Protecting Satellites: Learning from the Past to Secure the Future

Abigail C Teron; Dr. Luis Vicente
Polytechnic University of Puerto Rico
abigailteron@gmail.com; lvicente@pupr.edu

Abstract

Satellites are indispensable to modern society, underpinning critical functions such as communication, navigation, weather forecasting, and military operations. However, their increasing significance has rendered them prime targets for cyberattacks. In this investigation, we shall examine how cyber threats to satellites have evolved over time, analyzing pivotal incidents, their repercussions, and the broader implications for satellite security and national defense.

Commencing with early vulnerabilities in satellite communication protocols, this study explores key historical events, including signal jamming, unauthorized access to command-and-control systems, and the deployment of targeted malware. Through rigorous case studies, we highlight how state-sponsored adversaries and other malicious actors have exploited weaknesses—such as insufficient encryption and insecure data links—to inflict service disruptions, financial losses, and threats to national security.

As technological advancements drive towards greater satellite interconnectivity, their attack surface correspondingly expands, amplifying their susceptibility to cyber threats. We underscore the pressing necessity for resilient satellite architectures and advanced cyber defense strategies. Lessons drawn from historical incidents underline the efficacy of adopting zero-trust architectures, implementing robust encryption standards, and employing sophisticated anomaly detection systems.

By understanding the evolution of satellite cyberattacks, we shall foster improved preparedness for future challenges. This analysis seeks to inspire engineers, researchers, and policymakers to prioritize the fortification of cybersecurity measures, ensuring the protection of these vital systems in an increasingly contested space domain.

Keywords: Cyberattacks, Satellites, Satellite Security, Signal Jamming, Malware, Space Systems

Introduction

Since the first launch, satellites have become integral to modern life. No longer just silent objects orbiting above, satellites now broadly connect people, power economies, support defense operations, and help keep societies running reliably for everyone. They back each of the 16 critical infrastructure sectors identified by the Cybersecurity & Infrastructure Security Agency (CISA), and eleven of those sectors heavily depend on their secure and reliable operation (CISA, 2024; Georgescu & Botezatu, 2016). These include essential services such as communication, defense, energy, finance, healthcare, transportation, and more. Without satellites, the world would face widespread disruptions—from faulty GPS navigation and impaired emergency responses to compromised financial systems that threaten national security.

Satellites, regardless of their actual value, are rarely immune. Over time, cyber threats have evolved onto and multiplied at targeting satellite systems through jamming, spoofing, data interception, and unauthorized access. Every sector of our critical infrastructure has been affected by it greatly. Even when some infrastructure fields use satellites less, like chemical or nuclear fields, their small use still makes them prone to possible dangers.

Since 1985, when the first satellite cyberattack occurred, such attacks have gradually become more advanced. Several of the same vulnerabilities exploited decades ago remain highly exploitable today. These

exploitable vulnerabilities reveal deep gaps within space system cybersecurity. As satellite networks grow increasingly larger and linked, potential damage of a single breach vastly multiplies.

This paper focuses upon documented cyberattacks targeting the satellite system at the space segment, not on ground segment. While several of the incidents remain classified, the ones publicly known already depict the scale and seriousness of the threat. By tracing a number of historical attacks, we aim to highlight certain key vulnerabilities along with individual lessons learned, because as satellites become more critical to our lives, securing them is not optional; it's necessary. The question we should make isn't how many satellites will be attacked, it's whether we're fully ready.

The Rise and Fall of Satellites

The space age began around the late 1950s, representing at once the dawn for a new era of human investigation and technical improvement. As the world's first artificial satellite, Sputnik-1 was successfully launched into orbit on October 4, 1957, marking the Soviet Union's entry into space and starting a major competition between global superpowers. Initially, satellite technology found use mainly for scientific studies and also within initial surveillance, thus setting the stage along its gradual evolution into a vital element within current infrastructure. Vanguard 2, which initially launched in 1959, innovated a special type of Earth weather monitoring prior to the decade's conclusion, showing that satellites possessed definitive purposes apart from military spying (Neufeld, 2018).

Throughout the 1960s, certain initial communication satellites distinctly emerged overhead in the sky. Syncom 3 achieved geostationary orbit, an accomplishment self-assured to change global communication (Whalen, 2002). Throughout that decade in time, weather-watching satellites grew in number overall, and reconnaissance and surveillance technologies quickly got better in quality overall, which was key throughout the Cold War. The capability toward observation, of communication, and during navigation out from space was no longer within a distant dream. It was a definite reality taking shape from high above the Earth.

In the 1970s, several satellites considerably changed from research and military uses, widely broadening their scope in worldwide navigation and Earth's monitoring. The initial Global Positioning System (GPS) satellites were at launch, originally designed for military use but ultimately transforming the way within which civilians navigate the world. During 1972, Landsat greatly transformed the detailed observation across Earth's multiple terrains, presenting a viewpoint on prominent ecological shifts and key resource handling. Meanwhile, IntelSat IVA, accurately launched during 1975, considerably expanded global communication capabilities, readily enabling international telephone connections on a large scale (Neufeld, 2018).

As we look back throughout the decades comprehensively, we can observe special technical milestones from the past distinctly that shaped the evolution of satellites. Sputnik-1's debut during the 1950s commenced the space race, setting off an era of initial discovery and also surveillance. Earth observation, communications, as well as weather monitoring each saw a large rise during the 1960s, while navigation coupled with global connectivity through the GPS alongside commercial telecommunication satellites were introduced during the 1970s. Over time, satellites slowly grew quite advanced, rather flexible, and increasingly vital to today's society.

Table 1: Primary uses of Satellites from 1950s to 1970s

Decade	Primary uses of Satellites
1950s	● Space Exploration ● Scientific Research ● Reconnaissance ● Early weather observation
1960s	● Communications ● Weather monitoring ● Reconnaissance
1970s	● Navigation ● Earth observation ● Communications

As the 1980s unfolded, the satellite industry saw a dramatic transformation within its structure. The existence of sufficiently tinier and acceptably more inexpensive satellites made space technology greatly more obtainable, triggering the subsequent swift growth of many satellite constellations. The field that once belonged only to governmental as well as military organizations was now turning into a business, letting industries along with private firms use their own setups. However, this broad expansion came along. It came along with certain unexpected outcomes.

Satellite communications sales, at first commended as a global connection revolution, also created vulnerabilities that had not been anticipated before. By comprehensively extending satellite technology throughout the civilian sector, we unknowingly opened the door into a broad new era of cyber threats—a reality that would only become gradually apparent as attackers began exploiting fundamental weaknesses within satellite networks. The initial pursuit of progress unintentionally formed a fresh combat zone, where the precise networks built to unite and defend people might now be used to harm them.

80s Satellite's Cyberattacks

The 1980s marked a turning point within satellite technology. Satellites were not only for military and government use, they started to have a bigger part in global communications. In this decade the surveillance capabilities improved along with the KH-11 series, in addition to NOAA-7's improvement in weather forecasting. However, that largest alteration occurred with the total marketing of satellite communications, which, despite guaranteeing total worldwide connectivity, also subjected those systems to further weaknesses (Neufeld, 2018).

This decade marked the initial few documented satellite cyberattacks. What had formerly been tightly controlled became generally accessible and widely exploitable by others. In September of 1985, four Polish astronomers interrupted a government broadcast in Toruń to transmit pro-Solidarity messages, in the earliest documented hijack. Telewizja Solidarność (TV Solidarity), showed that satellite signals could be accessed and could be repurposed (Downing, 1984).

An interesting incident took place in the U.S. in April 1986, when John R. MacDougall, known as "Captain Midnight," interrupted HBO's signal using a satellite to protest subscription prices, sending the text: "Good Evening HBO from Captain Midnight $12.95/month? "No way!" for four and a half minutes (Lin et al., 2024).

Indonesia underwent multiple accusations of eavesdropping on U.S. satellite imagery in 1987, causing a large alarm regarding sensitive data access. During that same year, Thomas Haynie hijacked Playboy Channel's satellite signal. He was replacing the signal with static text displaying certain Bible verses (Fritz, 2013).

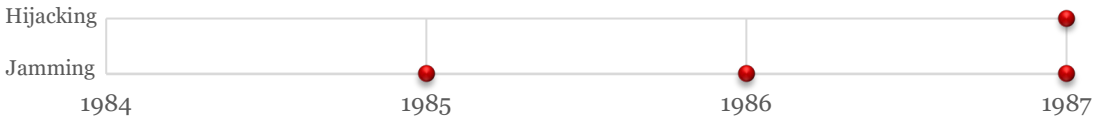

Figure 1: 1980s Satellite's Cyberattacks

By the close of the decade, certain major satellite cyber incidents had been recorded: three definite hijackings and one clear eavesdropping case. The United States led forth with two attacks, followed then by Poland and Indonesia, setting the stage for the increasingly advanced satellite threats that would follow in later decades.

90s Satellite's Cyberattacks

The 1990s showed marked improvements within satellite features, most notably in Earth observation, environmental monitoring, and remote sensing. Satellites were generally used for tracking climate patterns, natural disasters, and high-resolution imaging. A highlight across the decade remained within the Cassini-Huygens mission, launched during 1997 for the exploration of Saturn, presenting a strong push toward deep space exploration (Del Canto Viterale, 2023).

Nonetheless, accompanying said advance was a special increase of satellite cyberattacks. Contrary to the four particular incidents during the 1980s, the 1990s recorded nine separate attacks, along with increasing sophistication across governmental and commercial satellite operations. Attack methods included several jamming, cryptographic exploitation, and under wide-ranging hijacking.

Back in 1993, hackers exploited weak encryption for the distribution of BSkyB pay-TV channels all through an apartment complex, marking the first known cryptographic breach upon a satellite system. The next year, Iran was suspected of allegedly jamming ArabSat and AsiaSat broadcasts, and Gregory Manzer was convicted for developing tools to break VideoCipher encryption used directly by HBO and ESPN.
In 1996, the Indonesian government entirely jammed Apstar-1A with its own Palapa B1 satellite to block foreign broadcasts. Concurrently, the Turkish government started blocking MED-TV via Eutelsat, with attacks continuing until 1999. Apstar-1A was once more disrupted in 1997 by Indonesia, due to frequency overlap; this was categorized as an unintentional attack.
During 1998, the most severe attack occurred when the ROSAT X-ray satellite, jointly operated by the U.S. and Germany, was hijacked through certain malicious ground commands. The attackers turned the satellite's solar arrays to the sun, overheating batteries and causing mission failure, a prominent case of cyber-caused physical harm to space hardware.
By 1999, cyber warfare had reached into several military applications. These military applications had many implications. In Chechnya, Russia forced its way into satellite telephone systems, severing separatist communications. That same year, the British Skynet military satellite system was hijacked, with attackers demanding a ransom before the restoration of access (CNET, 2002). This showed the start of space coercion as a web threat, ending a decade of higher risks in the cosmic framework.

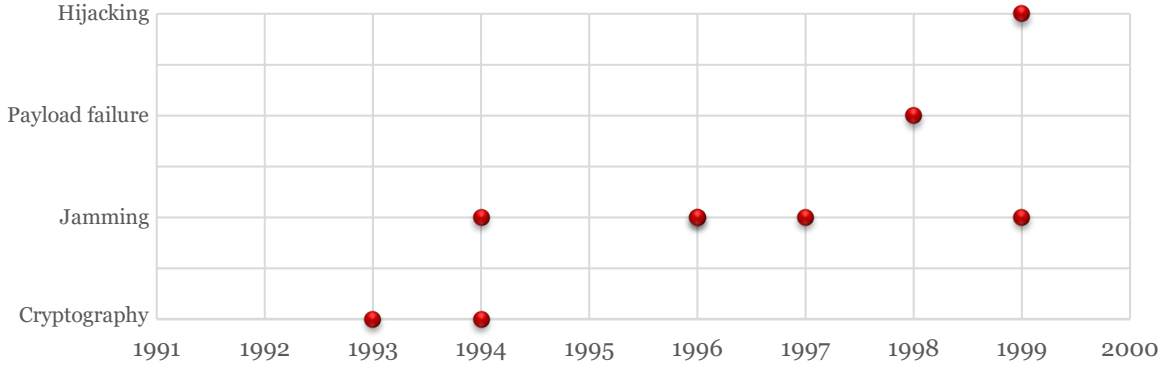

Figure 2: 1990s Satellite's Cyberattacks

The 1990s determined that cyberattacks on satellites are a growing worry for security. Indonesia along with Russia both had a pair of incidents, while jamming emerged as the most common attack type, in addition to cryptographic breaches and hijackings attacks. This pattern showed an evolution to RF exploitation with encryption avoidance, thus paving the path for much more advanced risks within later decades.
By the initial 2000s, it was obvious that satellites were never simply vulnerable to technical or ecological issues, they had turned into actual targets within cyber warfare, geopolitical conflicts, and likewise criminal activity. Many attacks of the 1990s had turned satellite cybersecurity from abstract theory into a pressing necessity.

2000s Satellite's Cyberattacks

The 2000s represented a great surge in satellite ability, spurred by fast expansion within worldwide communications, internet availability, and environmental monitoring. Satellites became important in real-time navigation, global intelligence, as well as digital connectivity. But along with increased reliance, from it came growing cyber vulnerabilities.
The 2000s, unlike past decades' few, politically driven attacks, experienced a surge in satellite cyberattacks' frequency and sophistication. Individual nation-states fully used jamming as a definite geopolitical weapon, while many rebel groups and a few dissidents hijacked signals for propaganda, turning satellites into actual digital battlegrounds.
In 2000, Iran frequently disrupted rival broadcasts using Eutelsat, and Greek testing saw British and U.S. tanks suffer recurrent GPS jamming. In 2002, Chinese TV was hacked by Falun Gong to broadcast dissent. In 2003, Iran interfered at Telstar-12 to stop regime-change messages, and Cuba jammed Voice of America signals carrying Iranian opposition content. Same year, AsiaSat was disrupted by Falun Gong, who sent another protest message. This attack was repeated in 2004 against AsiaSat.
In 2005, Tamil rebels hijacked a satellite channel in order to broadcast pirated TV across different countries. Then, Libya disrupted the European TV and government communications. In 2006, Libya

completely jammed satellite phones throughout civil unrest, while Israeli forces illegally hijacked Hezbollah-linked satellite TV to deliver threats, in addition to China purposefully disrupting U.S. satellite sensors on an American spy satellite.

In 2007, Tamil rebels took over IntelSat for nearly two years to broadcast their propaganda (U.S. Economy and SR Commission, 2011). That very same year, Landsat-7 experienced about 12 minutes of cyber interference, and Terra AM-1 suffered exactly two signal disruptions, two minutes in June 2007 and nine minutes in October 2008 (Liebowitz, 2011).

In 2009, a single telecom satellite broadcasting BBC as well as Farsi content was jammed, likely by state actors. That year, Iraqi rebels employed commonly available programs (SkyGrabber) so as to catch unsecured U.S. drone footage, and Egypt disrupted the UK-based Al-Hiwar satellite station (BBC Monitoring World Media, 2013).

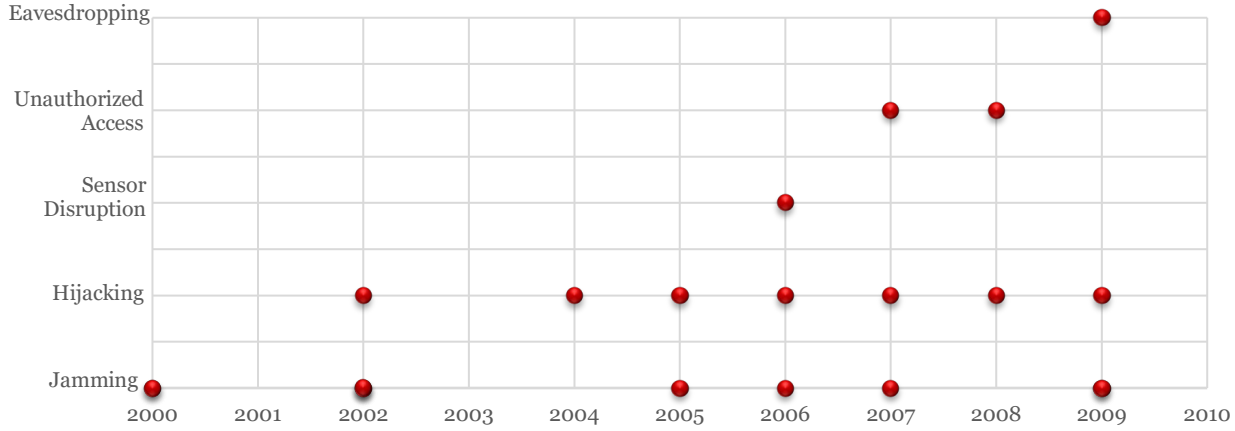

Figure 3: 2000s Satellite's Cyberattacks

The 2000s presented a rapid escalation in satellite cyberattacks, considering quantity and difficulty. China led along with four incidents, followed by Taiwan with three. There existed nine jamming incidents, the most commonplace sort of attack, followed by five of hijackings. Attacks were frequently repeated as well as sustained, unlike earlier decades when they were singular.

This decade revealed an obvious link between the overall expansion of diverse satellite networks along with their increasing cyber vulnerability. As reliance upon satellites mounted, critics noted their value to spy, censor, wage psychological war, cause military upset, and commit financial shakedown. What began as a restricted cybersecurity issue then became a worldwide security threat. Several more advanced attacks are setting the stage in the years ahead.

2010s Satellite's Cyberattacks

The 2010s represented a shift in satellite technology, as small satellites, miniaturization, and private space ventures grew in, expanding global connectivity (Del Canto Viterale, 2023). Satellite constellations substantially increased, the zone vulnerable to cyberattacks also grew, jumping to 19 noted cases, almost twice the attacks in the 2000s within it. Wide-ranging jamming, persistent hacking, and common hijacking turned to tools of state control, military disruption, and political messaging.

In 2010, Iran blocked broad global TV on Eutelsat during its revolution celebration, while Jordan cut Al Jazeera's satellite signal, including World Cup telecasts. That same year, North Korea began years-long GPS jamming against South Korea (BBC Worldwide Monitoring, 2013).

LuaLua TV, from Bahrain, was jammed within simple hours after its 2011 launch; the same year, Ethiopia jammed satellite opposition TV using Chinese technology. Libya moved fast to restart blocking satphones, as Saudi Arabia blocked Iran's news TV, and Deutsche Welle saw strong blocking on Hotbird 8 (BBC Worldwide Monitoring, 2013).

In 2012, Eritrea completely jammed Radio Erena, and Ethiopia directly retaliated by jamming ArabSat. Eutelsat was jammed by Syria, as well as North Korea interfering along with the South Korean military's satellites (BBC Worldwide Monitoring, 2013).

In 2013, Turksat was jammed by Azerbaijan, and Al Jazeera by Egypt. In 2014, China noticeably disrupted many NOAA weather satellites, ArabSat was jammed directly over Ethiopia, Egypt thoroughly jammed many comedy shows, and Hamas briefly hijacked Israeli Channel 10 to broadcast a serious threat. Russia-

linked Turla, along with APR28 disabling French TV network TV5Monde, exfiltrated data via satellite in 2015. In 2016, Russia upset a soccer show in Ukraine, and Saudi hackers seized an Israeli show after show upset, for example, Big Brother.
Then in 2018, Israel jammed Syrian satellite TV, and Russia disrupted the GPS of Finland and Norway. Finally, China launched one GPS spoofing attack in 2019. Detected through multiple maritime satellite systems, this presented the increasing global reach and complexity of space-based cyber warfare.

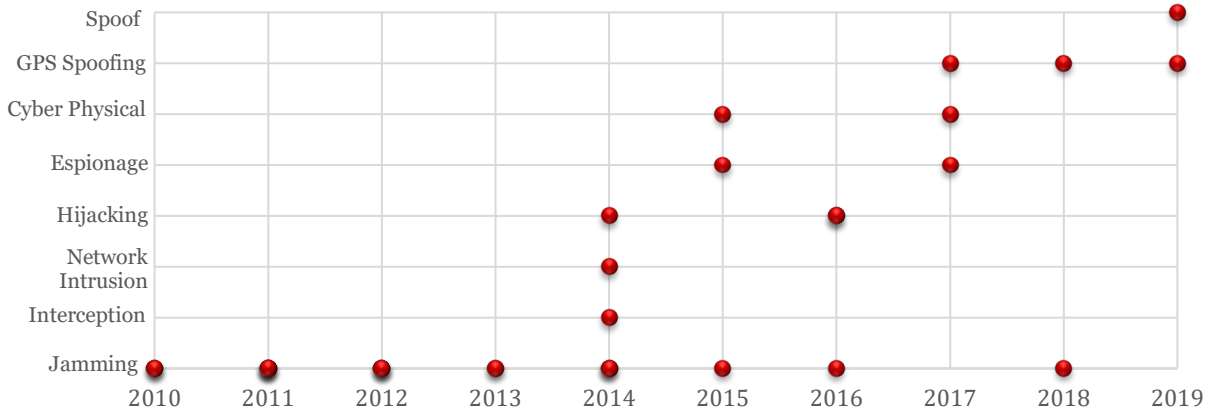

Figure 4: 2010s Satellite's Cyberattacks

The 2010s strengthened satellite cyberattacks as a core element of modern warfare as well as in information control. China helped governments in jamming tech, while North Korea as well as Middle Eastern nations emerged as major players, repeatedly targeting satellites.
Jamming remained the decade's most frequent attack method, as well as incidents showing a special shift from isolated cases to sustained, politically driven interference across many nations and years.
This increase stresses upon one stark truth: when satellites multiply, threats also multiply. The 2010s proved something. Absolutely no satellite, civilian or military, is safe ever. Previously uncommon disturbances are now a global security issue, which sets up the chance for cyber threats ahead that are more advanced and persistent.

2020s Satellite's Cyberattacks

The 2020s, the golden age of satellites, saw a large surge within space technology, caused mostly by SpaceX's rocket constellations. Between 2020 and early 2025, the number of active satellites grew 75%, from 2020 to 2025. Of the 11,833 satellites active in 2025, 84% are in Low Earth Orbit, 3% in MEO, and 12% in GEO (Orbiting-Now, 2025).
This growth initiated a new period of global broadband as well as linked constellations, but also introduced a number of cybersecurity risks. A single breach into one linked satellite could compromise entire networks, triggering common disruption. In the 2020s, satellite cyberattacks are already more advanced; vulnerabilities are used by state actors, hacktivists, and criminal groups.

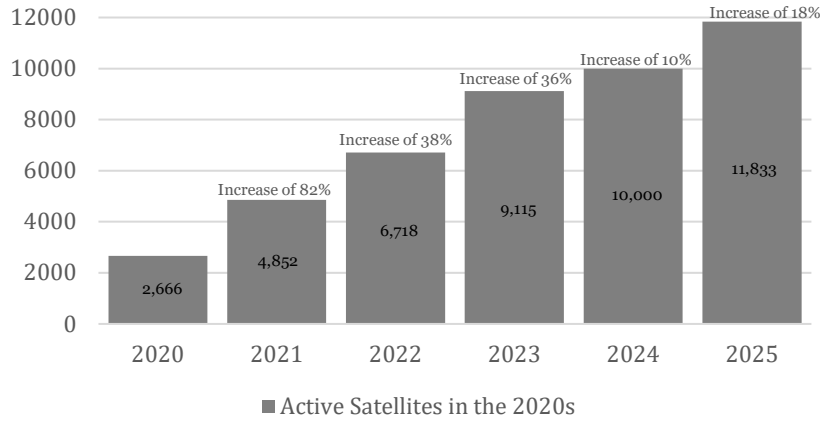

Figure 5: Operating Satellites in the decade of 2020

In 2020, one of the first major incidents of the decade involved GPS spoofing, along with ships near Norway, Libya, Malaysia, as well as Russia sailing in circles off San Francisco's coast due to manipulated navigation data. This revealed continued weaknesses in satellite navigation, causing worries for aviation, maritime as well as military safety.

In February of 2022, one initial supply chain attack occurred, directly targeting ViaSat's KA-SAT network. The cyberattack, linked up with Russian cyber units, disrupted internet services throughout Ukraine and Europe and disabled around nearly 5,800 wind turbines throughout Germany (CyberPeaceInstitute, 2022; Viasat, Inc., 2022). Subsequently, SpaceX deployed Starlink to Ukraine, which was then met by repeated Russian jamming efforts to disrupt its service (Holmes, 2024).

In March of 2022, hacktivist group Network Battalion 65 (NB65) hacked into Roscosmos, Russia's space agency, and disrupted satellite imaging for cyber retaliation. This showed non-governmental groups could now hit space programs of nations.

At approximately mid-2023, the Iranian group APT33 (Peach Sandstorm) deployed backdoor malware in order to gain wide-ranging access into satellite and communications networks as well as a tactic that bypassed direct space asset targeting (Newman, 2024). Russia, throughout the year, kept up its jamming attacks upon Starlink, reinforcing satellites' place in the Ukraine war (The Hacker News, 2015).

Following the local internet cut in 2024, Myanmar's criminal groups used Starlink to maintain operations. The unregulated commercial satellite use had related risks (Burgess, 2025). During March, Ukraine's 1+1 Media Group faced common broadcast disruption from Russian jamming. From April 29 until May 31 2024, Estonia experienced wide-ranging GNSS jamming, affecting aviation along with key services.

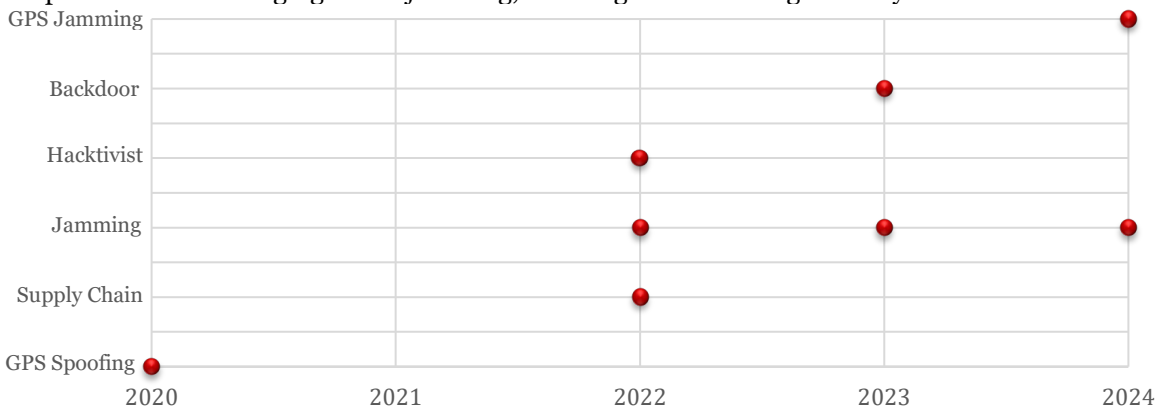

Figure 6: 2020s Satellite's Cyberattacks

The 2020s have thus far seen nine satellite cyber incidents in four years, a telling sign of growing cyber warfare. The very first supply chain attack caused billions in damages, affecting power grids along with critical services across many countries. Since then, GPS and GNSS jamming has grown into more commonness, hurting into aviation, military in ops, and during emergency response.

Russia is the leader in satellite cyberattacks of the 2020s. These include signal jamming, espionage, and supply chain breaches. Iran, North Korea, China, and several cybercriminal or hacktivist groups have posed further threats, heightening the growing complexity.

In the middle of a process of expanding satellite constellations, coupled with rising interconnectivity, the potential risk for large-scale breaches along with cascading failures continues to increase. The 2020s prove satellites are no longer purely passive infrastructure, they are specific active targets within modern cyber warfare, thus making sufficiently strong defenses, important international coordination, along with immediate real-time threat detection necessary.

Conclusion

As satellites evolved from research tools, to vital infrastructure, given communication, security, and navigation, the rise into interconnectivity brought forward grave cyber weaknesses. The satellite cyberattacks' development, from hijackings during the 1980s to supply chain breaches with GNSS jamming during the 2020s, shows a clear trend: greater reliance brings greater risk.

Each decade brought many new threats, encryption flaws, jamming, hijacking, and intrusions affecting entire satellite operations. What began as several isolated incidents back in the 1980s and 1990s escalated into geopolitical cyber warfare around the 2000s. By the 2010s, several state-sponsored attacks became

routine, and in the 2020s, supply chain compromises and GPS spoofing have affected both military and civilian life.
Today, satellites are frequent targets in warfare. They are frequent targets in espionage and crime. With space for it rapidly commercializing, along with constellations from it multiplying, cyber threats have crossed over borders, threatening global industries as well as to security. The 2022 ViaSat KA-SAT attack largely proved that breaches upon satellites can cripple critical infrastructure throughout entire nations.
Outer space is no longer a safe zone. Orbit shares vulnerabilities like Earth's networks, and if left without protection. Satellite systems might cause devastating real-world consequences.
To address this, the global space community has to take up strong cybersecurity steps to impose firm encryption and use real-time threat finding. With zero-trust architectures, along with AI-based anomaly detection, and wide-ranging global cooperation will be necessary.
Our present day lives are supported by satellites. Protecting them is not just technical, it's a matter for global security. The precise next frontier into cybersecurity isn't purely on Earth, it is in orbit.

References

Barrett, T. (2024, November 10). *Looking to the skies: The importance of satellite cybersecurity*. Edu.au. https://www.ussc.edu.au/the-importance-of-satellite-cybersecurity

BBC Worldwide Monitoring. (2013). *UK-based Al-Hiwar satellite TV off-air after deliberate jamming*. *Jamming of Al-Jazeera TV broadcasts traced to Jordan. Iran's Arabic TV said "jammed by Saudi Arabia."* South Korean satellite comes under North jamming attack. BBC Monitoring Asia Pacific. *World broadcasters condemn satellite jamming*. *North Korea increases jamming electronic signals against South Korea*.

Burgess, M. (2025, February 27). Elon musk's Starlink is keeping modern slavery compounds online. *Wired*. https://www.wired.com/story/starlink-scam-compounds/

CISA. (2024). Critical Infrastructure Sectors. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

CNET (2002). *Satellite hack raises security questions*. CNET. https://www.cnet.com/tech/mobile/satellite-hack-raises-security-questions/

CyberPeaceInstitute. (2022). *Case Study - Viasat*. Cyberpeaceinstitute.org. https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat

Del Canto Viterale, F. (2023). *Transitioning to a New Age in the 21st Century: A Systemic-level Approach*. *11*(5), 232.

Downing, J. D. H. (1984). Samizdat in the Former Soviet Bloc. *South End Press*. https://doi.org/10.4135/9781452204994.n22

Fritz, J. (2013). Satellite Hacking: A Guide for the Perplexed. *Culture Mandala*, *10*(1), 5906.

Georgescu, A., & Botezatu, U. (2016). CRITICAL INFRASTRUCTURE DEPENDENCY ON SPACE

Holmes, M. (2024, January 22). *10 defining moments in cybersecurity and satellite in 2023*.

Satellitetoday.com. (2023) https://interactive.satellitetoday.com/via/january-february-2024/10-defining-moments-in-cybersecurity-and-satellite-in-2023

Liebowitz, M. (2011, October 27). *Hackers interfered with 2 US government satellites*. Space. https://www.space.com/13423-hackers-government-satellites.html

Lin, P., Abney, K., & Jenkins, R. (2024). Outer space cyberattacks: Generating novel scenarios to avoid surprise. In *arXiv [cs.CR]*. https://doi.org/10.2139/ssrn.4868227

SYSTEMS. Scientific Bulletin of Naval Academy, 19(1), 398–404.

McCreight, R. (2023). Gauging the Impact of Satellite & Space Systems on Critical Infrastructure[CI]: Risk Management is Neither an Enigma nor a Mystery for CI Systems Security. *Journal of Homeland Security and Emergency Management*. https://doi.org/10.1515/jhsem-2022-0054

Neufeld, M. J. (2018). *Spaceflight: A Concise History*. MIT Press.

Newman, L. H. (2024, August 28). Notorious Iranian hackers have been targeting the space industry with a new backdoor. *Wired*. https://www.wired.com/story/iran-peach-sandworm-tickler-backdoor/

ORBITING-NOW. (2025). Active satellite TLE data and information. Orbit.ing-now.com. https://orbit.ing-now.com/

US Economy and SR Commission. (2011). *2011 annual report to congress, Chapter 2, section 3: The implication of China's civil and Military Space Activities*. www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf

Viasat,Inc. (2022). *KA-SAT Network cyber attack overview*. Viasat.com. https://www.viasat.com/perspectives/corporate/2022/ka-sat-network-cyber-attack-overview/

Whalen, D. J. (2002). *The origins of satellite communications, 1945-1965*. Smithsonian Institution Scholarly Press.