 1980s, the majority of viewers watched satellite television channels without paying provider fees. Dealers selling satellite TV receiver antennas sprang up across the country – it was a highly profitable business. One such dealer was John MacDougall, who later became famous as Captain Midnight.

HBO, founded in 1972 and a pioneer in satellite television broadcasting, had overlooked DTH technology but had no intention of accepting the loss of its subscriber base that had stopped paying for viewership. Alongside other companies, HBO successfully lobbied for the Cable Communications Policy Act of 1984, which secured cable operators' right to scramble their transmitted signals. Just two years later, HBO implemented signal scrambling, after which sales of equipment for the illegal viewing of premium satellite channels plummeted, and John MacDougall, like many other dealers, lost his income.

Around that time, he took a job as an operations engineer at Central Florida Teleport, a company engaged in uplinking data to satellites. Around midnight on April 27, 1986, following the end of his shift – during which he had maintained a movie broadcast for the People's Choice network – John MacDougall repositioned the antenna in accordance with protocol. Supposedly by accident, the antenna ended up pointing at a satellite one of whose transponders was broadcasting for HBO. John knew the satellite's coordinates and transmission frequencies from publicly available manuals and enthusiast magazines. Acting impulsively, according to his own account, he generated a television graphic – a message for HBO – adopted the pseudonym Captain Midnight, and initiated transmission at high power. John overrode the movie broadcast with the following message: "Good evening HBO from Captain Midnight! $12.95 a month? No way! (Showtime/Movie Channel beware!)." The HBO viewership at the time of the interrupted broadcast was approximately 14.6 million people.

Figure 2. The message that HBO viewers saw while watching the thriller "The Falcon and the Snowman" late at night on April 27, 1986

For a minute or two, John MacDougall and the HBO engineer engaged in a duel to increase signal power; however, the engineer gave up, fearing damage to the satellite, after which John ceased his transmission.

The notion that this act was spontaneous is contradicted by the fact that a week earlier, John MacDougall had already interfered with an HBO broadcast – albeit without any message, simply by transmitting a test card. On July 22, 1986, he appeared before a federal court, which sentenced him to one year of probation and fined him $5,000.

John MacDougall became a hero in the eyes of many satellite antenna and satellite television vendors. The Captain Midnight Grassroots Coalition was formed in his support, whose spokesman Donald Cochran stated, "While there are those who consider Captain Midnight a criminal for his unauthorized transmissions, there is another group made up of home satellite dish owners, small business people, and rebels, who support his actions as a non-violent and non-destructive protest in the best American tradition."

John MacDougall was convicted under 47 U.S.C. §301, "License for radio communication or transmission of energy," although the application of this statute in this particular case appeared legally questionable. Representatives of the satellite industry, concerned about the potential for increased interference and the risk of satellite damage due to input overload, urged Congress to pass new criminal legislation, which became 18 U.S.C. §1367, "Interference with the operation of a satellite." A year later, this legislation was used to convict and sentence Thomas Haynie, a satellite communications technician at the Christian Broadcasting Network (CBN) in Virginia Beach, to probation. In September 1987, he overrode the broadcasts of the American Exxxtasy Channel and Playboy TV with text messages urging viewers to repent and heed the word of God. The hacktivists made little effort to hide: maximum publicity only helped them achieve a greater impact.

Alongside ideologically motivated incidents, there were also acts of outright vandalism. Among these was the Max Headroom incident – an act of television signal hijacking in Chicago on November 22, 1987. Unlike his predecessors, the hacker did not broadcast text messages but rather a video recording in which he appeared wearing a mask of Max Headroom, a character from the 1985 film of the same name. The incident comprised two episodes. The first occurred on WGN-TV at 9:14 PM: during the broadcast of a sports news segment, the signal suddenly dropped, and nine seconds later, a person wearing a Max Headroom mask and sunglasses appeared on the screen, twitching in different directions. The second episode occurred the same evening on WTTW at 11:15 PM, during a broadcast of the Doctor Who series. For a minute and a half, the threat actor broadcast outrageous video footage that elicited a mixed reaction from viewers: it upset and even frightened some, while amusing others. Law enforcement agencies never managed to identify who was behind the attack. Shortly after this incident, the Chicago channel WMAQ-TV intentionally

inserted the scandalous video recording during a sports news broadcast and received a barrage of messages inquiring about the hack. This provided the channel with what would be called viral marketing today.

An incident that naturally fits into this sequence of events was brought to light by a story published in the New York Times on September 16, 1987. The article reported that a group of West German computer enthusiasts had breached NASA's international computer network and rummaged freely through the data for at least three months before being detected. The Hamburg-based organization Chaos Computer Club, which claimed to be speaking on behalf of the anonymous group that breached the network, stated that the attackers had installed a Trojan that enabled them to bypass security procedures and gain access to 135 computers on the network. The network in question was the Space Physics Analysis Network, intended primarily to provide authorized scientists and organizations with access to NASA data. The network's security system was provided by an American company, Digital Equipment Corp. According to both users and official NASA representatives, the network was widely used by scientists in the US, UK, West Germany, Japan, and other countries, and did not transmit classified information. NASA explained that the purpose of the network was to provide easy access to unclassified data, and that any individual or organization engaged in NASA-related research could apply for access. The potential damage from the threat actors' activities could have involved the modification or destruction of information; however, Chaos Computer Club representative Wau Holland denied reports of any data modification, characterizing such actions as contrary to the hacker ethic. It should be noted that at the time, the word "hacker" referred to an amateur computer enthusiast, not a threat actor causing harm.

Thus, in the 1980s, ordinary threat actors began attacking space systems. The motives during that period included self-assertion, propaganda, and piracy in a relatively noble sense of the word. However, it was only a matter of time before they began to profit from intentionally inflicting damage.

1990–1999. Computerization of space systems

In the 1990s, threat actors seeking to gain access to television broadcasts fully focused on decoding satellite television channel signals. Although this can be classified as attacks on the user segment of space systems, there was nothing distinctly "space-related" about this activity. The primary attack vector involved installing a decoder on the TV signal receiver; the decoder could, for example, spoof the provider's official smart card containing valid keys for viewing television channels, or connect to a computer to dynamically decrypt a recorded television broadcast signal. One of the pioneers of this type of

hacking was Markus Günther Kuhn, known as the inventor of the Season7 decoding device, which gained widespread popularity in the early 1990s. In an open letter dated May 23, 1996, addressed to the European Commission, which had held a hearing on "Legal Protection for Encrypted Services in the Internal Market – Consultation on the Need for Community Action" on March 6 of that year, Markus Kuhn stated that he used his decoder not for commercial gain or to view paid content, but exclusively to watch television channels that the official German provider did not decrypt: these channels were not prohibited, but they remained inaccessible for viewing. Markus Kuhn's list of publications confirms that he is, in fact, a researcher and scientist. Naturally, pirates fully exploited both his work and the research of others for their own commercial gain.

Attacks on ground segment systems can also have other objectives: gaining unauthorized access to information, source code, and control functions for the purpose of extortion, or even attempting to influence space missions. It is precisely this area that interests the general public. However, by no means do all claims regarding hacking incidents or their consequences receive unequivocal confirmation.

Speculations about a hack of the ROSAT X-ray observatory's control system spread widely across the internet and are still published as confirmed facts today. The satellite, launched in 1990, was equipped with a German-made X-ray telescope, an American high-resolution imaging instrument, and a British telescope for extreme ultraviolet observations. The combination of such equipment provided extensive capabilities for observing and studying the entire celestial sphere.

Initially, the international mission was slated to last 18 months; however, active operations continued for over eight years, during which the system discovered more than 150,000 predominantly unknown X-ray sources. The failure of a star sensor in 1998 caused the telescope to "look" directly at the Sun, resulting in severe damage (most likely solar panel failure). The ROSAT satellite conducted its final astronomical observation on December 17, 1998; it was powered down on February 12, 1999, and deorbited on October 23, 2011. In 2008, a theory surfaced in the news and on the blog of the well-known cybersecurity expert Bruce Schneier that the sensor failure was caused by a cyberattack on the Goddard Space Flight Center: allegedly, threat actors, after gaining access to the code, were able to reposition the solar panels in such a way that they were destroyed. NASA experts subsequently refuted this theory, although they did confirm there had been an instance of unauthorized access to the Goddard network in 1998. To quote: "In 1998 there was an intrusion of some kind into the NASA-Goddard network which contained the source code for the flight

software of several NASA satellites. According to the author of the report, 'exploitation of the comm link could not be ruled out' – presumably the fear was that someone could use knowledge of the code to use their own ground station to command a satellite, or separately hack in to the NASA ground station. But despite the report, this just can't have happened with ROSAT... all we had were copies of the downlinked science data. All commanding, scheduling and operations of ROSAT were done from Germany at GSOC – NASA had no role in the spacecraft commanding. ROSAT was an elderly satellite in 1999, its main mission long completed. Its failure is not surprising and is fairly well understood."

At the same time, it remains unclear whether we are dealing with speculations on "Russian hackers" (who were specifically blamed for the ROSAT failure) or with the concealment of the consequences of a supply chain attack. We are unlikely to ever know the answer to this question, although the incident continues to be widely discussed. The incident involving the takeover of a British Skynet satellite features just as frequently. The Skynet network provides support for the strategic and tactical nuclear forces, as well as the United Kingdom's naval, air, and land forces. The country's Ministry of Defence describes the network as "essential to support all aspects of modern military operations." In early 1999, British aerospace authorities noticed an irregularity in the position of a military communications satellite, one of four spacecraft in the Skynet family. They soon received an anonymous message demanding a ransom in exchange for control over the satellite's positioning systems. This case is cited in many sources as a significant early example of space terrorism and satellite hacking.

The UK Ministry of Defence did not acknowledge the incident. Moreover, an analyst from a publishing house specializing in military issues refuted the technical feasibility of hacking the command-and-control link. He stated that in order to execute an attack by overpowering the control signal with a stronger one (a jamming attack, as in the Captain Midnight case), threat actors would need a "very, very high-powered transmitter, and someone would have detected that." A "man-in-the-middle" attack is also difficult: unlike radio waves, which propagate in all directions, the microwaves used form a "narrow" beam that spreads by only three centimeters for every 10,000 kilometers traveled. Furthermore, the locations of the transmitting stations mean that intercepting and altering the signals would require building a tower in south-west London. There remains the theoretical possibility of a direct attack on the control systems, but the analyst asserted that "You cannot get in unless you... are at one of the Ministry of Defence's sending locations. The only way in would be through the American system during a time of war, but this is not a time of war" and that "the UK system is much better [than the American one] as it is

absolutely stand alone." There is obviously a great deal of speculation and emotionally charged denial of the very possibility of an attack in these statements. Nevertheless, plausible scenarios such as an insider attack and the imperfect isolation of the control systems, which could have led to their compromise, should not be ruled out. However, the general public is unlikely to ever be told about this.

It turns out that based on available information, the attacks on space systems in the 1990s can neither be confirmed nor refuted. At the same time, certain things can be stated with certainty.

Attacks on the user segment, especially in the realm of satellite television, began to bring financial gain to threat actors. This provided an impetus for the development of commercial cryptographic protection tools, albeit a rather modest one: the need to ensure backwards compatibility of technologies, to comply with legislative requirements, including export restrictions, and the scalability requirements for solutions remained limiting factors.

Attacks on the ground segment were conducted and were successful; however, the actual consequences and damage, as well as the incidents themselves, were suppressed whenever possible. Nevertheless, some incidents subsequently became grounds for political speculation.

The threat of cyberattacks in the space industry began to gain weight, yet ensuring cybersecurity was still not a top priority: the industry itself and the state of the space race did not always leave resources and time for identifying and fixing vulnerabilities in systems.

2000–2009. The politicization of attacks

In the 2000s, the dissemination of political statements and interference in information and propaganda channels became the objective of many attacks. In addition, first attempts were made to interfere with the operation of uncrewed systems and attack spacecraft control systems connected to the internet.

Just as in the 1980s, several jamming attacks on satellite television occurred at the same time – these were also hacktivist in nature, but were politically motivated. In 2002, political and religious activists (some of the organizations associated with them are recognized as undesirable and extremist in the Russian Federation) repeatedly intercepted the signal of the SinoSat satellite, interrupted the broadcasting of China Central Television and the China Education Television channel, and broadcast opposition videos and messages over the air. Chinese authorities stated that the presumed source of the signal

was located in Taiwan, and the Taiwanese government did not immediately respond to this accusation. The incidents were followed by mass arrests of the activists' supporters. Dozens of individuals convicted of various episodes of intercepting the television signal for broadcasting videos were sentenced to up to 20 years in prison.

A similar incident occurred in early 2007 in Sri Lanka. The Liberation Tigers of Tamil Eelam (LTTE), recognized as a terrorist organization by many countries, used one of the transponders on a satellite belonging to the major communications operator Intelsat for unauthorized television and radio broadcasts to the US and Europe. Resolving the incident required international cooperation: the Sri Lankan ambassador was forced to appeal to US officials. By late April 2007, Intelsat confirmed that it had successfully disabled the Tamil Tigers' ability to use its facilities, thereby disrupting the group's propaganda operations. This action was part of a broader campaign to counter the LTTE's logistics during the final stages of the Sri Lankan Civil War, often referred to as Eelam War IV.

Interference with broadcasting (jamming attacks) was practiced not only by rebels but also by authorities. In 2009, during elections in Iran, the government not only banned the operation of the BBC's Persian-language television and radio service but also took active technical measures, including powerful jamming of the satellite signals for BBC Persian and BBC World News, as well as the blocking of the bbcpersian.com website.

Such attacks are not technically complex: they merely require access to the equipment. In general, during the 2000s, the issue of resilience and information security was not a top priority unless it involved direct commercial profit from broadcasting. The following example provides clear evidence of this.

In 2009, in Iraq, insurgents used software to intercept live video feeds transmitted from satellites to American Predator drones (and, according to some reports, Reaper drones). This enabled them to obtain the information needed to evade US military strikes or to conduct surveillance. The shareware SkyGrabber product, licensed at a mere $26, was widely used in the late 2000s to passively intercept data from satellites, including movies, music, images, and other content downloaded by other users. In essence, it was a network packet analyzer and sniffer – the data channel between the satellite and the ground station, which was accessed by the program, was unencrypted, making it difficult to even call such an interception a hack.

The interception was discovered by US military personnel in Iraq when they apprehended a Shiite militant whose laptop contained files of drone video feeds. Several months later, similar files were found on the laptops of other

insurgents, leading to the conclusion that the interception of data by militant groups was systematic. The lack of encryption during data transmission from military drones was subsequently attributed to the limited time available to deploy the drones, as well as the fact that the manufacturer had patented some of the communication technologies used, making common encryption systems incompatible with those technologies. According to some officials, the US government had been aware of this vulnerability since the American campaign in Bosnia in the 1990s, but the Pentagon assumed that adversaries would not be able to exploit it. Nevertheless, the issue was acknowledged as a vulnerability and was subsequently addressed.

However, it cannot be said that the issue of space system security was ignored. In an article from October 28, 2011, Bloomberg News, citing a draft report by the US-China Economic and Security Review Commission, stated that in 2007–2008, a NASA ground station in Norway repeatedly recorded prolonged interference with the operation of the Earth observation satellites Landsat-7 and Terra AM-1. "A Landsat-7 earth observation satellite system experienced 12 or more minutes of interference in October 2007 and July 2008. Hackers interfered with a Terra AM-1 earth observation satellite twice, for two minutes in June 2008 and nine minutes in October that year," the draft said, citing a closed-door US Air Force briefing. In the final report, specific incidents are no longer mentioned, but it is stated that "China has developed the capability to wage cyber warfare and to destroy surveillance satellites overhead as part of its tactical, asymmetrical warfare arsenal. With its highly developed reliance on systems of command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR), the American military is significantly exposed to such attacks." Chinese officials denied this information, stating that "this report is untrue and harbors ulterior motives."

At the same time, by no means did all incidents have a political subtext or result from targeted attacks. The widespread proliferation of malware in the 2000s also affected random systems that later ended up in space. For example, laptops delivered to the International Space Station (ISS) in July 2008 were found to be infected with a computer worm known as W32.Gammima.AG. The cosmonauts used these laptops for email correspondence, and they lacked any security solutions. The malware, most likely introduced via an infected removable drive, was designed to steal online game passwords and did not cause damage to ISS systems. According to a NASA statement, malicious programs had "traveled" to space before, although this occurred infrequently.

2010–2019. Further growth and increasing complexity of attacks

In the 2010s, attacks on drones utilizing the satellite communication link as an attack vector evolved further. In 2011, the American RQ-170 Sentinel drone was brought down in Iran instead of landing at its American base in Afghanistan. An Iranian engineer involved in reverse-engineering the hacked drone stated that the Iranian side had managed to exploit a known GPS vulnerability to alter the landing coordinates: the Sentinel mistook a location in Iran for its base in Afghanistan.

It is noteworthy that in April 2011 alone, the US Air Force Scientific Advisory Board published a "Report on Operating Next-Generation Remotely Piloted Aircraft for Irregular Warfare", which contained an assessment of the reliability of the communication link between the drone and the ground control station. According to the document, American drones face the following threats (excerpt):

- Jamming of commercial satellite communications (SATCOM) links is a widely available technology. It can provide an effective tool for adversaries against data links or as a way for command and control (C2) denial.
- Operational needs may require the use of unencrypted data links to provide broadcast services to ground troops without security clearances. Eavesdropping on these links is a known exploit that is available to adversaries at an extremely low cost
- Spoofing or hijacking links can lead to damaging missions, or even to platform loss.

The document, which addresses countermeasures against threats to positioning, navigation, and timing, emphasizes that “There is a wide range of methods that a determined adversary can use for attacking RPA guidance and navigation systems.

- Small, simple GPS noise jammers can be easily constructed and employed by an unsophisticated adversary and would be effective over a limited RPA operating area.
- GPS repeaters are also available for corrupting navigation capabilities of RPAs.
- Cyber threats represent a major challenge for future RPA operations. Cyber attacks can affect both on-board and ground systems, and exploits may range from asymmetric CNO attacks to highly sophisticated electronic systems and software attacks.”

The cybersecurity of satellite systems began to receive significantly more attention. For instance, in 2013, the US initiated an internal IT security audit of the National Oceanic and Atmospheric Administration (NOAA), which manages the Joint Polar Satellite System (JPSS). A memorandum from 2014 reported numerous security vulnerabilities classified as "high-risk" within the JPSS ground system. Over 9,100 vulnerabilities were linked to outdated or improperly configured software. More than 3,600 security policy violations were identified, including password issues. It was specifically noted that three vulnerabilities, which had been identified during a penetration test as early as 2012, still remained unpatched by 2014. However, in its response letter, the agency reported on the measures taken and confirmed that even the Heartbleed vulnerability – which only became publicly known in April 2014 – had been remediated.

Attacks on satellite communication operators were executed as part of numerous cyberespionage campaigns. One example is Icefog, launched no later than 2011, whose victims included government organizations, military departments, defense contractors, shipbuilding firms, telecom and satellite operators, industrial and high-tech companies, as well as media outlets, predominantly in South Korea and Japan.

The quantitative growth and qualitative increase in the complexity of attacks in the 2010s naturally affected the sphere of satellite technologies, which cybercriminals began using increasingly to their advantage.

For example, some advanced APT groups circumvented the problem of domain and malware command-and-control (C2) server takedowns by shifting to satellite internet channels to mask their campaigns. The C2 servers of the HackingTeam, Xumuxu, and Rocket Kitten APT groups were spotted on satellite internet IP addresses. However, the most interesting and unusual of these was the Turla group. It breached several DVB-S satellite internet providers, the majority of which provided downstream internet links to the Middle East and Africa. Executing such attacks requires relatively affordable equipment: a satellite dish (the size of which depends on geographic location and the specific satellite), a low-noise block downconverter (LNB), a dedicated DVB-S satellite tuner (PCIe card), and a computer running a Linux OS. Unlike two-way satellite internet, downstream internet links are used to accelerate downloads: they are inexpensive, simple to install, and lack encryption. This creates opportunities for their malicious exploitation.

The threat actors monitored unencrypted traffic transmitted over the downstream satellite link to identify actively used IP addresses. These IP addresses were then specified in the malware's configuration, so that following a successful infection, all of the victim's data would be sent to those

addresses. Upon detecting a call from the malware in the traffic, the C2 server would send a response via standard, inexpensive terrestrial, communication links using a spoofed IP address. This was essentially a man-in-the-middle attack, and in many cases, there was no need to suppress the response of the legitimate IP address owner: a packet arriving at a closed port would most likely be dropped by the firewall (which is a best practice for slow links).

Researchers noted that the method described above is easy to implement and provides a higher level of anonymity compared with conventional methods, such as renting a virtual private server or compromising a legitimate server. The only limitation is the requirement to be located within the satellite internet provider's coverage area. Researchers expressed concern that financially motivated cybercriminals might adopt this method, but apparently, this limitation proved to be a significant deterrent (or such instances simply remained undetected).

In 2017, the operations of another APT group named Whitebear, which had ties to the Turla group, were described. As with Turla, infrastructure was built using compromised websites and hijacked satellite connections.

In 2018, Symantec analysts reported discovering a cyberespionage campaign by the Thrip group targeting satellite, telecommunications, and defense organizations. The company's blog noted that "Thrip had targeted a satellite communications operator. The attack group seemed to be particularly interested in the operational side of the company, looking for and infecting computers running software that monitors and controls satellites." This led researchers to suspect that the attackers' motives extended beyond espionage and might have included the intentional disruption of system functionality. Another target of Thrip was an organization specializing in geospatial imagery processing and mapping. Computers running MapXtreme Geographic Information System software – designed for developing custom geospatial applications and integrating location data into other applications – were attacked. Computers running Google Earth Server and Garmin imaging software were also targeted. Technical details of the attack, promptly reported by news agencies, led researchers to conclude that threat actors from China were behind it.

In a study dated 2019, Symantec analysts reported on ongoing attacks by the presumably Chinese group against satellite communication operators in Southeast Asia.

Overall, the 2010s were characterized by an increase in the number of attacks, including those on space systems. The trend toward maintaining secure IT infrastructures intensified, particularly in the public sector. Nevertheless, skilled

threat actors continued to discover both attack vectors into systems and methods for exploiting technologies for their own benefit.

2020–2024. Modern attacks

In the early 2020s, space systems became even more popular targets among cybercriminals. The evolution of attacks proceeded in line with general trends: supply chain attacks, espionage and cyber extortion in the user segment of space systems, signal jamming and spoofing attacks, and infiltration of the communication links of the satellite systems' ground segment. Attacks can be highly targeted. For example, in 2024, researchers from Proofpoint identified a targeted campaign distributing emails that affected fewer than five organizations – Proofpoint clients in the United Arab Emirates associated with aviation and satellite communications, as well as critical transportation infrastructure.

The malicious messages were sent from the email address of a compromised organization that had an established, trusted business relationship with the targets, and customized lures were used for each victim. A new backdoor named Sosano was discovered during the investigation of this campaign.

In the user segment, cyberattacks also directly affected service consumers. Notably, attacks on devices in the user segment may not be directly related to space technologies. For example, the vulnerability of Starlink Wi-Fi routers to a CSRF attack (CVE-2023-52235, CVSS score 8.8) could just as easily exist in network equipment unrelated to satellite communications technology. Nevertheless, the damage caused by attacks exploiting such vulnerabilities can be greater than in networks connected to the internet via other technologies. Satellite internet is expensive and is typically used in areas with few or no alternatives. Therefore, the failure or malicious reconfiguration of satellite communication devices entails elevated risks – primarily the unavailability or prolonged downtime of isolated systems and infrastructures.

A vivid example is provided by an incident that occurred in early 2022, when a cyberattack affected more than 5,800 wind turbines with a combined capacity of over 11 gigawatts. Enercon notified the German cybersecurity regulator BSI about the incident and contacted satellite communication providers to resolve the outage, which, according to Enercon's data, affected around 30,000 satellite terminals used by organizations across various sectors throughout Europe. The regulator publicly confirmed a malfunction of equipment at one of the satellite communication operators that limited the ability to conduct maintenance on some wind turbines, though it disclosed no further details. It later became known that the cause of the outage was a cyberattack on the

satellite communications operator Viasat, which provides broadband access for private users in Ukraine and across many European countries.

It was revealed that the initial attack vector was a misconfigured VPN device that threat actors used to gain remote access to the KA-SAT network. After moving laterally through the network, the attackers exploited vulnerabilities in home modems – specifically, according to the operator, they "overwrote key data in flash memory on the modems, rendering the modems unable to access the network, but not permanently unusable." The network remained offline for several days. Analysts at SentinelOne hypothesized that the threat actors leveraged the KA-SAT management mechanism via a supply chain attack to distribute wiper malware targeting modems and routers. Such malware overwrites key data in the modem's flash memory without rendering it completely inoperable and in need of replacement. The attack and the malware were named AcidRain. In 2024, research was published on the next generation of this malware – the destructive AcidPour wiper. Unlike its predecessor, which targeted specific models of satellite communication modems, AcidPour targets a broader spectrum of devices, including Linux-based routers and satellite internet modems, as well as data storage arrays. AcidPour has been linked to the Sandworm APT group.

Attacks on the Global Navigation Satellite System (GNSS) receivers have become widespread in the user segment. GNSS is an umbrella term referring to any satellite-based positioning, navigation, and timing (PNT) system that provides the relevant information to receivers. A GNSS conforms to the diagram presented at the beginning of the article and similarly consists of three segments: the space segment (satellite constellations), the ground segment (ground control stations, monitoring stations, and ground antennas for data transmission), and the user segment (consumer devices ranging from smartphones to receivers on aircraft and maritime vessels).

In 2023, the international civil aviation incident and event information-sharing group OpsGroup reported a sharp increase in GNSS signal spoofing incidents in the Black Sea region, which in a number of cases compromised aircraft navigation. The reports cited false and jammed GNSS signals affecting civil GPS signals; as a result, aircraft navigation systems displayed inaccurate location information or no information at all. In the worst cases, the consequences were extremely severe: the complete loss of onboard navigation, the failure of the inertial reference system, and undetected deviation off course toward hazardous areas and hostile airspace.

One such attack vector is the exploitation of ground GNSS receivers that are available over the internet and contain known or new vulnerabilities. A study by Kaspersky examines the primary preconditions for and examples of attacks on

internet-exposed GNSS receivers. At least two hacktivist groups conducted such attacks in 2023. In May, the hacktivist cybercriminal group SiegedSec gained access to satellite receivers in Colombia in response to the country's authorities' arrest of a hacker. Later, in mid-2023, the same group attacked the devices of several US organizations and claimed to have gained access to satellite receivers in Romania. Another group actively targeting satellite receivers in 2023 was GhostSec. Over the course of the year, it attacked numerous GNSS receivers across various countries, including Russia and Israel. The attackers claimed that in some of the attacks, they not only gained access to satellite receivers but also deleted data from the compromised devices, demonstrating the potential damage that such incidents can cause. Kaspersky researchers analyzed data on vulnerable GNSS receivers in collaboration with 70 vendors of receivers used worldwide. It was revealed that more than 3,000 receivers are vulnerable to internet-based attacks.

Attacks on the GNSS ground segment make things difficult for transportation that relies on GNSS data and services. The inability to determine an aircraft's location complicates separation and airspace positioning, making it more difficult for the crew to plan the flight and make decisions. Using multiple satellite systems (GPS, Galileo, GLONASS) can mitigate the spoofing of one of them, but it will not help against signal jamming.

In conclusion, over the past decade, a multifaceted confrontation has unfolded in the segment of cyberspace responsible for the operation of space systems. It involves both state-sponsored hacking groups and individual hacktivists. Complex supply chains introduce additional risks and complicate the allocation of organizational responsibility for ensuring security.

Conclusion

Looking at incidents at the dawn of the space age, we should speak not of cyberattacks, but rather of technical incidents involving space systems. Even then, it was evident that a minor bug could cause the most severe consequences, that the human factor was the root cause of many unfortunate incidents, and that well-established processes and their oversight were not a whim, but a necessity for preventing and mitigating the negative impact of errors and omissions during the development and operation of systems.

The use of space systems in the civil sector – primarily to provide communication and entertainment services – led to the emergence of the first threat actors. Initially, attacks were hacktivist in nature, but they soon became commercialized. One cannot speak of any significant diversity in attacks during

that period; however, the confrontation between satellite television operators and pirates already revealed many issues relevant to modern information security: the denial and suppression of incidents, the desire to solve a technical problem within the legal and organizational domain, the emergence of vulnerabilities in commercial technologies driven by the desire to quickly sell a product or service, and the "arms race" in the realm of signal scrambling and code breaking.

Cyberattacks on space systems, which emerged alongside internet technologies, evolved in parallel with them. Today, space systems have in many cases become a single point of failure for critical systems and infrastructures. State-sponsored APT groups have long shown an interest in satellite systems, both in terms of interfering with their operations and leveraging them for their own purposes. The proliferation of space technologies makes them attractive to financially motivated cybercriminals as well.

The field of space system cybersecurity still almost entirely lacks a regulatory and legal framework, causing uncertainty regarding applicable measures and controls. There is no single comprehensive treaty dedicated to cybersecurity in space. Instead, there is a set of principles derived from general international space law, UN resolutions, and the norms governing cyberspace on Earth. Thus, international legislation in the field of information security in space resembles a “patchwork quilt” woven from the principles of general space law, applicable norms of international cyber law, and emerging “soft law.” Currently, the primary focus is not on creating a new treaty, but rather on detailing and adopting, by consensus, norms of responsible behavior designed to mitigate the risks of cyber conflicts in space – though these are unlikely to deter motivated threat actors.

***

Information from this article was partially presented in the lectures “Histories of Space Missions through the Prism of Information Security” and “Security of Satellite Communication Systems” at the Museum of Cosmonautics, as part of a partnership agreement between the museum and Kaspersky.

Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT) is a global Kaspersky project aimed at coordinating the efforts of automation system vendors, industrial facility owners and operators, and IT security researchers to protect industrial enterprises from cyberattacks. Kaspersky ICS CERT devotes its efforts primarily to identifying potential and existing threats that target industrial automation systems and the industrial internet of things.

Kaspersky ICS CERT ics-cert@kaspersky.com