SSPC MONOGRAPH SERIES NO. 3

CYBER THREATS TO SPACE DOMAIN: RISKS AND RESPONSES

AJEY LELE

Society for the Study of Peace and Conflict
https://www.sspconline.org/

SSPC MONOGRAPH SERIES

Layout & Cover: *Excel Solutions, Noida*

Cover Photos/Representational: (Open Source)

REVIEW: *SSPC Monograph series manuscripts undergo a rigorous review and editorial process by in-house and external subject matter experts and scholars.*

PUBLICATION DISCLAIMER: *The views expressed in this Monograph are those of the author, who holds responsibility for the Content, Research, and Presentation of facts contained in this work.*

Published by Society for the Study of Peace and Conflict, Po-Bo: 10560, JNU Old Campus, New Delhi, 110067 (https://sspconline.org)

Table of Contents

INTRODUCTION

Usually, the word 'dimension,' say from the perspective of Physics, gets recognised as 'direction'. For any object on the earth, there are three dimensions: length, width, and height (X, Y and Z). Time is considered as the additional fourth dimension. This dimension is essential to identify the position of the object. The position of the object doesn't always need to remain static; as time changes, the position could also change. Hence, time becomes the fourth dimension. It is also called as time-space dimension. The special Theory of Relativity was put forward by Albert Einstein in 1905. As per this theory, space is intimately connected to time via the cosmic speed limit of light. It could be said that the universe is a four-dimensional place. There are three dimensions of space (north-south, east-west, and up-down) and one dimension of time (past-future). Some theories have also presented the idea of a fifth dimension above an extra dimension of space (micro-dimension). Broadly, space or outer space could be viewed as a free and primarily unoccupied area around us. It is an area beyond the earth's atmosphere or minus the atmosphere. There are some interesting views regarding the number of dimensions of space. They vary from one dimension to many dimensions. Mainly because in space, there are mutually perpendicular axes at each point within it. For some time now, mainly two theoretical postulations are getting debated. First, as per the String Theory, the universe operates with ten dimensions. Second, M-theory bonds together the five most possible variants of string theory and introduces the concept of an 11^{th} dimension. All this makes us realise we know a bit about outer space, mainly our solar systems. Space is vast and possibly dimensionless. There are billions of galaxies and stars yet to be entirely discovered or understood, and our knowledge of space continuously evolves.

On the contrary, the idea of Cyberspace is not real but virtual. It is about a virtual computer world. Such a world constitutes an electronic medium that enables online communication and denotes the virtual computer world, which is used to facilitate online communication. Cyberspace exists owing to the internet, which is a network of private and public networks. In 1984, William Gibson, an American-Canadian speculative fiction writer, published a science fiction book called Necromancer, where he first used the word cyberspace. As per him, broadly, cyberspace is an online world of computers and components of society who use these computers. Was William Gibson aware of the so-called dimension lessness of outer space and hence thought it prudent to suffix the word space to cyber, or did it happen just accidentally? Whatever may be the case, looking at the shear expanse of the domain of cyber, which could be said to include perceptions of artificial and ambient intelligence, emerging generations of the internet like Internet 2.0/3.0, big data, blockchain technologies and some other

technologies it appears that the word cyberspace indirectly demonstrates the multidimensional expanse of the cyber word.

There is an apparent connection between the worlds of outer space and cyberspace. It is not the purpose over here to get into the details regarding which laws of physics these worlds obey and try to establish some form of a scientific connection. It is important to consider cyber and space fields as arenas freed from time and geographical territory. Here, one world is real, and the other is virtual; hence, it cannot be the story of two parallel worlds. However, it is important to state that these worlds have some commonalities and some dependence on each other in a broader sense.

From an erudition standpoint, it could be said that the ideas of humans using space and cyberspace have origins in the 20th century. Humans involving themselves in stargazing has a very long history. Humans are aware that the Moon is the Earth's natural satellite. Natural satellites are those astronomical bodies which orbit a planet or other big 'heavenly' bodies like dwarf planets, minor planets/asteroids. But it was only in the 20th century, precisely since 1957, humans started launching artificial satellites into space, which have multiple utilities for humankind. There is no exact answer regarding when the first computer was invented since there are different categories of such machines, like mechanical and electrical computers. In 1948, a professor of mathematics from the United States (US), Dr Norbert Wiener, is known to have first used the word cybernetics.

Modern-day computers are high-speed data processing devices that store and process high data volumes. Such devices, mainly those in the supercomputer category, have a tremendous capacity to undertake complex arithmetic operations and handle a large volume of data. Cyberspace exists in bits and bytes: zeroes and ones (0's &1's), simply electronic impulses. Being virtual, cyberspace has no specific boundaries and characterizes the connected space between various computer networks.

There are variances between these two 'spaces', namely outer space and cyberspace. Outer space is a natural situation, while cyberspace is a human-made one. Outer space is a vast, timeless domain, while cyberspace characterises various data elements stored and processed online. It could also be viewed as a simulated reality presented by multiple devices, including the Internet.

In a digital world, cyber systems could be confronted by launching various attacks on them. These are not physical attacks but attacks on their operating software. Mainly, such attacks are undertaken to gain unauthorized access to systems that are operative in cyberspace or are present in a standalone form. These attacks are known to disable, disrupt, destroy, or control these systems. Such attacks could involve destroying, stealing and manipulating the data. There is also a possibility the perpetrators of the attack can take over the control of computer systems.

At present, cyber threats are known to affect various targets. Today, computers are a part of almost every system that human operates. Many sectors of human activity worldwide, like airline operations, hospital functioning and operations of various governmental departments and private industries, have been hampered owing to cyber-attacks on several occasions. Activities like operating the doors for dams, which control water flow, are controlled by computers. Hence, theoretically, even they could be manipulated by cyber means, and a perpetrator of cybercrime can create mayhem by giving rise to artificial flooding.

Artificial satellites have been launched in outer space for over six decades. Digital systems are at the heart of various assemblies and sub-assemblies that develop and operate satellites. Hence, there is a possibility of satellites in space coming under deliberate human-engineered cyber-attacks. It is important to note that there could be various active and passive ways to hamper the health of the satellite. Unfortunately, cyber could have a direct or indirect footprint in such attacks. It is also important to note that space-based assets are strategic and are not immune to geopolitical power politics and conflicts.

This monograph explores the multifaceted nature of potential cyber threats to space architecture. Given the dynamic and evolving nature of such threats, it's neither a scientific thesis nor a technology profile, and it doesn't promise a comprehensive view of cyber threats in the space domain. As technology progresses, threat and response strategies could change within the space and cyber realms. This work aims to evaluate the challenges that cyber threats pose to space architecture, albeit in a limited scope, and to delve into the cyber threat facets of the space domain.

This monograph, free from stringent stylistic and formatting norms, offers a nuanced discussion. The first section, following the introduction, provides insights into cyber security and threats. Subsequent sections debate diverse threats to space security, present instances of actual cyber-attacks in space, identify specific cyber threats to space security, including examples of GPS jamming, and explore measures for countering cyber-attacks on space systems. The penultimate section discusses policy directives by various states. Lastly, it concludes with some remarks and recommendations. Repetitions within this work typically stem from shared perspectives among global agencies on threat identification and response. These views and directives are presented unaltered, leading to occasional repetitions.

CYBER SECURITY AND CYBER-THREATS: AN OVERVIEW

In general, the expanse of cyber security is vast. Cyber security is defined mainly based on the result expected by an individual or group of people or a government or a private enterprise about what they want to secure. Cyber security is a catch-all term to define the practice of protection against every form of cybercrime. Such crimes could involve data thefts, data manipulation, defacing websites, and money-related wrongdoings to international digital weapons. Cyber security is a discipline that covers the processes to defend devices and services from electronic attacks by different actors, including individuals, non-state, and state actors.[1] It is imperative to ensure cybersecurity mainly for two reasons: to ensure the overall safety of individual systems and the network itself and to avoid data theft.

It is important to realise that space system investments have significantly changed over the years. Some call the present era of activities in the space domain a New Space era. In this era, a significant surge in investment in the Earth observation market has been witnessed owing to the increasing applicability of satellite imagery and signals intelligence. Space systems are playing a major role in environmental conservation efforts too. Global broadband services are helping to connect rural and remote areas and providing fault-tolerant networks for critical services. Satellite broadband revenue is steadily growing, and the market is expected to expand further. New satellite constellations (hundreds and thousands of satellites) are being launched, mainly for Internet services. Another critical application is a satellite geolocation service, which provides dedicated receivers with precise time and position data. The market for all these services is rapidly growing. In the strategic realm, the use of satellites in warfare is increasing.

Various wars/conflicts fought during the fag end of the 20th century and in the 21st century have demonstrated that present-generation fighting platforms like aircraft, ships & submarines and tanks depend greatly on space technologies. The firing of munitions is happening in various wars with assistance from space. Military systems have There are harsher security requirements for military systems. Here multiple measures such as encryption, frequency hopping, and anti-jamming practices are

[1] Karin Kelley, "What is Cyber Security and Why it is important?", *Simplilearn,* January 30, 2023, https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cyber-security.

implemented.[2] However, worldwide, barring a few major powers, primarily space architecture, is getting used in the dual-use technology mode. Every space system that has assisted the armed forces is not hackproof. The Russia-Ukraine war has shown that the services of private space players also have much relevance during wartime. Mostly, commercial satellites have limited cyber security provisions. All this indicates that, even in the era of new space, the cyber challenges to satellite systems do exist, and unfortunately, the attack frequency has increased much.

In the cyber domain, concerns about cyber security have been there for a long time.[3] The period of 1970s saw the need for cybersecurity. The first known virus, the Creeper virus, was born in 1971. The predecessor to the internet, the Advanced Research Projects Agency Network (ARPANET), arrived during the decade. Then came the famous 'I'm the creeper; catch me if you can!' message to the world, connected with a programme developed by Bob Thomas, an ARPANET developer, using PCs connected to the network. With this, a programme switched from one machine to another for the first time. It was a harmless experiment, but it possibly could be viewed as the first computer worm recorded in the history of cyber security.

Since the 1980s, computer attacks have started happening mainly on the computer systems of political and scientific importance in the US. In 1983, a movie called War Games, a science fiction techno-thriller film got released, which had a plot involving malicious computer software giving commands to nuclear missile systems etc. This science fiction made people aware of the possible realities for the future, like the chances of intentional tampering with computer systems. The terms 'Trojan Horse' and 'computer virus' debuted in the same year. Throughout the Cold War, the threat of cyber espionage increased. The term Cybersecurity first appeared in 1987. Possibly, the first antivirus programme could have transpired much before that. Also, 1987 marked the beginning of commercial antivirus programmes with the release of Anti4us and Flushot Plus.[4]

Over the years, cyber-attacks have managed to work their way into nearly every operational networked system. There have been attacks on critical infrastructure assets like water, gas, and energy sites. Some known instances exist where an entire country has been halted by unleashing a cyber offensive. In the spring of 2007, Estonia (a small Northern European country which borders the Baltic Sea and the Gulf of Finland and has an estimated population of 11 to 13 lakhs) fell under a cyber-attack campaign lasting

[2] Mark Manulis, C.P. Bridges, R. Harrison, et al., "Cyber security in New Space," *Int. J. Inf. Secur.* 20 (2021): 287–311.

[3] The 1962 case of password stealing the database via punch card involving Allen Scherr, who launched a cyber-attack against the MIT computer networks, is known as the first cybercrime case in the modern history.

[4] Akhil Bhadwal, "The History of Cyber Security: A Detailed Guide", *Knowledge Hut*, July 14, 2023, https://www.knowledgehut.com/blog/security/history-of-cyber-security.

a total of 22 days (27 April and 18 May of 2007). The attacks were part of a broader political fight between Estonia and Russia over relocating a Soviet-era monument in Tallinn (capital city of Estonia). The attacks were generally carried out by Denial of Service (DoS) or Distributed Denial of Service (DDoS) methods. Various familiar approaches were used, including ping flood, udp flood, malformed web queries, e-mail spam, using SQL injection etc. Many of these attacks succeeded at non-critical sites like web servers, e-mail servers, DNS servers and routers. The targeted units involved the president and various other agencies for governance like the parliament, police, banks, businesses, Internet service providers (ISPs), and media.[5]

Launching the cyber-attacks witnessed in Estonia is not challenging, and a range of actors, from individuals to groups to state agencies, can launch such attacks. It has been observed that almost 80% of hackers who mount such attacks are self-taught and habitually have gaudy imaginations. They can mount cyber-attacks on ground installations, systems operating in the air, ships, and space. They can send wrong signals to various electronic systems, which are used for controlling and coordinating various critical infrastructure sites, or to the platforms used for human/logistic travel like buses, ships, and aircraft.[6] For example, by manipulating global space-based navigation systems (say GPS), the altitude information could be changed, leading to an accident of an airliner or a cruise ship.

Broadly, the types of cyber-attacks include virus & worms attack, Phishing Attacks and Denial-of-Service Attacks. Then there could be attacks on passwords and various codes of the software. Structured Query Language (SQL) allows individuals to access and engineer databases, and there are SQL Injection Attacks where the attacker can access information that was not proposed to be revealed. For many years, the targets for cyber attackers have been business houses, banks, airlines, railways, educational institutes, and medical facilities. Many attacks have also happened on government and military establishments. Today, such attacks are happening on space establishments too.

States and private agencies have been operating satellites for some decades now, and the cyber threat is also not a new phenomenon, so obviously, the question arises 'Why now'? This is primarily because, at present, the networks are changing from terrestrial (land) based communications to the cloud, taking benefit of satellites to move data over large, international expanses. In addition, there has been a much increase in the number of satellites circling on low Earth. The costs towards launching have also

[5] Rain Ottis, "An analysis of the cyber-attack on Estonia," *Cooperative Cyber Defense Centre of Excellence*, October 2018, https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.

[6] Zac Amos, "How secure are satellites from cyber-attacks?", *CyberTalk,* May 26, 2022, https://www.cybertalk.org/2022/05/26/how-secure-are-satellites-from-cyber-attacks/

significantly lowered, helping more players invest towards having their space assets. This is making a more significant number of available targets for hackers. Correspondingly, the costs of jamming and control-takeover technology are dropping. With increasing dependence on satellites for the conduct of various activities in day-to-day life, any attack on space systems would lead to disastrous consequences. Also, increased global connectivity to industry units combined with the nationwide rollout of 5G communications could help create additional opportunities for hackers to intercept space-bound communications.[7]

Satellite operations are primarily directed from ground stations. Here various technologies are put in place for guiding and controlling the satellites. These ground stations mainly offer entry points for cyber with significant possibilities available for the potential (intelligent) hackers. At times, defending such systems from possible cyber intrusions becomes difficult due to the availability of a vast number of entry points for infiltration. This makes tracing cyber incursions difficult and taking timely decisions towards shutting down the system (temporarily, to avoid the initial outburst) to stop the attacks. Another common flaw with all satellite units is the use of long-range telemetry for communication with ground stations. The uplinks and downlinks are typically transmitted through open telecom network security protocols, which the hackers could easily access. A hacker can access any downstream systems connected to the satellite by interrupting the satellite signal. With this, it becomes possible for the attacker to trespass through an establishment's network starting from the infiltrated satellite ground station. IoT (Internet of Things) devices that utilize satellite communications permit extra points of entry for hackers.[8]

Specific vulnerabilities in satellite networks could come from various corners, and some believe that the human factor and supply chain vulnerabilities should be the primary concern. Cyber risk and cybersecurity are mainly about people behind consoles and controls rather than technology manipulation[9]. The human factor is the leading cause of worry since they could mount an attack by 'default' or be intentionally manipulated to cause damage. In the present-day world, supply chain vulnerabilities could be targeted digitally. There could be two important aspects related to the supply chain. One, to cause economic damages to the adversary, the attacker could manipulate the supply chains of various industries of that state by hampering their satellite-based

[7] Paul Ferrillo, "Protecting Space-Based Assets from Cyber Threats", *Homeland Security Today*, Oct 17, 2020, https://www.hstoday.us/subject-matter-areas/cybersecurity/protecting-space-based-assets-from-cyber-threats/

[8] "Cyber Concerns for The Satellite Sector", *Archon Secure*, February 2020, https://www.archonsecure.com/blog/satellite-cybersecurity.

[9] Mark Holmes, "The Growing Risk of a Major Satellite Cyber Attack", *Satellite Today,* https://interactive.satellitetoday.com/the-growing-risk-of-a-major-satellite-cyber-attack.

connectivity structures. Two, the supply chain dependence of the satellite industries themselves could be compromised.

Dependence on satellites is increasing for various commercial reasons. Various companies now use satellite systems to deliver data services, including satellite imagery, broadband communications, and value-added GPS services. Hence, it is vital to ensure that space assets do not face any challenges related to cyber-security. Such security threats would have an adverse impact on businesses too.[10] Many states have significant dependence on space assets in managing critical infrastructure. These states realise that any compromise with these systems could lead to a major catastrophe in case of any issues with their critical infrastructure. Today, there are various options available for the cyber attacker to cause damage: such attacks can compromise ground setups, manipulation of satellite control systems is possible and intentional deorbiting of satellites could be attempted.

Almost everything is at stake, with satellites at the centre of human activity. Satellites are a part of the complete cyber environment as they stimulate global communication. They accentuate the network-based communication system and data transmission by helping very small-aperture terminal (VSAT) networks for various services to broadcasters, Internet service providers (ISPs), governments, the military, and other sectors. Several activities, such as communications, economic services, aviation and maritime sector-related services, various trade practices, weather observation and climate data storage units, and defence, have direct data links to social, commercial and defence activities globally.[11] Huge dependence on satellite systems makes them a lucrative target for potential cyberattacks.

It is even possible that cyber attackers can take total control of a satellite. Once the system is under the control of an unethical actor, then the threats become too severe. In such a case, there is not only a danger to the satellite alone, but it can be guided to crash on another satellite, thus creating considerable space debris. Cyber threat is not the only threat the systems in space encounter. Understanding the threat matrix for space systems before getting to the specifics of cyber threats to space architecture is crucial. It is essential to realise that almost every autonomous, mechanical, electrical, and optical system will most likely have a digital component. Hence, even the so-called non-cyber threats to space security could also suffer from cyber-related threats.

[10] Chuck Brooks, "The Urgency to Cyber-Secure Space Assets", https://www.forbes.com/sites/chuckbrooks/2022/02/27/the-urgency-to-cyber-secure-space-assets/?sh=45845c3a51b1e

[11] "Space Satellites and Cybersecurity", February 22, 2021, https://x-phy.com/space-satellites-and-cybersecurity/

UNVEILING THE THREATS TO SPACE SECURITY

The space age could be said to have begun with the launch of the satellite called Sputnik (1957) by the erstwhile Soviet Union. Since then, various nation-states and private agencies have invested in space technologies mainly for socioeconomic development and scientific investigation. Over time, with technological improvements, the range for utilising space-based systems has expanded. Space has become important for commercial, security and foreign policy tenacities. The 1991 Gulf War did majorly showcase the relevance of space technologies in warfighting. In this war, mainly the US (and allied) forces were found using satellite systems in navigational, communicational and intelligence-gathering roles with perfection. Since then, armed forces in many parts of the world have focused on ensuring that their security architectures get all the assistance from space systems. Modern-day weaponry is designed and developed based on new technological advances and disruptive technologies. Such weaponry and new state-of-art weapon delivery platforms greatly depend on satellite systems for their performance. This is pushing for the development of new satellite systems for strategic use. Also, some ideas of putting weapons in space have been put forth. All this has led to the realisation that space systems are the most vital assets for modern-day militaries. Since space technologies have emerged as critical assets for ensuring national security, there is also a realisation that such systems emerge as critical targets for the adversary. Hence, there is a need to safeguard such assets in space. Also, it is important to note that space possessions need not necessarily be only wartime targets for an adversary. They could try to (mostly covertly) destroy/disturb them for bringing in economic instability or running down the enemy state's social fabric.

Space is emerging as a major business sector. Space sector exploration is projected to create USD 1.2 trillion in retail revenues in 2020-2030. The perspective of space-based services has driven an inflow of private actors into what was once regarded as a predominantly government-dominated environment[12]. Space tourism promises a great future. Human space travel for recreational purposes has already begun, with agencies like Virgin Galactic and Blue Origin taking tourists to the boundary of space (80 to 100 km altitude above the earth's surface). Space tourism activities are expected to surge in the future with the initiation of orbital, suborbital, deep space, and Lunar/Martian space tourism in a big way.

The first satellite Sputnik got launched in 1957, and within two years, in 1959 the UNGA appointed a Committee on the Peaceful Uses of Outer Space (COPUOS). This indicates that security was always a concern for the space domain since the beginning.

[12] "Will the battle for space happen on the ground?", *World Economic Forum*, May 25, 2022, https://www.weforum.org/agenda/2022/05/increased-cybersecurity-for-space-based-services/

The 1960s to 1980s was when two major powers were also competing with each other in the area of military technology supremacy. Hence, since its early inception, space technologies also had a definitive military angle. Hence, space security has had an extensive expanse since the beginning spanning various dimensions of the military to human security. Security is relevant for defending space assets in outer space and protecting ground-based structures for managing satellites. So far, two fundamental ideologies with respect to the connection of space activities to international law have been known to have subjugated the discourse. They involve the right of access to space and the freedom of navigation in space. Administrations are known to endorse freedom of access to space and use of space for human security purposes[13].

There is an increasing dependency on space technologies for the management of critical infrastructure, for defence forces and for achieving foreign policy objectives. Space access offers deterrence positional for the states. However, the state must contextualise this ability of space technology correctly. Deterrence is mainly based upon the opponent knowing that its challenger is ready to respond in the domain of space if required militarily. Modern-day militaries depend on the following core areas towards using space-based assets. They include:[14]

- Positioning and navigation: Enabling precision strikes, force navigation or combat search and rescue missions
- Integrated tactical warning and threat assessment: Securing force protection, providing crucial information on missile launches and thus allowing attribution
- Environmental monitoring: Enabling meteorological forecasting and sound mission planning
- Communications for command-and-control purposes
- Intelligence, surveillance and reconnaissance (ISR) capabilities: Providing intelligence on and off the battlefield and informing targeting decisions

All this makes space infrastructure a suitable target for attack. At this stage, states know that any direct attack on the adversary's space assets would unnecessarily escalate the conflict to outer space. At the same time, states understand that there is a need to evolve a space deterrence mechanism. They are aware that developing and demonstrating destructive capabilities during peacetime would help them leverage

[13] Michael Sheehan, "Defining space security," in *Handbook of Space Security*, ed. Kai-Uwe Schrogl, et al. (New York: Springer Science, 2015), pp. 8-9.

[14] Karl-heinz Brunner, "Space and Security: NATO's Role", Science and Technology Committee (STC), Preliminary Draft Special Report,
October 10, 2021, https://www.nato-pa.int/download-file?filename=/sites/default/files/2021-04/025%20STC%2021%20E%20-%20SPACE%20AND%20SECURITY%20-%20BRUNNER_2.pdf

them for geopolitical and geostrategic gains when needed. Various technology developments happening in this regard are known as counter-space technologies.

It is complicated to define what establishes a space weapon precisely. Any technology capable of damaging space-related assets in outer space or on the ground could constitute a space weapon. At present, no major attempts are visible towards specifically developing space weapons. But, since technologies are available, which could be easily converted to offer weapon capabilities, some states have already started designing and developing counter-space technologies, possibly as some form of deterrence (but not limited to) mechanism.

The following are the categories of counter-space technologies:[15]

- Kinetic Physical: Technology intended to create permanent and irreversible destruction of a satellite or to ground support infrastructure through force of impact with an object or a warhead. Such technology includes direct-ascent anti-satellite (DA-ASAT) missiles and co-orbital systems. The co-orbital systems are satellites placed on similar orbits and can be directed (if required) to intercept or interfere by means of a close orbital rendezvous.

- Non-Kinetic Physical: Technology meant to create interference or temporary damage and physical impact on space systems without physical contact. This includes electromagnetic pulses or directed energy (laser beams or microwave bombardments) technologies.

- Electronic: Technology that uses radiofrequency energy to interfere with or jam communications to or from satellites but does not cause permanent physical damage.

- Cyber: Technology that uses software and network techniques to compromise, control, interfere, or destroy computer systems linked to satellite operations.

Amongst the four categories of the threats identified above, this work focuses on analysing cyber threats. There are certain commonalities between cyber threats with the electronic threats. Here more than the technology, it could be said that the overall camaraderie in approach shows some similarities. Hence, a brief review of electronic threats is in order before getting to the debate on cyber threats to space systems.

An electronic attack involves electromagnetic energy and directed energy to control the electromagnetic spectrum or attack a rival. Presumably, hither the targets would be mostly the communications to (and from) the satellites and communication satellites themselves. Satellite communications systems are susceptible to uplink and downlink

[15] A major debate on Counterspace Capabilities could be found at https://swfound.org/counterspace/.

jamming or spoofing. The jammer needs to operate in the same radio band as the system being jammed. Uplink jammers on the ground should be powerful enough to undertake the jamming operations. But the ground-based downlink jammers need not be much powerful. Commercial satellite ground communications equipment has electronic jamming capabilities that can easily be used to disrupt the functions of some satellites. Many countries also have military jamming capabilities. Most commercial and civil satellites lack built-in protection measures and are vulnerable to electronic attacks. Various examples of satellite jamming or interference include intentional jamming or jamming that happened due to the interference caused (in such cases, the satellite location becomes an issue and mainly such positioning happens without the approval of the International Telecommunications Union, ITU, which is otherwise mandatory). One famous case of electronic interference is the 1997 South Pacific Island nation of Tonga case. Here, Tonga had accused Indonesia of deliberately jamming APT's Apstar-1A, which had been moved to the 134-degree east orbital slot.[16] Possibly, this was a deliberate act by Indonesia.

Presently, more sophisticated technologies for satellite jamming are emerging. For instance, Russia has developed a handheld GPS jamming system.[17] A small unit the size of a mobile (one-watt version) can deny access to GPS (aircraft's GPS receiver signal) out to 50 miles; a slightly larger version can jam up to 120 miles. In general, military communications sent via commercial communications satellites (COMSATs) are mainly vulnerable to jamming. Any off-the-shelf satellite communication (SATCOM) equipment could be easily used to jam commercial COMSAT links.[18]

Many states understand that control of space is crucial for military activities. Satellite-based inputs are increasingly becoming vital for the survival of the defence forces. The primary limitation of space launches is the cost factor. It is costly to carry weight into the space. The price of reaching the low earth orbit (LEO) could be more than US$10,000 per Kg. Private industries are working towards lowering this price (Space X can manage this with an approximate cost of US$ 3000). It is also important to note that carrying much weight to space is technologically challenging. Hence, the satellite's casing is usually intestinally kept very thin and brittle, mainly due to cost and technology issues. Owing this, even a small amount of debris can impact the life of the satellite. To overcome such weaknesses, states have started investing in satellite-hardening technologies. Hence, in future, launching a physical attack (like using KKV) may not always be rewarding.

---

[16] Tom Wilson, "Threats to United States Space Capabilities", https://spp.fas.org/eprint/article05.html#21

[17] Kevin Rothrock, "The Kremlin Eats GPS for Breakfast", *Moscow Times*, October 21, 2016, https://www.themoscowtimes.com/2016/10/21/the-kremlin-eats-gps-for-breakfast-a55823,

[18] Tom Wilson, "Threats to United States Space Capabilities", https://spp.fas.org/eprint/article05.html#21,

Nevertheless, the options like jamming the satellites or launching a cyber-attack on the satellites remain viable (and preferred) options. This is not to argue that countermeasures against such attacks are impossible to conceive. However, it has been observed over the years that the cyber domain is dynamic and new threats continue to emerge. Also, in a relative sense, launching a cyber-attack is very cost-effective.

Satellite systems and related services remain vulnerable to probable cybersecurity threats and hostile attacks. Since, for all these years, such a threat was not much envisaged, it has been realised that there are possible gaps in various software packages and related algorithms, which the potential cyber hackers easily exploit. Mainly, there could be issues with imperfect codes from the point of view of cyber security. Such codes would be perfectly able to do the job they have been designed for. However, they may lack the mechanism to judge the quality of incoming data (the act of a hacker), and there could be no desired security walls.

It is important to factor in a satellite's entire lifecycle to realise the possible options for cyber intrusion. A bug will be made to enter the satellite system during its development on the ground. Hence, all due care needs to be taken since the initialisation of the satellite development project itself. At every step, from manufacturing to launch to operationalising and functioning of the satellite, there could be options available for the intruder. The ground segment comes into the picture when the satellite system's monitoring and contacting begin from the launching stage. The possible intruder could look for various options for entry into the system, and even the Telemetry, Tracking and Command (TT&C) systems could offer an opening for the intruder. There are some known cases where such forced entry into the system has happened.

Before discussing various technical and geopolitical aspects of such attacks, the following section enumerates some incidences where such attacks have taken place and caused significant damage. Some instances mainly associated with GPS jamming are mentioned in the section covering cyber threats to space security.

FROM THEORY TO REALITY: DOCUMENTED CYBER ATTACKS IN THE SPACE DOMAIN

It is challenging to trace the actual occasions regarding the satellite systems getting hacked by cyber means. There could be many reasons for this. Possibly, initially some years back, when such a threat was not known, satellite operators could not have even realised what went wrong with their space-based systems and why there was a disturbance in the services. Subsequently, even after the nature of the threat has become apparent, there could still have been some geopolitical and economic apprehensions from the sides of the satellite operators regarding openly accepting the jamming/hacking of their space systems. Also, in the field of cyber, attribution is always an issue. Hence, states always find it uneasy to openly accept the hack since they cannot announce the crime's perpetrators, at least immediately. Owing all this, there is a possibility that, all space infrastructure-related cyber-attacks are not publicly known. But this is slowly changing, and inputs are available regarding various hacks associated with space systems. On occasions, there is circumstantial evidence indicating an attack, while in some cases, there are direct indications.

It is important to note that an attack on operational satellites is not the only threat to the space architectures of the states/agencies. To date, various types of cyber-attacks involving satellites in space, during the launch phase, or on the ground infrastructure which controls satellites. Also, various systems storing satellite-acquired data have been attacked. Some information is available (in open source) regarding various such types of attacks. For many decades one of the most robust space programmes in the world has been that of the US. This programme also remains the most cyber-threatened space programme. The National Aeronautics and Space Administration (NASA) is an independent agency responsible for the US space programme. Generally, NASA has been found as a transparent agency which puts various information concerning its activities in the open domain. Some such examples, mainly associated with NASA, are mentioned below.

NASA has a history of being targeted by hackers, with many incidents dating back to the late 1990s. It has been argued that such attacks have some linkages with Russia and China. It has been found that NASA's networks have been mainly vulnerable due to the accessibility of their systems to outside researchers and contractors. There have been many cases when the attackers remained undetected for several months and were able to access and steal a large amount of data.[19]

[19] Michael Benis, "NASA's Network Security Breaches: A Brief History", *LinkedIn*, Jan 9, 2023, https://www.linkedin.com/pulse/nasas-network-security-breaches-brief-history-michael-benis; Keith

As per the US intelligence agencies, six known examples of hackers successfully interfered with or even commanded unauthorised manoeuvres of NASA satellites before 2011. Many of these attacks happened between 2007 and 2008. Some known cases include the damage caused to the US-German ROSAT X-Ray satellite. This satellite was launched on Jun 01, 1990. Interestingly, this satellite had a design life of 18 months. However, it operated for around eight years. The operations were shut down on Feb 12, 1999. As per some reports, the hackers had taken over the control of the spacecraft by entering the computers of the Goddard Space Flight Center in Maryland and were able to disturb the settings of the solar panels. This satellite was used for peering into deep space, was rendered useless after it turned suddenly towards the sun damaging the High-Resolution Imager by exposure. The attack supposedly originated from Russia. However, some experts believe that though there was a security breach with the NASA network in 1998, there is still no evidence that a cyber-attack had led to the failure of ROSAT, and the satellite got damaged after an attitude control problem.

It was reported that in 1999, the hackers had taken control of Britain's SkyNet satellites and asked the government for ransom. Britain had a three-satellite system called Skynet 4, a family of military communications satellites. It was reported that the hackers had intercepted the link between Skynet's control centre and the ground station. Possibly, the hackers had succeeded in reprogramming a satellite control system. This blackmail threat was a nightmare scenario for the British security forces. However, officially the government had denied the happening of any such activity. In 1997, trespassers had penetrated computers in the X-ray Astrophysics Section of a building on NASA's Goddard Space Flight Center campus. They had seized computers delivering data and instructions to satellites. They successfully transferred vast amounts of information, including e-mails, through a series of stops on the Internet to computers overseas.

During 1999-2002, a 15-year-old Jonathan James succeeded in penetrating the US DoD and NASA computers. James entered 13 computers at the Marshall Space Flight Center in Huntsville, Alabama. He stole and downloaded a lot of data, including information about the temperature and humidity within the living quarters at the international space station (ISS).[20] It also included stealing secret data on rocket engine designs: Delta and Atlas rockets that power intercontinental missiles, Space Shuttle's main engines enhancements, and Lockheed's F-35 Joint Strike Fighter. The information is supposed to have made its way to China.

Epstein and Ben Elgin, "Network Security Breaches Plague NASA," *Newsweek*, November 20, 2008, https://www.cs.clemson.edu/course/cpsc420/material/Papers/NASA.pdf,

[20] Gary Cohen, "Throwback Attack: A Florida teen hacks the Department of Defense and NASA", April 08, 2021, https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-a-florida-teen-hacks-the-department-of-defense-and-nasa/,

During 2003-2006, an alleged Chinese operation codenamed 'Titan Rain' targeted US defence and aerospace installations, including NASA, gathering sensitive military data. The information collected included a stockpile of aerospace documents with hundreds of detailed schematics about propulsion systems, solar panelling, and fuel tanks for the Mars Reconnaissance Orbiter. Titan Rain, perhaps was the first case of state-sponsored espionage from China. The operation compromised several agencies within the US and UK governments. Along with NASA, various other government agencies came under cyber-attack. The attacks were publicly revealed in 2005 but have happened since at least 2003. The UK government agencies were reported under attack till 2007.

A cyber-trespasser is believed to have poked around NASA's Ames Research Center in Silicon Valley in 2004. The situation led to a panicked technician pulling the plug on the facility's supercomputers to limit the loss of secure data.

A malignant software programme (2005) gathered data from computers in the Kennedy Space Center's Vehicle Assembly Building. This location was undertaking the maintenance of the Space Shuttle. The programme, called stame.exe, sent information regarding the Space Shuttle to a computer system in Taiwan. The hack was simultaneously carried out at various NASA centres, and at least 20 gigabytes of compressed data (the equivalent of 30 million pages) was routed to the system in Taiwan.

In 2006, top NASA officers were misled into opening a fake e-mail. An email was clicked by NASA officials, which was an infected link. This led to the agency's Washington headquarters allowing budget and financial information access. Also, this led to the leakage of information regarding the size and scope of every NASA research project, space vehicle deployment, and cutting-edge satellite technology. Due to concerns about computer network exploitation during 2006, NASA facilities barred all incoming Word attachments from its computer systems.

The US Air Force accused Chinese hackers during 2007-08 of temporarily jamming their satellites. The Chinese were known to have used the connection from a ground station to affect the operation of the earth observation Landsat 7 and Terra (EOS AM-1) satellites. Perhaps, China was testing the vulnerabilities of the US space systems. The Landsat 7 satellite encountered 12 minutes of 'interference' in Oct 2007; the Terra had such interference lasting for two minutes during June 2008. While a month later, the Landsat was again impacted for 12 minutes. The Chinese 'testing' continued till Oct 2008, when the functioning of Terra got interfered with for nine minutes.

On June 20, 2008, Terra EOS (earth observation system) AM–1, a NASA-managed programme for Earth observation, experienced two or more minutes of interference. The responsible party achieved all steps required to command the satellite

but did not issue commands.[21] While on October 22, 2008, Terra EOS AM–1 experienced nine or more minutes of interference. During both these incidences, hackers allegedly gained control of the satellite, although they did not execute any commands.[22]

One another case happened in 2008 when hackers had loaded a Trojan horse in the computers at Johnson Space Center in Houston, Texas. These hackers then used the Trojan horse to access the uplink to the International Space Station and disrupt certain operations onboard, such as email. The attack was helped by ISS onboard computers running older software for which security fixes are no longer available. Two years later, a Chinese national was detained for hacking activity targeting US government agencies. Seven NASA systems, many containing export-restricted technical data, were compromised.

On April 8, 2010, China Telecom advertised erroneous network traffic routes that sent US and other international Internet traffic through Chinese servers for around 18 minutes. Other servers worldwide immediately adopted these routes, sending all traffic to about 15% of the Internet's destinations through Chinese servers.[23] This incident affected traffic to and from US government and military sites, including those for NASA.

A Romanian hacker TinKode supposedly obtained sensitive information from NASA's Goddard Space Flight Center and the European Space Agency (2011), which he made publicly available online. The information included Login credentials for admin, content management, databases, email accounts, file upload (FTP), and other vital systems. NASA's Jet Propulsion Laboratory (JPL) had reported suspicious network activity (2011) involving Chinese-based IP addresses, which gave intruders access to most of JPL's networks.

In 2013, a former NASA contractor and a Chinese national, Bo Jiang, was arrested as he was attempting to return to China with a large amount of information that he was not entitled to possess. There were major concerns in NASA about such espionage and export control violations. This act led NASA to undertake various preventative and security measures. They had shut down access to an online database and banned new requests from Chinese nationals seeking access to its facilities. Also, Chinese contractors working at NASA centres implemented a complete ban on remote computer access.

[21] Michael Khan, "Are US satellites being hacked by China?" December 16, 2011, https://scilogs.spektrum.de/go-for-launch/us-bericht-china-hacken-satelliten-kontrolle/

[22] "Counterspace Weapons 101", June 14, 2022, https://aerospace.csis.org/aerospace101/counterspace-weapons-101/

[23] See, Nate Anderson, "How China swallowed 15% of 'Net traffic for 18 minutes", ASR Technica, November 18, 2010, https://arstechnica.com/information-technology/2010/11/how-china-swallowed-15-of-net-traffic-for-18-minutes/

Understanding the nature of China's threat in 2013, the US Congress passed a provision prohibiting the Commerce and Justice Departments, NASA, and the National Science Foundation from buying any information technology system produced, manufactured, or assembled by China. Before this, the Wolf Amendment (a law) was passed by the US Congress in 2011, which prohibits any form of China and NASA collaboration.[24]

There have been cases of Chinese hackers meddling with the US weather systems and satellite network during 2014. The Chinese hackers had interfered for 4-5 minutes in the conversation through video chat via satellite during a high-profile Indian government meeting in October 2017[25]. China had denied any such involvement. Also, the affected states were not much forthcoming regarding the occurrence of such attacks.

Around 2015, Kaspersky Lab, a cybersecurity solutions lab, identified that a group of Russian-speaking threat actors, active for over ten years, have been hijacking satellite-based Internet links to hide their whereabouts.[26] This group was known as the Turla cyber-espionage group (Snake or Uroburos). They had identified an easy and inexpensive method to hijack downstream bandwidth from various ISPs and packet-spoofing to obtain a much higher degree of anonymity than any other conventional method, such as renting a Virtual Private Server (VPS) or hacking a legitimate server. It was inferred that the initial investment could have been around $1,000 for undertaking such attacks, and ongoing maintenance costs have been even lesser per year. It was found that for high-profile targets, the attackers exploit an extensive satellite-based communication mechanism in the final stages of an attack to help them to hide their traces.

---

[24] Different information mentioned about NASA suffering from cyber-attacks is based on, Jason Fritz, "Satellite hacking: A guide for the perplexed," Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies: Vol. 10 (1), http://epublications.bond.edu.au/cm/vol10/iss1/3

[25] Various cases discussed here are mostly based on sources such as, Younis Dar, "Why Satellite Hacking Has Become The 'Biggest Global Threat' For Countries Like US, China, Russia & India?", *Eurasian Times*, October 24, 2020, https://eurasiantimes.com/why-satellite-hacking-has-become-the-biggest-global-threat-for-countries-like-us-china-russia-india/; Lev Grossman, "Did Hackers Hijack a British Military Satellite?", *Time*, March 01, 1999, https://content.time.com/time/magazine/article/0,9171,20673,00.html; "British hackers attack MoD satellite", *Telegraph*, March 01, 1999, https://web.archive.org/web/20070510032306/http://www.telegraph.co.uk/connected/main.jhtml?xml=/connected/1999/03/04/ecnhack04.xml; "ROSAT reentry", *Jonathan's Space Report*, No. 649, October 25, 2011, https://planet4589.org/space/jsr/back/news.649.txt,

[26] It is world's largest privately owned cybersecurity companies. They operate in around 200 countries and territories and have offices in more than 30 countries. However, it may be noted that the US federal government had banned this antimalware provider in federal information systems in 2017 owing to the concerns about Kaspersky's links to the Russian government.

The tactics used by Turla group to hide the location of its Command-and-Control (C &C) servers: [27]

• The group first 'listens' to the downstream from the satellite to identify active IP addresses of satellite-based Internet users who are online at that moment.

• They then choose an online IP address to mask a C&C server without the legitimate user's knowledge.

• The machines infected by Turla are then instructed to exfiltrate data towards the chosen IPs of regular satellite-based Internet users. The data travels through conventional lines to the satellite Internet provider's teleports, then up to the satellite, and finally down from the satellite to the users with the chosen IPs.

It was a very carefully developed plan by the Turla attackers. They had instructed infected machines to send data to ports closed mainly by default. A valid user's personal mechanises (PCs) will simply drop these packets while the Turla C&C server, which keeps those ports open, will receive and process the exfiltrated data. The infection is known to have spread to more than 45 countries. Incidence indicates that end users' operations could be a threat despite all precautions to make the system tamper-proof.

During 2020, two Russian COSMOS satellites (Cosmos 2542 and sub-satellite 2543) in orbit had come extremely close, within 160 km of the US spy satellite. Cosmos 2542, a Russian inspection satellite, had synchronized its orbit with USA 245.[28] It is not clear why such a close approach was made. There were also fears that the Russian satellite could have intentionally collided with the US satellite. It is unclear what the exact intent was over here, was that a (satellite) kill mission or some offensive singling agenda? Luckily, the event passed without any damage. There are some major learnings from this event. It demonstrated that 'satellite attacking a satellite' is no longer science fiction but a possible reality. This incident is not a classic case of any cyber-attack on satellite. However, it is imperative to note that the entire command and control system for undertaking such dangerous manoeuvres has significant cyber dependence and some minor mistakes to lead to dangerous situations.

On Mar 17, 2022, the US government advised satellite operators to put their guard up in the wake of a cyberattack that disrupted internet services in Europe provided by Viasat's KA-SAT. It was a cyberattack by unidentified hackers, possibly Russian. It was a remote sabotage of a satellite internet provider's service. The

[27] Mike Lennon "Russian-Speaking Turla Attackers Hijacking Satellite Internet Links", *Security Week*, September 09, 2015, https://www.securityweek.com/russian-speaking-turla-attackers-hijacking-satellite-internet-links/

[28] "2 Russian satellites are stalking a US spysat in orbit. The Space Force is watching", *Space.com*, https://www.space.com/russian-spacecraft-stalking-us-spy-satellite-space-force.html

broadband satellite internet access in Ukraine was disturbed when the Russian invasion of Ukraine was happening. Possibly, it was part of the preparatory stage of the battle. The digital blitz on the satellite service began on Feb 24, 2022, between 5 am and 9 am, the same period Russia had started with the initial phase of the battle with missile launches. This was when the satellite modems belonging to many European customers were hit offline. The hackers had disabled modems that communicate with Viasat Inc's KA-SAT satellite that supplied internet access to some European customers, including Ukraine[29]. The major sufferer of this attack was the German energy industry.

German wind turbine operators faced major faults with the satellite connections of their systems. There was a massive disruption in the operations of around 5,800 wind turbines in central Europe, which was felt from Feb 24, 2022, onwards. The disruptions were known to have impacted 11 gigawatts (GW) worth of wind turbines. It was realised that the cyber disruptions had affected about 30,000 satellite terminals used by companies and various organisations associated with the operations of these turbines. As mentioned earlier, the disruptions occurred due to the failure of the KA-SAT communication satellite belonging to Viasat. There was a clear indication of the cyber-attack by the Russians. However, in all probability, it was not an intended attack on the German wind turbine network. Still, the timing matched with Russia's invasion of Ukraine, possibly due to collateral damage from a cyber-attack on a primarily military target by Russia[30]. It needs to be realised that satellite services play a very vital role towards operating modern-day military machinery. The Russian thinking would have been about stalling any immediate response from the Ukraine forces after they had invaded that country. It took more than two weeks for Viasat services to return to normalcy.

On Oct 29, 2022, one of the world's largest astronomical observatories suffered a major cyber shock. A cyber-attack occurred on Chile's Atacama Large Millimeter Array (ALMA) observatory. This observatory is a constellation of 66 radio telescopes worth about $1.4 billion. The entire unit captures high-quality images of the weak radio waves emitted by distant astronomical objects (which could be as far as 13 billion light years away). The attack on ALMA's computer systems forced the agency to shut down servers and operating computers. It was an extensive attack which halted all

[29] Sandra Erwin, "Cyber warfare gets real for satellite operators", *Space News*, March 20, 2022, https://spacenews.com/cyber-warfare-gets-real-for-satellite-operators/ and James Pearson et al, "U.S. spy agency probes sabotage of satellite internet during Russian invasion, sources say", *Reuters*, March 12, 2022, https://www.reuters.com/world/europe/exclusive-us-spy-agency-probes-sabotage-satellite-internet-during-russian-2022-03-11/

[30] Marian Willuhn, "Satellite cyber-attack paralyzes 11GW of German wind turbines", *PV Magazine*, March 01, 2022, https://www.pv-magazine.com/2022/03/01/satellite-cyber-attack-paralyzes-11gw-of-german-wind-turbines/ ; Subhash Yadav, "Loss of control over Enercon Wind turbines due to satellite outage highlights cyber risks, March 02, 2022, https://www.saurenergy.com/solar-energy-news/loss-of-control-over-enercon-wind-turbines-due-to-satellite-outage-highlights-cyber-risks

astronomical observations. Some major testing efforts (for precision calibration etc.) were required once the system was recovered before declaring the telescopes functional again.[31]

All the incidents mentioned above clearly indicate the nature of the threat to satellite-related infrastructure is real and increasing. The following section discusses the kinds of existing cyber threats to space security.

[31] Daryna Antoniuk, "Cyberattack on observatory in Chile raises concerns about security of space tech", *The Record*, November 07, 202, https://therecord.media/cyberattack-on-observatory-in-chile-raises-concerns-about-security-of-space-tech/?utm_source=substack&utm_medium=email; Liam McAneny, "Chilean Telescope Back Online after Cyber Attack", Dec 28, 2022, https://www.cybersecurityconnect.com.au/technology/8538-chilean-telescope-back-online-after-cyber-attack

IDENTIFYING AND EXAMINING CYBER-THREATS TO SPACE SECURITY

Over the years, satellites have become an inseparable part of human sustenance. Every country in the world is not having satellites of their own. Still, they continue to depend on satellites' assistance for various purposes. From television signals to navigational pointers to mobile and other commutations to knowledge of weather situation, various forms of information on which the daily survival of the citizens of this world depends is significantly based on the inputs received from various satellite systems.

This (over) dependence on satellites comes with some limitations too. The most obvious limitation is that space infrastructure becomes an obvious target for any adversary. As mentioned here, different options exist to destroy or disable the adversary's satellite. Cyber is emerging as one of the most important and viable options. To understand the nature of cyber threats, it could be prudent first to identify how the satellite systems broadly function.

Information Technology (IT) based systems/applications that most space systems have are complex and difficult to hack. However, the back-end systems are increasingly linked with commercial front-end systems, which hackers could easily crack.[32] In the present-day context, space-based systems are called 'cyber-physical' systems. Each system consists of space, ground, and user and link segments[33]:

Space Segment: The satellite or spacecraft itself orbits above the Earth.

Ground Segment: It comprises everything that aids in launching and connecting with the satellite from Earth. Launch facilities, data relay stations, control centres, ground stations, various receiving stations within and outside the country, ship stations, and specific radar installations become a part of the ground segment. Any forced (digital) entry in the ground segment allows the attacker to manipulate command and control systems and tamper with data. Because of their role in data collection, the ground stations and terminals get directly exposed to the threat of cyber spying from various

[32] Chuck Brooks, "The Urgency to Cyber-Secure Space Assets", *Forbes,* https://www.forbes.com/sites/chuckbrooks/2022/02/27/the-urgency-to-cyber-secure-space-assets/?sh=45845c3a51b1e,

[33] Frank Schubert, "Satellite cyber security is more important than ever – here's why", January 31, 2023, https://www.protect.airbus.com/blog/satellite-cyber-security-is-more-important-than-ever-heres-why/; "Space Based Platforms And Critical Infrastructure Vulnerability (Mccreight)", in R.K. Nichols (et.al)., Space Systems: Emerging Technologies And Operations, New Prairie Press, 2022. Available at, https://kstatelibraries.pressbooks.pub/spacesystems/chapter/exploration-of-key-infrastructure-vulnerabilities-from-space-based-platforms-mccreight

actors. Furthermore, due to the military dependence on satellites, their importance to national security renders ground systems prime targets for disruption, hacking and physical damage. Various cyberattacks on the ground infrastructure exploit network vulnerabilities and permit the attacker to trap ground station personnel to download their computer systems' different malware and Trojans without releasing the nature of the threat. Clever entry into the ground station's network helps attackers to access the satellite directly. With this unfriendly access, the attacker can execute a Denial of Service (DoS) attack and possibly take over Industrial Control Systems (ICS). With this, the attacker offers itself two options: either to take over the control of the satellite or to cause damage to it.

Space Segment: The satellite or spacecraft itself orbits above the Earth. Presently, old satellites are more vulnerable to cyber attackers owing to their limited capability to face cyber-attacks. At the same time, the threat to new satellites continues to exist since the field of cyber security is dynamic and new cyber threats are continuously getting invented. Old satellites were built with no (or very little) cyber security consciousness; today, small satellite manufacturers do not prioritise security to save costs. Cyber threats to space segments typically stem from vulnerabilities in ground stations, network components, and receivers that receive the data from the satellite, thus allowing the attacker to infiltrate the network but not get detected. Another hazard may involve introducing malware into the satellite's hardware in the supply chain. Penalties for cyberattacks on satellites could also be provoked due to the rising connection and use of Internet of Things (IoT) devices. Major disruptions to communication channels across countries could happen if there is an attack on a communication satellite. Owing to increasing human dependence on satellites, any such attack could lead to chaos and even risks of compromising national security.

Link Segment: Constitutes of all-important communication links transmit information between various segments. This involves the signal transmission between the satellite, ground station, and satellites. The most perceived threat consists of the jamming of GPS signals. This group of satellites launched for global navigation rely on radio signals sent from the satellite to identify the users' location. It has been found that the GPS jammers end signals over the same frequency as the GPS device. This allows the attacker to override or distort the GPS satellite signals. Such jammers are commonly accessible and do not cost much. This increases the possibility for non-state or poor state actors to opt for this option if required.

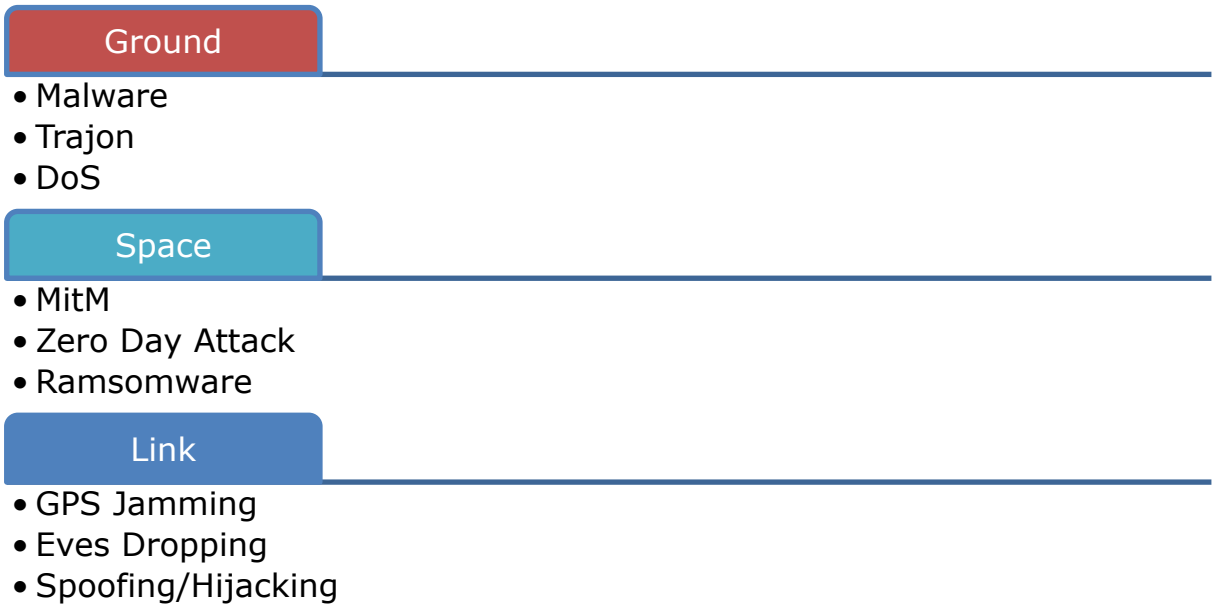
So technically, a satellite cyber-attack could be viewed as an attack which intentionally interferes with any of the above segments, covering both the physical and cyber world. Such attacks typically have three purposes, to ex-filtrate data (break confidentiality), tamper with data (break integrity), or disrupt a service (break

availability). This amounts to jamming and spoofing satellite navigation signals in the physical world. In the cyber world, it could mean silently intercepting unprotected data.

It is essential to realise that any organisation with satellites of their own or one relying on space-based systems could be severely impacted by such attacks.

There would be a range of affected parties, from governments to militaries to private agencies to common people. The entire society could also get adversely impacted by such attacks. The assaults could be made by any agency or even individual, and they need not be state-centric all the time. Various actors could carry out these cyber-physical attacks, including state and non-state actors and hacktivists. Even some people can carry such attacks for the sake of excitement too. With the increasing number of satellites in space, the possibility of attacks increases simply because there are more targets out there.

The following diagram presents the nature of segment-wise threats to space systems:[34]



A brief explanation of the terms used above:

Malware (malicious software) attack affects illegal actions on the victim's system.

Trojan is a type of malware.

Ransomware is malware that threatens to block user access unless a ransom is paid.

[34] "Space Satellites and Cybersecurity", https://x-phy.com/space-satellites-and-cybersecurity/

DoS (denial-of-service) is carried out by a nasty actor who aims to render a computer or device unavailable to its intended users.

MitM (man in the middle) attack: A perpetrator positions himself in a conversation between a user and an application to eavesdrop or impersonate one of the parties. The idea is to steal personal information.

Zero-day-attack: Targeting a software vulnerability unknown to the software or antivirus seller.

Jamming is when the single is intentionally blocked (by electronic/cyber interference). Spoofing is when a GPS receiver is made to calculate a false position. Hacking means the intentional compromise of digital devices.

Eavesdropping means secretly (stealthily) listening to others (victims') conversation or communications.

There could be different methods to undertake a cyber-attack on space infrastructure. It could involve the following: [35]

- The majority of attacks could involve acts of jamming, spoofing, and hacking. Generally, such attacks could happen on communication networks.
- Attacks on satellites could happen by targeting their control systems or mission packages. It is also possible (a bit difficult) to take control of the satellite to exploit its inherent capabilities. After taking over the control of the satellite, the attacker could shut it down, alter its orbit, take control of its solar panels, or deliberately expose it to the sun in such a fashion (damaging levels of highly ionizing radiation) that the damage could be caused.
- The more accessible options are possibly available, which is about targeting the ground infrastructure. Here attacks could be launched on satellite control centres, the associated networks and data centres and any other facility linked to the data reception, data broadcasting, up-linking and downlinking nodes or data stored facilities. There are chances that any such attack could immediately impact the weather transmission and weather forecasting systems.

Following could be some of the possible attacks which could (or have) happen (happened) during various satellite missions:

[35] David Livingstone and Patricia Lewis, "Space, the Final Frontier for Cybersecurity?", *Chatham House*, September 2016, https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf

- Sabotage of ground system capabilities by exploiting the ground system to network with a satellite maliciously
- Communications hacking on Telemetry, Tracking and Control (TT&C) systems through command link injection, replay attacks, or electronic attacks like jamming and spoofing
- Malicious features entrenched during hardware development and looking for vulnerability exploitation
- Software-defined radio compromise
- Software flaws and vulnerabilities exploitation
- Insider threats

From the point of view of countermeasures against the possible cyber-attacks on space infrastructure, it is important first to understand the diverse nature of the threat. Since cyberattacks can mostly occur across multiple segments like space, communications links, and ground setup, there is a possibility of attackers identifying different approaches to plan and launch an attack. The attacker could work towards denying ground telemetry and mission data processing practices, disallowing all communications to the satellite, blocking the ground's ability to control the satellite, conceding mission data, infiltrating mission data, or even affecting commands on the satellite which is not programmed.

While analysing the cyber threats and vulnerabilities to different satellite missions, it is essential to factor in the physical nature of the space vehicle and its area of operation (nature or orbit, altitude etc.). The satellite must be able to communicate, maintain trajectory, and deliver power to mission-significant components. Exclusively for launching a cyberattack following satellite subsystems could be viewed as vulnerable:

- Attitude Determination and Control (AD&C)
- Command and Data Handling (C&DH)
- Electrical Power and Distribution Subsystem (EPDS)
- Propulsion Subsystem (PS)
- Structures and Mechanisms Subsystem (SMS)
- Telemetry, Tracking, and Command (TT&C)
- Thermal Control Subsystem (TCS)

The boundary is typically considered the communications link (radio frequency link/ground system) for satellites. If the boundary is breached, the system reaming stable is less likely. This is because very little internal protection exists within the satellite. These limitations allow the adversary to gain access to the system.

It has been observed that in recent times cyber-attack is emerging as an attractive option for adversaries. Such attacks are easy to plan and are most cost-effective compared to other anti-satellite options[36]. Moreover, cyber-attacks need not necessarily be 'point targets' (from an impact perspective) and can have a large attack radius, targeting a complete constellation of satellites ('area targets'). Some operational satellites in space (say weather or comminutions satellites) have been there for around one decade. Such satellites have a life period of fifteen to twenty years and were launched some years back. They mostly have old systems without proper firewalls and hence are unsafe. When such systems were designed, the cyber threat angle was prominent. More importantly, software updates for the systems in space are not preferred for various reasons. Hence making old but operational satellites up-to-date from a cyber security perspective is not much feasible.

Broadly, it has been observed that since the cyber threat has become prominent, attacks on space systems are happening using techniques like jamming, spoofing, and hacking. Jamming is an old art—some of the first instances of jamming date to the beginning of the 20th century. In 1902 and 1903, the Royal Navy and US Navy are known to have tried to jam radio signals by transmitting 'on top' of the signals to be jammed. During World War I, some naval engagements involved radio jamming. Subsequently, around 1935, Radar was first tested in England, and within the next three years, the inverters of this system also started testing (successfully) techniques to jam this system[37]. It could be said that the extrapolation of a known understanding of jamming techniques is now getting implemented in the space sector.

Satellite jamming is a method of electronic violence that interferes with communications travelling to and from a satellite. It is achieved by emitting noise of the same radio frequency (RF) within the field of view of the satellite's antennas. As discussed earlier, space capabilities constitute a space and ground segment. Then there are communication nodes or links which tie them together. Satellite jammers threaten opponents' abilities via the communication segment. This act can be performed by using land-based ship-based, or air-based systems. Such acts are not fully fatal attacks. The target system returns to its original state once the jamming signal is turned off.

There are two key types of satellite jamming. One is uplink jamming. There is an intentional interference with the signal from a ground station or user terminal to the

[36] The above discussion is based on "Cyber security in the skies – protecting satellites from attack", August 12, 2021, https://trustedcomputinggroup.org/cyber-security-in-the-skies-protecting-satellites-from-attack/; Also, Zac Amos, "How secure are satellites from cyber-attacks?", *Cyber Talk*, May 26, 2022, https://www.cybertalk.org/2022/05/26/how-secure-are-satellites-from-cyber-attacks/, and "Protecting Space Systems from Cyber Attack", *Medium*, March 31, 2022, https://aerospacecorp.medium.com/protecting-space-systems-from-cyber-attack-3db773aff368.

[37] Daniel T. Kuehl, "Blinding Radar's Eye: The Air Force and Electronic Countermeasures in World War II", *Air Power History*, Vol. 40 (2), Summer 1993, pp. 14-24

satellite. Here, the idea is to confuse the satellite, and for this purpose, an RF signal of the same frequency as the targeted uplink signal is transmitted to the satellite. This makes it difficult for the satellite transponder to differentiate between the jamming and actual signals. Two, downlink jamming. Here the target is the single sent by satellite to ground-based or airborne receivers. This signal is disrupted using RF signals that mimic the frequency of the downlink signal. The purpose is to prevent ground users from receiving transmissions from the satellite.

Technically, uplink jamming is more complex because greater transmitting power is required to reach the satellites' transponders. However, this type of jamming is more effective, owing to its ability to degrade the satellite's signal for all its users. The impact of downlink jamming is limited and local. Since the impact of such jammers happens inside the field of view of the receiving terminal's antenna, the impact becomes restricted[38]. It needs to be noted that jamming is not a very difficult 'art' to master. Presently, jamming technologies are commercially available too. There have been various instances of jamming signals (for jamming space infrastructure) originating from states which are not much known for their technology proficiency.

Continuously, satellite jamming incidences do get reported. The after-effects of such jamming incidents have the potential to cause major disruptions. It has been observed that many jamming incidents occur in the case of the global navigation satellite system (GNSS). The received GNSS signal has low power. This is because it travels a very long distance, and the nature of the signal's propagation medium adds to the reduction in power. Therefore, GNSS signals are vulnerable to signal interference, which can initiate severe degradation or interruption in GNSS position, navigation, and timing (PNT) services[39]. Such jamming could lead to misguiding or manipulation of the signal. Some incidences of satellite jamming and the impact caused are indicated below:

The fight for the freedom of information is continuing in states like Iran for many decades. There are many Persian-language satellite TV channels broadcasting into Iran from the diaspora. The Iranian government views these channels as an attempt by the West to push for a change in the political structure of Iran. Here the state-sponsored satellite jamming is known to be taking place for some time now. Such satellite jamming

[38] Pavel Velkovsky, Janani Mohan, And Maxwell Simon, "Satellite Jamming: A Technology Primer", April 03, 2019, https://res.cloudinary.com/csisideaslab/image/upload/v1565982911/on-the-radar/Satellite_Jamming_Primer_FINAL_pdf_bdzxwn.pdf

[39] Haidy Elghamrawy et al, "Experimental Evaluation of the Impact of Different Types of Jamming Signals on Commercial GNSS Receivers", *Appl. Sci*. 2020, 10(12), 4240, https://www.mdpi.com/2076-3417/10/12/4240

is a form of censorship like Internet censorship, whereby the Iranian government forbids access to and inhibits the free flow of information[40].

It is a speculation, and the US administration is unlikely to offer any indication about the veracity of this claim. The US RQ-170 Sentinel drone was found in Iran in December 2011. In all possibilities, the stealth drone was captured by spoofing its GPS coordinates, a hack that deceived the drone into landing in Iranian territory instead of where it was programmed to touch down. Various circumstantial evidence confirms the Iranian claim that they had managed to hoodwink the drone and make it land in their territory.[41]

On October 27, 2018, more than 40 drones crashed during a 100-LED-equipped drone show organised to celebrate the annual Wine & Dine Festival in Hong Kong. No one was heart during this indecent. However, the loss of drones caused some US$ 127,500 to the organisers. It was noticed the GPS signals for the drones were interfered with by someone. It was a case of the jamming of GPS signals.[42]

In November 2018, Russia was suspected of disrupting GPS signals during NATO's Trident Juncture exercise. This exercise was conducted from October 25-November 07, 2018, with the participation of the air, land, and sea components. Around 50,000 personnel from 31 NATO Allies and partner countries participated, with hardware of about 250 aircraft, 65 vessels and about 10,000 vehicles. The exercise was held around the regions of central and eastern Norway, the surrounding areas of the North Atlantic and the Baltic Sea, including Iceland and the airspace of Finland and Sweden. The Russian attack involved faking signals by broadcasting incorrect GPS signals structured to resemble genuine ones.[43] The disturbances were noticed from October 16-November 07, 2018. Possibly, Russia did undertake jamming around its Kola Peninsula, the region that shares a common border with northern Norway and Finland. GPS signals for some ships were possibly spoofed, making those ships move away from their planned destination. Experts believed the attacks were essentially

[40] "Satellite Jamming in Iran: A War over Airwaves", November 2012, https://www-tc.pbs.org/wgbh/pages/frontline/tehranbureau/SatelliteJammingInIranSmallMedia.pdf

[41] Dan Goodin "US spy drone hijacked with GPS spoof hack, report says", December 15, 2011, https://www.theregister.com/2011/12/15/us_spy_drone_gps_spoofing/

[42] "More than 40 drones crash in Hong Kong light show – no reported injuries", Unmanned Air Space, November 05, 2018, https://www.unmannedairspace.info/uncategorized/40-drones-crash-hong-kong-light-show-no-reported-injuries/

[43] Gil Baram and Omree Wechsler, "Cyber Threats to Space Systems: Current Risks and the Role of NATO", Joint Air & Space Power Conference 2020 Read Ahead, June 2020, https://www.japcc.org/essays/cyber-threats-to-space-systems/

spoofing attacks, which are known to be more complicated than undertaking jamming attacks.[44]

Earlier also, there was a maritime incident with suspicion directed towards Russia, which was reported in the Black Sea in the vicinity of position 44-15.7N, 037-32.9E on June 22, 2017, at 0710 GMT. The nature of the incident is reported as GPS interference.[45] Subsequent analysis indicated that separate vessels were affected and reported identical or very close locations. This is an indication of a large-scale spoofing attack. The ships also reported that their positions would periodically 'jump' from the actual location to the incorrect location, confirming that the GPS receivers could temporarily lose the lock on a spoof set of satellites, reacquire the real ones, and vice versa. This causes the typical random flipping between two well-defined locations.[46]

In December 2019, an intermittent GPS signal loss was experienced by an aircraft landing at Harbin airport in north-eastern China. This is known to have happened owing to a jammer installed at a nearby pig farm. The jammer was intended to deter drones manoeuvred by criminal gangs, mainly to drop packets infected with swine fever onto the herd. The infected meat used to be available at lower prices in the market. This indicates that using illegal jammers can have unintentional consequences for civil aviation, and at times such damages caused to even lead to aircraft accidents.

Norway did report GPS jamming in Jun 2020. The problems were reported from the far north of Norway, close to the Russian border. Norway has been known to be facing the problem since 2017 and believes that Russia could be behind such attacks. They have not been able to prevent such attacks.[47]

During the Ukraine-Russia conflict (2022), it was observed that Russia was intentionally undertaking satellite navigation jamming. Their area of interest was the Moscow region, and the interest appears to be to protect against any long-range strikes

---

[44] Brooks Tigner, "Russian GPS Jamming at NATO's Trident Juncture Exercise", *Real Clear Defense*, November 16, 2018, https://www.realcleardefense.com/articles/2018/11/16/russian_gps_jamming_at_natos_trident_juncture_exercise_113960.html; Also, see, "Trident Juncture 18", *NATO,* October 31, 2018, https://www.nato.int/cps/en/natohq/news_158620.htm

[45] "Mass GPS Spoofing Attack in the Black Sea?" RNT Foundation, July 12, 2017, https://rntfnd.org/2017/07/12/mass-gps-spoofing-attack-in-the-black-sea-maritime-executive/

[46] Michael Jones, "Spoofing in the Black Sea: What really happened?", *GPS World*, October 11, 2017, https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened

[47] Guy Buesnel "Thousands of GNSS jamming and spoofing incidents reported in 2020", *LinkedIN*, December 02, 2020, https://www.linkedin.com/pulse/thousands-gnss-jamming-spoofing-incidents-reported-2020-guy-buesnel

by Ukrainian drones.[48] This Russian military activity has also impacted the aircraft (civilian) flying in the region. GPS jamming incidents are known to have affected aircraft over Finland. This could be viewed as 'collateral' damage. It appears that the Russians may not be to hit the civil traffic, but their military action on occasion has led to causing problems for civilian airliners.[49]

The jamming efforts by Russia were continuously getting monitored. European aviation safety authorities have observed much increase in the incidents of GPS jamming owing to Russia's invasion of Ukraine. The European Union Aviation Safety Agency (EASA) has observed that in some instances, the jamming and spoofing forced aircraft into 're-routing or even to change the destination due to the inability to perform a safe landing procedure.' They had identified four areas where GNSS jamming and spoofing had increased after Russia attacked Ukraine. These areas include:[50]

- Kaliningrad region, surrounding Baltic Sea and neighbouring States.
- Eastern Finland
- The Black Sea
- The Eastern Mediterranean area, Cyprus, Turkey, Lebanon, Syria, Israel, and Northern Iraq.

Ukraine is known to have initiated drone attacks against military bases inside Russia (December 2022). Also, Russia was expecting some US-supported long-range strikes. It was observed that Russia had started jamming the GPS singles over its territory to deceive such attacks. Limited jamming was observed around December 05. However, the intensity has increased since December 11, and the cover area has expanded. Some agencies, like the Estonian defence intelligence firm SensusQ, have been monitoring the situation. During this period, various major Russian cities faced widespread GPS disruptions. The GPS jamming bubbles had covered hundreds of kilometres around cities like Moscow, Saratov, Volgograd, and Penza.

GPSJam system works by watching ADS-B signals sent by planes flying around the world. With these signals, people can track the aircraft's locations in the air. As part of ADS-B data, a plane's GNSS signal strength can be recorded. Space-based monitoring

[48] David Hambling, "Russia is jamming more GPS satellite signals around Moscow", December 23, 2022, https://www.newscientist.com/article/2353060-russia-is-jamming-more-gps-satellite-signals-around-moscow/

[49] Tom Bateman, "Russia responsible for GPS jamming in Europe, French air safety official claims", April 01, 2022, https://www.euronews.com/next/2022/04/01/russia-responsible-for-gps-jamming-in-europe-french-air-safety-official-claims

[50] Victoria Bryan, "EASA warns of intensifying GPS jamming incidents linked to war in Ukraine", March 17, 2022, https://www.aerotime.aero/articles/30513-easa-warns-over-gps-jamming-ukraine-war,

of GPS is also possible. Agencies like Aurora Insight use satellite-based RF sensors, which are known to provide a near-persistent picture of the global RF environment and enable GNSS users to know interference. Russia has been testing electronic warfare systems in Syria for some time now and is also known to be disrupting GNSS signals for some decades. In Ukraine theatre, they are known to have undertaken jamming/spoofing many times. They ensure the unavailability of GPS singles over their land as a defensive measure if required.[51]

A non-technical difference between jamming and spoofing[52] is that: jamming causes the receiver to die, while spoofing causes the receiver to lie. The best example to understand spoofing operations is to recognize them in the milieu of the Global Navigation Satellite System (GNSS) operations. Such systems are the constellation of satellites providing signals (positioning and timing data) from space to GNSS receivers. This entire process is called the use of Global Positioning Systems (GPS) for correct navigation.

GNSS signals have low power. Hence a weak interference source can cause the receiver to fail or to produce dangerously misleading information. The simplest way to make this system inoperable is to jam it by masking the satellite signal with noise. Spoofing is more sinister. Here, a false signal from a ground station is generated to confuse a satellite receiver.

Such spoofing could be done by imparting GNSS-like signals locally and making the receiver believe it is somewhere (which it is not). It is done by broadcasting incorrect GNSS signals designed to resemble a set of normal GNSS signals or by rebroadcasting true signals captured somewhere else or at a different time. Such spoofed signals could be altered in such a way as to cause the receiver to estimate its position to be someplace other than where it is or to be located where it is but at a different time, as decided by the invader.

Carry-off attack is a common form of GNSS spoofing attack. This is carried out by broadcasting signals synchronised with the genuine signals detected by the target receiver. Subsequently, the power of the counterfeit signals gradually increases, and the GNSS receiver starts tracking the false signals. Further, such signals are manipulated to report a different location from the genuine signals. Another form of GNSS spoofing is called Meaconing. This is a type of spoofing where GNSS signals are re-transmitted.

---

[51] Matt Burgess, "GPS Signals Are Being Disrupted in Russian Cities", *Wired*, December 15, 2022, https://www.wired.co.uk/article/gps-jamming-interference-russia-ukraine and https://aurorainsight.com/solutions/gnss-interference/,

[52] All details of spoofing operations in subsequent paras can be found at Maritime Global Security, https://www.maritimeglobalsecurity.org/media/1043/2019-jamming-spoofing-of-gnss.pdf,

Meaconing can be a simple replay attack or an advanced spoofing attack[53]. The technical requirements for such attacks are minimal and simpler equipment is required. The source of a meaconing attack could also be a GPS/GNSS repeater. Usually, such equipment is fitted in airport hangars to permit indoor reception of GPS signals (used for testing purposes). An attacker could increase the power of such a repeater, eventually sending a fake position out.[54]

Around March 2022, Elon Musk reported that SpaceX's Starlink satellite broadband service was facing signal jamming in Ukraine. Some Starlink terminals near battle areas were jammed for several hours. Since large parts of Ukraine's communications networks had suffered disruption amid airstrikes and invasion by Russian forces, a request was made to Mr Elon Musk to provide some assistance. Hence, his company SpaceX delivered many Starlink terminals to Ukraine to provide satellite communications. However, SpaceX was able to foil signal-jamming attacks quickly. Starlink could swiftly upgrade the software when the threat showed up and was able to adapt and stop the signal jamming quickly.[55]

Recently, there has been much concern regarding the hacking of satellites. The problem is nasty, and more potential targets are available in space owing to the increase in small satellite launches. It is only now that people are getting much more concerned about possible attacks on satellites. For many years the designers never thought that the people on the ground would attempt to hack a satellite/manipulate the signal. Some years back, satellites were designed and developed with limited memory and processing capacity. More importantly, there was no inbuilt capability for data encryption. The arrival of cheaper high-power antennas was welcomed without realising the possible vulnerability. Various possibilities for a potential hack do exist. Say, an attacker could access the systems on the Hubble Telescope and open its camera hatch while directed at the sun, wrecking the sensitive optics. A hacker could manipulate the system in such a way that the solar panels could be used to blow out the batteries[56]. As discussed earlier, satellites are susceptible to jamming attacks, disrupting important commands from ground controllers. Some view this as a significant (and most viable) cyber threat to the systems in space. Broadly, a cyber-

[53] Wahyudin Syam, "Meaconing: the most common type of GNSS spoofing interference attacks", October 15, 2022, https://www.wasyresearch.com/meaconing-the-most-common-type-of-gnss-spoofing-interference-attacks/

[54] https://www.maritimeglobalsecurity.org/media/1043/2019-jamming-spoofing-of-gnss.pdf

[55] Dan Swinhoe, "SpaceX's Starlink service facing signal jamming in Ukraine, Musk claims", March 07, 2022, https://www.datacenterdynamics.com/en/news/spacexs-starlink-service-facing-signal-jamming-in-ukraine-claims-musk/ ; Michael Kan, "Pentagon Impressed by Starlink's Fast Signal-Jamming Workaround in Ukraine", *PC Mag*, April 21, 2022, https://www.pcmag.com/news/pentagon-impressed-by-starlinks-fast-signal-jamming-workaround-in-ukraine

[56] Ryan Whitwam, "Hacking Satellites Is Surprisingly Simple", *Extreme Tech,* March 8, 2019, https://www.extremetech.com/extreme/287284-hacking-satellites-is-probably-easier-than-you-think

attack is not a monolithic threat. The threat can be posed by exploiting various methods and using various approaches. Different techniques and technologies could be used for stalling a cyber-attack on space architecture, including ground-based systems; hence, response to this threat could come through diverse means. At times, targeting services becomes easier for an attacker than attacking satellites; therefore, the threat identification method needs to consider these aspects.

Hardware-based attacks are likely to happen during the development and manufacturing phase. It is not impossible to damage the hardware of an operational satellite, but such efforts would require technology proficiency. More importantly, manipulating an operational satellite's software would give the desired output. There is a possibility of hardware attacks causing physical damage when the satellite is built. Also, the aggressor could target the supply chains to cause manufacturing delays.

New generation space systems are getting progressively interconnected and are computationally intricate. Hence, new concerns about the threat of cyberattacks have been raised. However, owing to some inbuilt security measures and the nature of modern technologies also make it difficult for the attacker to pull off an attack that easily. Also, there could be a potential risk of unintentionally unsettling other targets. At the same time, the satellites already in space have limitations regarding providing cyber security cover. It is difficult (almost impossible) to upgrade the computer systems that power these systems. This means if a cybersecurity vulnerability arises, it could be there for the complete life of the satellite. Cyberattacks have the potential to create chaos on strategic weapons systems and destabilize deterrence by generating uncertainty and confusion. Overall, it could be said that cyber coercions to space systems are posing fundamental challenges to enduring peace in orbit.[57]

[57] Danny Palmer, "Cybersecurity in space: The out of-this-world challenges ahead", *ZDNET*, December 07, 2022, https://www.zdnet.com/article/cyberspace-in-space-the-out-of-this-world-challenges-ahead/

STRATEGIES FOR COUNTERING CYBER ATTACKS ON SPACE SYSTEMS

In general, cyber threat is not a new menace. Various countermeasures are put in place to address cyber threats, and the process remains dynamic owing to the constantly evolving nature of the threat. Multiple actions to tackle cyber threats involve technical actions as remedies to counter these threats, policy actions identifying the proactive measures to address such threats and various other processes and devices which can prevent or mitigate the effects of cyber-related threats. Such practices began during the 1970s with the development of Antivirus software. With the evolution of the Internet, a wide array of technologies must be invented to counter diverse cyber threats. Modern software could perform multiple tasks like protecting the user from computer viruses and malware like spyware, ransomware, adware, trojans, and ransom hijackers.[58]

Globally, a significant amount of work has undergone towards understanding the requirements for cybersecurity. Various agencies have developed frameworks that help organisations better understand, manage, reduce, and communicate cybersecurity risks. These sources have emerged as important resources to address the challenges. Such documents are getting constantly updated to cater for new requirements. These cybersecurity frameworks are sets of documents describing guidelines, standards, and best practices designed to ensure the maintenance of cyber security. They help decrease an organization's exposure to weaknesses and vulnerabilities that hackers and other cyber offenders may exploit. These frameworks provide foundation, structure, and support to the organization's security methodologies and efforts. The organisations could develop need-based frameworks, like control, programme, and risk frameworks.[59]

Typically, the administration of the life cycle of an organization's cybersecurity risk management involves five concurrent and continuous functions: identify, protect, detect, respond, and recover. A cybersecurity framework is not an exact solution provider for a specific problem. It cites current standards, guidelines, and practices that

[58] Anton Terekhov, "History of the Antivirus," *Hotspot Shield*, https://www.hotspotshield.com/blog/history-of-the-antivirus/,

[59] "NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework", NIST, January 19, 2023, https://www.nist.gov/system/files/documents/2023/01/19/CSF_2.0_Concept_Paper_01-18-23.pdf; "What is a Cyber Security Framework: Types, Benefits, & Best Practices", *Simpleilearn,* February 14, 2023, https://www.simplilearn.com/what-is-a-cyber-security-framework-article

provide helpful direction to help an organization realise the desired result of every subcategory.[60]

Legality aspects of cyber threats have been studied globally, and an international group of experts from legal, technical, security and various other fields have come out with an academic, non-binding study on how international law applies to cyber conflicts and cyber warfare. This is known as the Tallinn Manual.[61] This manual was published on March 15, 2013. This effort is viewed as a first effort towards understanding and analysing the cyber challenge and related intricate legal issues. This manual's updated version, Tallinn 2.0, was released in February 2017. Over the years, this manual has been recognised as the most helpful document. It must be noted that this manual results from private individuals coming together and has no official backing of any state agency.

The United Nations is also important in developing a global understanding of addressing the threat of cyber warfare. In 2019, the UN established a Group of Governmental Experts (GGE) to advance responsible state behaviour in cyberspace in the context of international security. There were members from 25 countries who participated in the deliberations. This grouping took almost two years for discussions before submitting their report in 2021. The report identified the norms, rules, and principles for the responsible behaviour of States. The Group also observed a need to evolve a mechanism for confidence-building measures (CBMs) and made some suggestions to that effect. The Group considered that building confidence is a long-term and progressive commitment towards the sustained engagement of States. It was felt that positive participation by stakeholders could contribute to the effective operationalization and reinforcement of CBMs.[62] There was also a GGE on space. The UN GGE on the Prevention of an Arms Race in Outer Space had meetings during 2018–19. However, the group could not reach any consensus, and no outcome report was produced. In addition, efforts are being made to have a global view of the cyber threats to the space domain under the UN programmes like the UN OEWG, an open-ended working group on reducing space threats through norms, rules, and principles of responsible behaviours. There are OEWG for both cyber (ICT) and space domains.

Some additional multilateral-level efforts include debating these threats by the Consultative Committee for Space Data Systems (CCSDS, 1982), which is engaging

[60] Suzanne Lightman (et. al), "Satellite Ground Segment: Applying the Cybersecurity Framework to Satellite Command and Control: NISTIR 8401", Dec 2022, https://csrc.nist.gov/publications/detail/nistir/8401/final

[61] Tallinn, capital of Estonia, had received a major wave of cyber-attacks during 2007. This was an elaborate attack and impacted every major agency in the state including government, banks, media etc.

[62] "Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security", *UN General Asse*mbly, July 14, 2021, https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf

major space agencies (governmental or quasi-governmental organizations) of the world to provide a forum for discussion. It comprises 11 member agencies, 32 observer agencies, and over 119 industrial associates. Moreover, engagements should happen (or already happen) through other agencies like the Organization for Security and Co-Operation in Europe (OSCE) and ASEAN Regional Forum on cyber confidence-building measures.[63]

Nonetheless, ensuring the cyber security of satellites is not a straightforward proposal. Cyber threats to satellites are a bit of recent origin than other cyber threats, which have been known (and experienced) for many decades. The solutions for new types of cyber threats, which involve attacks on space systems, could be similar and different than the ones offered for other types of cyber threats. Relying solely on firewalls, intrusion prevention systems, and anti-virus software alone is not expected to prevent attacks on space systems. The target of cyber-attacks now extends from the traditional network field to a new network application setting based on various modern applications like AI and blockchain, industrial control systems, big data platforms, and satellite communication networks.[64]

It could be safe to say that no global standards exist regarding deciding on satellite security. In 2021, the Cybersecurity and Infrastructure Security Agency (CISA), a part of the US cyber defence agency, formed the Space Systems Critical Infrastructure Working Group. This multidisciplinary group is trying to understand the challenges and identify ways to help protect the space infrastructure the satellites build. The need to form this group emerged with a view that space is a potential risk vector to national critical functions and space infrastructure is a critical infrastructure that must be protected. This cross-sector space working group looked at governmental and commercial space infrastructure risks. Their primary concern was finding ways to mitigate cyber risks to position, navigation, and timing (PNT) services.[65] Some valuable suggestions have emerged from these deliberations.

Cyberattacks can arise across various segments within a space system architecture, which includes space, communications links, and ground segments. Specifically, the threat could come from an operational satellite's communications link,

---

[63] Caitríona Heinl "Outer Space as a Growing Security and Defence Domain: Strategic Lessons on Cyber Disruption", *Observer Research Foundation*, March 02, 2023, https://www.orfonline.org/expert-speak/outer-space-as-a-growing-security-and-defence-domain-strategic-lessons-on-cyber-disruptions; For more on CCSDS, visit https://public.ccsds.org/participation/member_agencies.aspx

[64] Arslan Mirza, "Cybersecurity Threats to Satellite Communications", *Medium,* December 21, 2020, https://medium.datadriveninvestor.com/cybersecurity-threats-to-satellite-communications-b35d83681723

[65] Dave Nyczepir, "CISA working group assessing cyber risks to space infrastructure", *FedScoop*, November 16, 2021, https://fedscoop.com/cisa-space-infrastructure-risk-assessment/; Also See, Zac Amos, "How secure are satellites from cyber-attacks?", *Cyber Talk*, 26, 2022, https://www.cybertalk.org/2022/05/26/how-secure-are-satellites-from-cyber-attacks.

i.e., the radio frequency link or the ground system.[66] Different approaches are being used to address such threats. In some cases, for the similar nature of the problem, more or less similar solutions are being worked on. In some instances, problem-specific solutions are applied for problems like handling cyber threats in small satellites or blocking the threats posed to communication satellites.

At present, along with state ownership, many private players possess assets in space. Old space systems essentially launched by the states are believed to be robust systems from an operations point of view. However, mostly these are 10 to 15 years old satellites which are still operational. They were designed, developed, and tested in an age that preceded cyber threats to space. This was when the thought of hackers making satellites as their targets was not on the horizon. Such legacy assets, nodes in space-based and space-to-terrestrial communications, serve as possible network entry points, much as endpoints (e.g., devices, servers, etc.) do in old-style information technology (IT) based networks.[67] In a relative sense, targeting such systems using cyber means is a bit easier because they are not digital attack resilient. Modern-day IT tools, assisted by AI, could be used to find soft spots in old satellite systems for launching an attack.

Mostly, the legacy systems (satellites launched one or two decades back or even much before that) were not designed with security in mind. There is a need to have some solutions to fix this technology gap. Then there are issues like the nature of actions to be undertaken if an attack occurs. Different solutions could exist for satellite systems and other related structures. If the attack is on ground stations, what actions must be undertaken? Would the solutions be similar if the attack is on small satellites in LEO or satellites in geostationary orbits? Also, what tactic must be implemented to resolve the crisis if the attack is on networks and radar installations? There would requirement of two types of measures to be undertaken: one, be proactive and, during the design and development phase itself, strengthen the systems in such a fashion that any cyber-attack could be throttled automatically; two, take action after the attack has been noticed, towards recovery and minimising the damage. A proactive action tool in the form of policy regulations, guidelines, checklists, and multilateral mechanisms to address the existing and possible threat is expected to play a major role in addressing this threat.

Conventionally, space and terrestrial systems were mostly isolated from each other. This is because each system serves a different set of users and necessities. However, this format has almost changed in the 21st century, with increasing interconnections between Earth-Space networks. For example, future smartphones could have satellite messaging capabilities for emergency communication without

[66] "Protecting Space Systems from Cyber Attack", *Medium*, March 31, 2022, https://medium.com/the-aerospace-corporation/protecting-space-systems-from-cyber-attack-3db773aff368

[67] Brad D. Williams, "Amid Space Race, Cybersecurity And Resiliency Remain Concerns: Experts", *Breaking Defense*, August 16, 2021, https://breakingdefense.com/2021/08/amid-space-race-cybersecurity-and-resiliency-remain-concerns-experts/

terrestrial connectivity. Digital transformation has also stemmed towards establishing interfaces between systems and, mainly, across traditional trust boundaries (partners, customers, etc.). Besides, the adoption of prominent LEO satellite constellations (for providing Internet services) drives the number and intricacy of ground control and service support set-ups, thus raising the potential attack surface[68]. Such aspects are correspondingly required to be considered while deciding on the countermeasures against cyber-attacks on space systems.

In future, the resilience of critical services on Earth will become even more intertwined with the strength of satellites in space. Satellite operators understand the importance of cybersecurity. For cybersecurity experts, there has been much exposure over the years in handling security requirements for governments, defence establishments and major critical infrastructure units like dams, oil & gas setups, shipping, railways, aviation, and finance. For all these sectors, a mechanism for cybersecurity is already in place in some form or other, and they have been time-tested. Due to the nature of the threat, this security system should always remain active and dynamic. For the space sector, various ideas put in place for such segments could find relevance. However, it also needs to be understood that the space sector has complexities. There are issues associated with third-party relationships. Satellite-based service infrastructures are complex and evolve, providing complete end-to-end services. There are various stakeholders operating in different parts of the organisation. The supply chain for hardware and software depends on multiple parts, making recognising accountability and liability for the definitive security and resilience of the services supplied problematic. It becomes challenging to identify where the functions and accountabilities of hardware manufacturers, software developers, satellite manufacturers, operators, and commercial users start and finish. Both in space and cyber domains, the regulatory frameworks have generally been unable to keep pace with technological evolution[69]. It is expected that such lag will always continue to exist. Suitable regulatory frameworks are essential but would take time to develop, especially if they are done at the UN/multilateral level. Hence, there is a need to evolve best practices, rules of roads or other such mechanisms by constructively (and regularly) engaging various stakeholders.

The legacy systems could be viewed as bent pipes in space. This means the uplink signal is received, amplified, translated to a downlink frequency, amplified again, and directed toward the earth using a high-gain antenna. Satellites receive data from Earth, such as TV signals, amplified and mirrored back to Earth. Such structures

[68] "Will the battle for space happen on the ground?", *World Economic Forum,* May 25, 2022, https://www.weforum.org/agenda/2022/05/increased-cybersecurity-for-space-based-services/

[69] "Will the battle for space happen on the ground?", DAVOS 2022, *World Economic Forum,* May 25, 2022, https://www.weforum.org/agenda/2022/05/increased-cybersecurity-for-space-based-services/,

could be easily compromised by using cyber means. Understanding these lacunas in the old satellite systems, some security measures are now put in place so that the new satellites have inbuilt protection before launch. Present generation systems are developing extra complex with the arrival of software-defined satellites. Now satellites are built to be resilient and robust and have the facility to function in isolation from each other if required. Satellites are connected to private networks keeping the Internet out of the loop. Modern-day satellite systems are software-defined satellites, allowing satellites to be reconfigured in space. With this, it is possible to adjust space-based services per the demand (requirement). Such systems can respond dynamically to various threats as they emerge.[70]

For any space architecture, the cyber security measures would differ depending on the segments under consideration, say ground segment or any other segments. Occasionally, it would depend on the satellite's location, say in LEO or any different orbit. The make and size of the satellite could also have some relevance for the attacker to plan an attack. Every segment would have its challenges. The ground and link segment controls are more diverse than the space segment. Though, some general security principles would apply across the board. Access control, authentication, authorization, password protection, anti-virus patches and other general provisions could be considered standard provisions and should be applied to any segment.

Some cybersecurity mitigation techniques have already been put in place by some major space agencies. They include: [71]

Access control management: There are guidelines to spot a phishing email.[72] Phishing is a high-tech trick that uses spam or pop-up messages to cheat people into divulging information.

Specialised Security Workforce: This unit studies the type of undergoing missions in detail and tries to identify if they require any specific measures to ensure cyber security. For example, missions to the Moon/Mars or missions like human space missions or the functioning of a space station. By undertaking critical analysis, appropriate security tools could be identified and developed. It also becomes helpful to engage the security research community for critical assessment. Such a process of engagement should not be a limited effort but an ongoing process since the nature of the threat is constantly evolving.

---

[70] "Will the battle for space happen on the ground?", *World Economic Forum*, May 25, 2022, https://www.weforum.org/agenda/2022/05/increased-cybersecurity-for-space-based-services/

[71] Gregory Falco, "Cybersecurity Principles for Space Systems", *Journal of Aerospace Information Systems*, Vol. 16 (2), February 2019, https://doi.org/10.2514/1.I010693.

[72] https://www.nasafcu.com/education-tools/security/security-articles/avoid-being-caught-by-a-phishing-scam

Fostering Security Culture: Cybersecurity awareness generation is much essential. Such awareness generation is necessary not only for the system research and manufacturing units but also for the suppliers and sub-suppliers. There is a need to ensure that the entire supply chain remains stealthy. Training and incentives are two critical aspects towards fostering a security culture.

Cybersecurity risk management is an evolving theme for defence and commercial satellite industries. The risk has been known for some time, and some measures have been put in place, as mentioned above, but more needs to be done. Satellite manufacturers and operators need to remain proactive and are expected to take various safeguarding measures well in advance. Some broad suggestions in this context are presented here. It needs to be understood that these suggestions are not inclusive regarding various cybersecurity risks.[73] Here the objective is to present basic concepts and make some mentions based on the literature review and some ideas inferred from the informal discussions with a few experts. Following is a list of security elements for defending space-based assets and satellites, along with ground-based control flight networks: [74]

Various security aspects will be built into each satellite through the system's design and development process.

1. Identity and access management (IAM): Those who get into flight control information and surfaces need to be recognized and confirmed by an IAM solution that will pass muster on the user using machine learning identifiers to prevent authorized access to critical vehicle functions.
2. Multi-check for IoT-related devices: Facility for updating IoT devices; no hard-coded passwords should be permitted.
3. The backbone of a cyber-resilient spacecraft should be a robust intrusion detection system (IDS). The IDS should constantly monitor telemetry, command sequences, command receiver status, shared bus traffic, and flight software configuration and operating states, anticipate and adapt to mitigate evolving malicious behaviour. Systems on board a spacecraft should be designed for cyber-safe mode. Logging should also be available to cross-check for anomalous behaviour.
4. Spacecraft developers should be able to realise a supply chain risk management programme. They need to certify that each vendor handles hardware and software properly and with an agreed-upon chain of custody. Critical units and subsystems should be identified and handled with different rigour and

[73] "Introduction to Cybersecurity for Commercial Satellite Operations (2nd Draft)", February 25, 2022, https://csrc.nist.gov/publications/detail/nistir/8270/draft.

[74] The inputs are taken almost verbatim from Paul Ferrillo, "Protecting Space-Based Assets from Cyber Threats", *Homeland Security Today*, October 17, 2020, https://www.hstoday.us/subject-matter-areas/cybersecurity/protecting-space-based-assets-from-cyber-threats/.

requirements than noncrucial ones and subsystems and built with security in mind. All software on the spacecraft should be carefully vetted and correctly handled through configuration management and secure software development processes.

5. The spacecraft and the ground system should self-sufficiently perform command logging and anomaly detection of command sequences for cross-validation. Instructions received may be stored and sent to the ground through telemetry and automatically checked to verify consistency between commands sent and received.
6. Protections should be made against communications jamming and spoofing, such as signal strength monitoring and secured transmitters and receivers; links should be encrypted to provide additional security.

Security elements for defending ground-based systems and network assets include:

1. Adopting cybersecurity best practices, including those aligned with the NIST[75] Cyber Security Framework (CSF).
2. Crucial network parts should be logically and physically separate to prevent virus-like (ransomware) attacks from scattering through the network.
3. Need to put various policies in place for incident response, business continuity and crisis communications plans, patching policies, BYOD policies and backup policies.[76]
4. Needs to hold quarterly employee training for all persons. The focus should be on aspects of spear-phishing and socially engineered email attacks.
5. Various concerned agencies are required to assume an effusive vendor supply chain risk management package that touches all primary and tertiary vendors.
6. It is vital for each ground-based space system and facility to adopt machine learning intrusion detection systems to help protect against anomalous and potentially malicious activity.
7. All ground-based space systems, services, and space manufacturers and retailers should be required to join the Space ISAC to cooperate by sharing threats, alerts, and incident evidence.[77]

Globally, some government networks have developed a dependence on commercial satellites. Unfortunately, such commercial satellites do not have a higher level of

[75] The National Institute of Standards and Technology (NIST) was founded in 1901 and is now part of the US Department of Commerce. NIST is one of the oldest physical science laboratories.

[76] 'Bring Your Own Device' is a policy that allows employees in an organization to use their personally owned devices for work-related activities.

[77] The Space ISAC (Information Sharing and Analysis Center), a US based agency serves to aid cooperation across the global space industry to increase the ability to prepare for and respond to vulnerabilities, incidents, and threats; to provide timely and actionable information among member entities; and to serve as the basic communications channel for the sector regarding this information.

protection built into them. Commercial satellite operators have started ensuring more security for their systems, and new satellites are getting launched with more security features. However, mainly owing to commercial interests, some limitations do exist. Now mostly, the use of hybrid networks with multiple transport choices is found to be gaining traction with different agencies. This involves software-defined networking, where other traffic types are placed over terrestrial or satellite links. Such networks are found to offer a better degree of protection.[78]

There are various options available to understand cybersecurity vulnerabilities. In the overall cyber domain, for many years, one option gets identified as an important preference, which helps to find the faults in the system or to check the security excellence of the system. This process involves intentional hacking of cyber systems. An Ethical Hacker (also called a White Hat Hacker) is an expert who penetrates a computer system or network resource on behalf of the system developers or managers. The ethical hacker evaluates the security quality of the system and identifies vulnerabilities in target systems, networks, or system infrastructure. Organizations employ them to pick on potential security vulnerabilities. Ethical hackers usually find security exposures in unreliable system configurations, recognized and unidentified hardware or software vulnerabilities, and operational weaknesses in process or technical countermeasures.[79] Every system mostly comes with some vulnerabilities, which get overlooked during the design stage. At times, owing to the rapid development in technology, new options emerge to harm the old systems intentionally. Constant efforts are underway to check the robustness of the space systems. Various efforts are making to determine whether unauthorized access or other malevolent actions are possible by using cyber means to attack these systems. Here the idea is to find vulnerabilities before cyber rogues do it.

The US Air Force and Defence Digital Service had planned a satellite hacking challenge, the Space Security Challenge 2020: Hack-A-Sat. The purpose was to test hackers' capabilities, skills and ingenuity in answering cyber security contests to the space systems. Exciting ideas have emerged from this competition which would go a long way to strengthen the cyber security for space systems. Beyond technical challenges for top hacking teams, this competition aimed to spread awareness of the need for cybersecurity in space and offer opportunities to educate up-and-coming hackers.[80]

---

[78] Sandra Erwin, "Cyber warfare gets real for satellite operators", *Space News*, March 20, 2022, https://spacenews.com/cyber-warfare-gets-real-for-satellite-operators/

[79] Garry Kranz, Linda Rosencrance, Michael Cobb, "Ethical Hacker", *Tech Target*, May 21, 2021 https://www.techtarget.com/searchsecurity/definition/ethical-hacker

[80] "Satellite hacking challenge shifts to fully virtual event", Air Force (US), May 13, 2020, https://www.af.mil/News/Article-Display/Article/2185826/satellite-hacking-challenge-shifts-to-fully-virtual-event/ and "Hack-A-Sat 2020", https://cromulence.com/hack-a-sat

There is an interesting case of an intentional (ethical) hacking of an old communications satellite. Security researchers had hacked a decommissioned communications satellite called Anik F1R. This hack demonstrated that the threat is not only for the operational satellites but also for satellites that have been retired but still not moved into their ultimate resting place, the graveyard orbit. For hackers, it is possible even to communicate with such satellites. Airbus Defence and Space manufactured Anik F1R (C- and Ku-band frequencies). It was meant for video distribution to cable systems and broadcast contributions and covered the United States and Canada. This satellite was launched in 2005 and had a design life of 15 years. Its GPS /WAAS (Wide Area Augmentation System) Payload was disabled on May 15, 2022. The agency that undertook that hack had obtained permission to access the satellite and its commercial uplink facility. In principle, by covertly undertaking such a hack, the states (or not-state) who want to broadcast propaganda could do it without launching their satellite.[81]

Primarily, cyber threat to space systems is a relatively new idea. There is no mention of such threats found in the literature from the Cold War era. There was much understanding of the possible threats to satellites during that period. However, the debate mainly revolved around the limitations of the then-earth-based weapons regarding posting threats to high-altitude satellites. There were some future technology predictions which could be employed as anti-satellite weapons. These included kinetic-energy weapons (rail guns and homing missiles), space-based mines, directed-energy weapons (particle beams, optical lasers, x-ray lasers, and microwave weapons) and powerful earth-based lasers. However, there was no mention of cyber threats. The technology (hardware and software) posing a cyber threat to space systems is still evolving. The process towards developing countermeasures would remain dynamic.[82] Some of the ongoing efforts in that direction are discussed below.

The private sector is developing various countermeasures against cyber-attacks on space systems. In 2020, the US Department of Defence engaged an agency to develop support for a critical Air Force and Army Anti-jam Modem (A3M) programme under the US Space Force's Space and Missile Systems Center (SMC). Under this programme, the Air Force and Army should get a secure, wideband, anti-jam satellite communications terminal modem for tactical satellite communication operations. The jam-resistant modems are (possibly) supporting SMC's Protected Tactical Waveform technology, an anti-jam capability functioning on military satellite communication

[81] B. David Zarley, "An old satellite was hacked to broadcast signals across North America", *Freethink.com,* April 14, 2022, https://www.freethink.com/space/decommissioned-satellite-hacking

[82] S. Fetter, "Protecting Our Military Space Systems", in Edmund Muskie, ed., *The U.S. in Space: Issues and Policy Choices for a New Era*, (Washington, DC: Center for National Policy Press, 1988), pp.1–25.

stations through the Wideband Global Satcom constellation.[83] Specific details of this programme are not known for obvious reasons.

During Mar 2023, the US Space Systems Command (SSC) demonstrated its ground-based anti-jamming satellite communications (SATCOM) capability using an on-orbit operational satellite. The event demonstrated over-the-air Protected Tactical Waveform (PTW) connectivity between a Protected Tactical Enterprise Service (PTES) Joint Hub and a test terminal and over-the-wire connectivity to a PTW-capable modem developed by the Army Airforce Antijam Modem Program Office. PTW provides joint warfighters with critical anti-jam capability. As per reports, PTES is the aiding ground system (mission management system, key management system, key loading and initialization facility, and joint hubs) for PTW operations over the Wideband Global SATCOM fleet. This would aid in improving military features with high levels of jamming resistance and connectivity assurance. Initial operational capability is projected to be fielded in 2024. Space Systems Command (SSC), the US Space Force field command, is responsible for acquiring and delivering resilient warfighting capabilities to protect their strategic advantage in and from space. They work with joint forces, industry and government organisations, and academic and allied groups to fast-track innovation and outpace emerging threats.[84]

The Defence Advanced Research Projects Agency (DARPA) is the US DoD's research and development agency. This agency is advancing emerging technologies for use by the US armed forces. They are also outsourcing some projects to the private industry. DARPA is collaborating with various agencies to ensure that the next generation of satellite communications is resilient to cyberattacks. One of their programmes pursues to develop reconfigurable, multi-protocol communications terminals that are small, lightweight, low-power, low-priced, and able to link several different satellite constellations in LEO. Companies are providing critical tools for proactive maintenance and protection of customers building the next generation of resilient space architectures. The task given to private agencies is evident. Their solutions should ensure that communications terminals associated with the space systems should be secure and resilient.[85]

---

[83] Emma Helfrich, "Anti-jam modem program to be supported by Comtech", *Military Embedded Systems,* May 28, 2020, https://militaryembedded.com/comms/satellites/anti-jam-modem-program-to-be-supported-by-comtech.

[84] "Space Systems Command demonstrates satellite anti-jam capability", *Space War*, March 14, 2023, https://www.spacewar.com/reports/Space_Systems_Command_demonstrates_satellite_anti_jam_capability_999.html

[85] "SpaceCREST Cybersecurity Platform will protect Space Communications hardware for DARPA program", *Space War*, December 08, 2022, https://www.spacewar.com/reports/SpaceCREST_Cybersecurity_Platform_will_protect_Space_Communications_hardware_for_DARPA_program_999.html

Some private industries have already started offering satellite security solutions with quantum technology. However, much work still needs to happen in this field. These technologies provide great potential in quantum computing, quantum cryptography and others. Quantum technologies are already being prototyped for space applications. Here the focus is on quantum sensing and quantum key distribution (QKD). Quantum computing (still in development) promises to break today's encryption. Quantum technology has been viewed as both a solution and a problem for space security. There is a view that measures must be taken to implement quantum-resilient cybersecurity on new and legacy satellites. Quantum computers could help to enable effective attacks on public critical infrastructure (PKI). Satellites rely on conventional PKI to secure their communications to keep data safe. With PKI being susceptible to attacks, what is required is to develop resilient forms of security for both satellite and terrestrial networks.[86]

Significant developments in cyber and AI skills increase the prospects of embedding intelligent autonomous systems in space to detect, respond and adapt to dynamic security threats. Advances in cloud computing and associated technologies would help the creation of dynamic distributed virtual infrastructures and services in space systems. Additionally, all this can lead to reviewing the space set-ups with new cloud services. Such services could include having a ground station as a service. This would allow operators to directly manage space-based resources like satellites and data movement from/to space via cloud data centres. However, new technologies would also come with backdrops and create new security challenges for space systems.[87] Hence, it is important to develop an inclusive strategy for the cyber security of space structures and related set-ups by factoring in new advances in information technologies.

[86] Patrick Shore, "The Final Frontier for Quantum-Resilient Cybersecurity: Why We Need to Incorporate Post-Quantum Cybersecurity into Satellite Communication Architectures", *Security Today*, September 09, 2022, https://securitytoday.com/articles/2022/09/09/the-final-frontier-for.aspx, and https://app.spaceimpulse.com/listings/satellite-risk-quantum-computers-will-steal-data-disrupt-infrastructure-46645165.

[87] Vijay Varadharajan, "Australia's space security strategy needs to aim higher", University of New Castle, Australia, May 08, 2021, https://www.newcastle.edu.au/newsroom/research-and-innovation/australias-space-security-strategy-needs-to-aim-higher.

STATE POLICY DIRECTIVES: AN ANALYSIS

Various states worldwide have clearly understood the nature of cyber-attack threats to their space infrastructure. As such, there are a minimal number of states (some private agencies, too) which belong to the category of spacefaring states (states having independent satellite launch capability). These states are required to be more aware of cyber threats. At the same time, many non-spacefaring states also have their own operational satellites and ground infrastructure. Hence, today, many states are required to protect their space assets from any possible cyber threat and are trying to remain prepared to address this threat by learning from global experiences. Various technologies and policy initiatives are getting evolved to address this threat. Agencies interested in the space domain continuously examine the risks and suggest multiple options.

States understand that these worries could differ for different types of satellites and ground infrastructures. Some states have publicised their policy directives towards risk mitigation, while some are possibly developing them. There is also a possibility that some states could be intentionally keeping their efforts undisclosed. This section takes a broad overview of accessible policies regarding a few countries. One is the US, a state with the most advanced space programme. Two, the European (specifically, German) view. Three, Australia, a non-spacefaring state with limited investments in the space domain, is a relatively new player but has significant growth ambitions. Four, China, which has leapfrogged in the space domain, has a major global trust deficit due to its opaque counter-space programme. Reviewing some of China's critical space-cyber projects to appreciate their focus for the future is also essential. Cyber tools to manipulate space systems have become both bane and a boon for a state like China. At the same time, it needs to be mentioned that this could be true in some other cases too. Fifth, India is an important middle-level spacefaring power.

UNITED STATES. In earlier sections, some references have already come regarding the US policy and efforts done by DARPA towards providing cyber security to space systems. For the US, which has around 5900 operational satellites, access to and use of space is a vital national interest. Naturally, cyber-related threats to space-based resources and supportive ground infrastructure pose increasing risks to their security structures and economic interest. Considering the necessity to address this threat holistically, in September 2020, the US President came out with a 'Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems'.[88] This policy applies to the civil and national security space systems and private space systems. It

[88] "Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems", National Security & Defense, September 4, 2020. Available at, https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/

emphasises improving cyber protection while developing space systems, including ground control networks. This directive essentially creates fundamental cybersecurity principles to direct and assist as the basis for the US approach to the cybersecurity of space-connected infrastructure.

The directive asks space operators to consider incorporating into their plans the following aspects:

- Ensure safeguarding command, control, and telemetry links using correct authentication or encryption measures
- Have in place physical protection measures for reducing the weaknesses of a space vehicle's entire control systems
- Protection against communications jamming and spoofing
- Protection of ground systems, operational technology, and information processing systems
- Ensure awareness generation and organise staff training
- Undertake appropriate insider threat mitigation precautions
- Get accurate cybersecurity hygiene practices underway, guarantee physical security for automated information systems, and intrusion detection methodologies
- Supply chain risks management

The directive expects various governmental agencies to work with the commercial sector. There are some other non-government space operators, and this directive should be useful for them. All such agencies should share information. They should define best practices, establish norms, and promote improved cybersecurity behaviours. The execution of the laid down guidelines should happen via the formulated rules and regulations. The overall approach should aim to enhance best practices and norms of behaviour in the cybersecurity domain. Subsequently, various government space regulatory bodies could adopt these rules and regulations.

A critical agency in the US dealing with various aspects of cybersecurity apart from being a measurement and metrology agency is the National Institute of Standards and Technology (NIST). They have developed a Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework). This agency also organizes various cybersecurity-related activities. Expanding on the ideas set forth by SPD-5, NIST has also done some work in space cybersecurity and developed cybersecurity tools, references, and guidance. Some details of these resources are as follows:

Foundational PNT Profile: Applying the cybersecurity framework for the responsible use of Positioning, Navigation, and Timing (PNT) Services (NIST IR 8323). The PNT Profile has been created by using the long-established NIST cybersecurity

framework. It is part of a risk management programme to help agencies manage risks in PNT services. Releasing that such profile creation cannot be a one-time process, NIST is also updating this profile by gathering stakeholder views.

Introduction to Cybersecurity for Commercial Satellite Operations (NIST IR 8270): Offers some broad guidance (basic concepts) for handling various aspects of cybersecurity risk management for commercial satellite operations. This document benefits the industry by providing sample references for additional information on appropriate cybersecurity risk management models.

Satellite Ground Segment: For addressing risks posed to the ground segment of space operations (command and control), it has been suggested that the provisions in the Cybersecurity Framework (CSF) could be applied. The document NIST IR 8401 defines the ground segment, outlines its responsibilities, and presents a mapping to relevant cybersecurity information references.

Hybrid Satellite Networks: A draft has been implemented to gather stakeholders' views regarding applying the NIST Cybersecurity Framework to hybrid satellite networks.

GERMANY. Apart from the US, European states like Germany have also developed guidelines on this subject. There is a considered view that Germany's security guidance for satellite safety from cyber-attacks could be a good model for broader cyber standards for the entire space industry. In June 2022, the German Federal Office for Information Security (BSI) implemented an IT baseline protection profile for space infrastructure. This document is discussed as the possible model for deciding on cybersecurity-related standards for the European space industry.[89]

This document is expected to help satellite companies immensely. It presents them with a conceptual roadmap to decide on minimum cyber measures to keep their supply chains safe. This could mainly help various businesses to have basic standard guidelines. The German guidelines list actions to protect satellites through different phases, like when they are being transported and tested and when they are in orbit. Broadly, it offers a proposition to decide on the minimum requirements for ensuring cyber security for satellites.

It classifies the protection necessities for different satellite missions from 'Normal' to 'Very High'. The focus is on every sector, which requires security measures to follow, from manufacturing satellite operations. The 'Normal' category relates to manageable damages, while 'High' associates with high-consequence damages capable

[89] "IT-Grundschutz Profile for Space Infrastructures Minimum Protection for Satellite", Federal Office for Information Security (Germany), June 30, 2022, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/profiles/Profile_Space-Infrastructures.pdf

of significantly limiting the operations. 'Very High' is linked to almost total shutdown. This document considers even the satellites that have past the end of their lifetime. Such spacecraft might contain various crypto secrets and necessitate monitoring even when sent to a graveyard orbit. The document takes a very pragmatic view on the issue at hand and categorially mentions that, albeit all procedures (as mentioned) are being followed, still 100 percent security cannot be realized.

Realizing that the cyber contests to space systems are going to continue, the EU has decided to be proactive and keen to develop secure technology for the future. Europe has approved a proposal to build a strategic network of satellites for critical infrastructure. This is a €2.4 billion project, and it should be viewed as an essential step towards the building of a secure network of satellites. Apart from Europe, this project, called IRIS (Infrastructure for Resilience, Interconnectivity and Security by Satellite), would also offer connectivity to the areas where broadband internet facilities and the entire African region are unavailable. It is expected to help both civilian sections of government departments and the military. European Space Agency (ESA) and the private sector would be involved in this project, which is expected to be a state-of-art constellation. Intending to provide secure and efficient connectivity and achieve digital transformation, it is likely that this project will give secure satellite communication when completed.

AUSTRALIA. Australian Space Agency is of recent origin, established in July 2018. There has been a major involvement of private agencies for a long towards providing Australia with various satellite-based services. Australia is keen to develop its space sector in a big way. The Australian Space Agency supposes that by 2030, their space sector will increase by three times (reach $ 12 b) and help create additional 20,000 jobs. Presently, Australia has around 33 working satellites in orbit. Different agencies in Australia have presented various policy options and rule structures regarding ensuring the safety of their space architecture. The Australian Space Cyber Framework offers a common framework for different elements of the space ecosystem to measure their security practices compared to established standards. It emphasises the need to assist the Australia Space ecosystem to fortify its cyber security posture. This framework could be viewed as a dynamic process where organisations respond to a questionnaire to determine the possible impact on their systems. An assessment of an organisation's cyber security maturity is gauged based on some set criteria. After applying the maturity assessment methodology, the minimum target state security posture an organisation should attain is determined.

The Air and Space Power Centre of Australia offers valuable and actual analysis and assistance on the strategic advance of air and space power to the Royal Australian Air Force. There is a realisation that dependence on private industry will increase in the near future. However, there is a possibility that the industry could cut corners due to

cost factors, including cyber security. Hence, the centre has identified three priorities, which may prove particularly important in building up satellite cyber resilience:[90]

1. **Awareness of Emerging Threats and Investment in Cyber Security:** To mitigate various known risks, there is a need for a greater focus on training. Also, efforts should be made to retain cyber talent and keep the equipment and knowledge up to date. Some programmes, like the Cyber Security National Workforce Growth Programme, could help train and raise greater awareness across the space sector.
2. **Further Knowledge Sharing Across the Civilian Space Sector:** Space Command remains at the centre of space security for defence. However, the nature of the threat indicates that civilian satellites are also not secure. Hence, it has been recommended that the Australian Cyber Security Centre, in association with the Space Command, could create cyber 'best practices' specific to satellite operators or agencies utilising space-based systems. Sharing of data and knowledge are prerequisites for developing a more holistic system. There also has been an emphasis on having more funding to develop correct structures to address the possible challenges.
3. **Cooperation with Like-Minded Countries to Enhance Cyber Security:** In the cyber domain, Australia has good associations with the states like the US and UK and Asian states like South Korea. Various agreements are already in place for collaborations. The US has placed their optical space surveillance telescope on Australian soil to track objects in space to help avoid collisions and monitor space debris. Now, Australia must work together to mitigate possible cyber threats to space architecture.

Australian Department of Home Affairs has presented a paper (November 01, 2019) written by an Australian lawyer, cybersecurity analyst, and policy analyst (Jonathan Lim) titled 'Safeguarding Australia's Assets in Space Cybersecurity for Satellites'.[91] This paper has given the following recommendations:

I. Formation of a Cyber Security Task Force to deal with Space-Related Assets.
II. Follow various International Laws and Principles put in place.
III. Ensure that Transparency and Confidence Building Mechanisms (TCMBs) are followed in true spirit.
IV. Acknowledge Cyber and Space as Critical Infrastructure Sectors.
V. Develop a Cyber Best Practice Toolkit for Space-Related Assets.

[90] Theodora Ogden, "Satellite Security in New Space", Air and Space Power Centre, Aug 29, 2022, https://airpower.airforce.gov.au/sites/default/files/2022-08/Ogden_Aug2022.pdf
[91] Jonathan Lim, "Safeguarding Australia's Assets in Space Cybersecurity for Satellites", WiseLaw, November 2019, https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-strategy-2020/submission-155.pdf

VI. Provide insurance cover to Space-Related assets with cyber-specific provisions.
VII. Intra and Extra Governmental Coordination.

Many similar policy suggestions are on the table in Australia and globally. It could be safe to say that, in the frameworks of policy structures for cyber-space complex, there could be some country (threat) specific differences in the solutions offered. However, there is much commonality in global approaches.

CHINA. China's investments in space are a bit different story than the rest of the world. China should be credited for rapidly and successfully developing in various space technology sectors. China has more than 600 operational satellites in space (March 2023). They have various successful ongoing programs like robotic missions to Moon and Mars. China has successfully developed a very accurate BeiDou Navigation Satellite System and is the only country in the world to have launched quantum satellites. China is the only third country in the world to have put astronauts (taikonauts) into space and has also built a space station where taikonauts conduct various experiments. However, by undertaking an ASAT test in 2007, leading to big debris creation, China has unnecessarily raised the ante of space weaponization. Today, despite Chinese declarations on space warfare, claiming to adhere to the peaceful uses of outer space, their intentions are suspected. Chinese writings as early as 2012 have declared the need for space dominance. Currently, China's development of counter-space capabilities presents a security challenge. Cyber is a vital component of China's counter space programme.

It is not the purpose over here to give a detailed expose about China's counter space programme. However, it would be interesting to know about the Chinese thinking regarding using cyber tools to damage advisories space structures. Mr Elon Musk was revered by many in China. However, SpaceX came under much criticism when an incident (2021) of two Starlink satellites of SpaceX coming dangerously close to the Chinese space station came to light. In 2022, a Chinse study came out projecting some interesting facts. This study has been carried out by researchers with the Beijing Institute of Tracking and Telecommunications. This institute is under the PLA's Strategic Support Force. Now, China has a researched view that they should have a counter-space system (hard and soft kill options) to address any future threat posed by constellation satellites. To achieve this, the Chinese agencies would first require to upgrade their existing space surveillance systems and other related networks. This study demonstrates Chinese thinking on this subject. Here cyber tactics would offer China an excellent option for a soft kill.

Presently, China focuses on understanding the expanse of various emerging space technologies. They are pushing their research and innovation efforts so that they would miss the ongoing revolution in space technology. China is known to be investing

in the space domain to understand quantum communications' relevance. They are keen to have a cyber-attack-free system, which could help them to secure their critical infrastructure. One system of important areas of focus for them is the integrated development of space and information technologies. Based on the thrust given by them from the point of view of funding, technology research and development and policy focus, it could be safe to say that China is following a specific plan towards advancing the process of space-cyber assimilation, jointly in civilian and military fields.

In 2016, what has been viewed as an engineering marvel, a venture dealing with the space-ground integrated information network (SGIIN), was approved. This is not a military venture, at least officially. This project highlights China's national strategic intentions towards promoting the comprehensive integration of space-based information networks, the Internet of tomorrow and mobile communication networks by 2030. With this project and the support of similar ventures, the push is on building a converged, high-speed, secure, and innovative digital infrastructure by deploying a new generation of space-based information network technology. China's vision for the construction of joint space-cyber facilities is echoed in the following straplines:

Functional aggregation: Focus on the satellite constellation industry for PNT and communications services and other possible multiple space-based functions.

Orbital combination: The aim is not to restrict LEO alone but to have a multi-layer space structure that combines satellite constellation systems in medium-Earth orbit and geosynchronous orbits.

Organizational diversification: Cyber and space are important for the Belt and Road Initiative (BRI). Involve multilateral platforms to push their agenda of improved space-based network coverage.

Force integration: Space and cyber arenas in China are basically under the total control of the People's Liberation Army (PLA). China's fifth military service plays a major role. The Strategic Support Force (SSF) was formed in 2015 to decide the policies and programmes in this field. China's 2019 defence white paper describes the role of the SSF. [92] The principal structure of the SSF is a two-tiered stratum of Cyber Force and Space Force. There is an (unseen) PLA stamp on almost every activity in this domain, and civilian structures become part of the 'game' under the canopy of Military-civil fusion.

Overall, China understands the seriousness of cyber threats in space. In recent times, there has been much learning from the satellite hacking incidences witnessed during the Russia-Ukraine crisis in 2022. There is much concern about the possible cyber dangers to the BeiDou navigation satellite structure. China's Ministry of Foreign

[92] "China's National Defense in the New Era", July 24, 2019, https://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html

Affairs has expressed concerns regarding the possibility of massive use of cyber means and the deployment of cyber forces during or before the start of any conflict. There is a feeling that any such attacks could even lead to irrepressible consequences, and there exists a possibility of triggering a nuclear strike. They argue that, a few years back, the US had considered developing policies like intensifying the scope of nuclear retribution if any major incident of non-nuclear strategic attack happens. Also, China is fully aware of the security issues of commercial birds. Against this backdrop, China is working on various governance procedures which could be applicable for domestic purposes and internationally. Some of them include:

Space environment management: China has various guidelines and procedures on space governance. The state also keeps track of activities related to the commercial space industry, in general, and those associated with small satellite constellations. They also ensure that the industry works in tune with the various regulations.

Cross-domain situational awareness: There is a realisation of the limitations of their available structures towards space situational awareness (SSA) and satellite cataloguing capabilities. Also, the scientific community is working on various ideas towards enhancing cyber situational awareness in space.

Zero trust architecture: In 2021, the China Electronics Standardization Association announced the 'Technical Specification for Zero Trust System,' their first national technical standard for zero trust architecture (ZTA). This is expected to offer a high degree of security. Zero Trust is a strategic method of cybersecurity that safeguards an organization by eradicating implicit trust and continuously validating every stage of digital interaction. This idea is entrenched in the belief of 'never trust, always verify.' [93]

INDIA. For the Indian state, ISRO is the principal space research and development organisation. The private sector is evolving, with start-ups doing some innovative work and ISRO doing the required handholding. There are approximately 60 Indian satellites out in space, which are operational. Since 1999, on a commercial basis, India has launched 422 satellites for 34 different countries as of March 26, 2023. India also has established a defence space agency (DSA, 2019) to cater for its strategic needs. In March 2019, India undertook an ASAT test, and its kinetic kill vehicle destroyed a target satellite at an altitude of 283 km. Such a low altitude was selected to avoid debris problems, and almost all the debris created vanished within one year.

The Indian Computer Emergency Response Team could be called a single point contact within the Ministry of Electronics and Information Technology to address various cybersecurity-related threats. India follows various global norms in space and

[93] "Zero Trust cybersecurity with Brama Systems", Brama Systems, https://bramasystems.com/news/zero-trust-security-brama-systems/

cyber and is a signatory to various important mechanisms. India gets viewed as a transparent power in both cyber and space domains. However, much needs to be done domestically in the combined domain of space and cyber. The National Cyber Security Strategy, which connects with the Data Security Council of India, does not reference space infrastructure. India has established the National Technical Research Organisation (NTRO) mainly to deal with technical intelligence. Such agencies are expected to invest towards gathering intelligence by using space-based assets. NTRO possibly has some cyber security mandate too. Ensuring the safety of security of space systems could be the mandate for such agencies. However, nothing is officially known in this regard. India has established a centre reserved for advancing the military space capacities within the DRDO. It is possible that this center could have some mandate to look at cyber threat aspects to space systems. ISRO, a leading global space agency, must take some proactive measures (their satellite design and production teams) to address the issues of cyber vulnerabilities. In open source, little is known about the cyber-related protective measures India took for its space sector. It is vital for a progressive space power like India, with significant commercial aspirations, to plan and devise an inclusive and orderly policy that shields space assets from cyber warfare. As a responsible and transparent space power, India needs to pronounce their policies in this regard.

CONCLUSION & POLICY RECOMMENDATIONS

Weaponization of space is a reality, and increasingly it is becoming clear that cyber threats to space systems will not only stay but are likely to inflate in the future. This is primarily because state actors (could be silent) increasingly depend on cyber as a critical (military) tool in their counter-space calculus. Along with kinetic weapons, cyber technology-based weapons could also be viewed as a subpart of deterrence architecture. This would primarily depend on how academicians can develop a theoretical and technological context about the role of cyber weapons against space targets in warfare. As such, these weapons have been recognised as usable weapons for long. The ongoing Russia-Ukraine conflict (since 2022) has already established its worth.

Using cyber weapons against space-based systems or associated ground infrastructure comes with some important advantages for the attacker. These weapons do not create space debris. Also, tracing the attacker is difficult (the issue of attribution). These are cost-effective weapons and could be launched with significantly less lead time. The user of such weapons could be an individual, a small group, a non-state actor or a state actor. Under these settings, it is evident that such digital options could be preferred for damaging the adversary's space-based capabilities. It would always have greater traction for the state and rogue elements.

The business of launching satellite constellations is on the increase, mainly owing to space-based Internet becoming a reality. There are other reasons, too, for the rise in the number of launches, like used for military, disaster management and particularly for smaller states, the necessity emerging due to nationalism. On the other hand, the threat to space systems is growing not only for military reasons but there could be some commercial reasons too. Remarkably, threats to space systems providing internet, navigation and communications services are increasing. Attacks on these systems would have consequences both for civil and military. Modern space systems have embedded 5G technologies. Supply chains have increasing dependence on space, cyber and blockchain structures. All this makes space-based systems lucrative targets, and cyber-attack emerge as the most viable option for evil actors.

Space security is a complex issue with no easy solutions in sight. In principle, space qualifies as a ‘global common’. However, it looks to be a utopian idea in the present context. States understand that cyber option as counter-space technologies is a double-edged sword. To protect their space systems, they need to find workable solutions. It is a reality that no existing rules, norms, or codes of conduct in space policy or cyber security policy can address this issue. Hence, the complex problem of identifying and mitigating cyber threats to the space domain requires a multipronged approach. There is a realisation that there cannot be one solution to this problem. States

would be required to be both proactive and reactive. Minimal options are available regarding anticipatorily securing legacy systems, and immediate reaction to limit the damage is necessary. The systems under development should be designed to withstand cyberattacks as far as possible.

The present-day space systems include various governmental and commercial plans. Interestingly, commercial space systems could also play a role in matters related to national security, and the Russia-Ukraine conflict has demonstrated that. Unfortunately, owing to finical reasons on many occasions, it has been observed that the cybersecurity-related aspects get (at times, inadvertently) overlooked in the case of commercial satellites. It is essential to realise that cybersecurity and space security are intricately related. There is a need to sensitise various agencies associated with these sectors about these challenges.

Defence-in-depth is about having multiple layers of security for rounded protection. To ensure the safety of space assets, it is important to evolve a mechanism with defence-in-depth techniques. This needs to happen across governments, various non-governmental agencies, and industry. All these actors are required to develop mechanisms to ensure that space systems and associated infrastructures are resilient to cyber compromise. Potential solutions should emerge at international levels as a collaborative effort. There is a need to develop common standers collectively. Achieving a policy acceptable to all could be challenging, but efforts should be made towards contriving some sort of universal panacea. There could be issues (commercial and strategic), particularly with states having technological leads, regarding sharing technical solutions. However, there is a need to work towards finding global answers (as far as possible), and for that purpose, various existing multilateral and UN platforms should be used constructively.

It is important to realise that traditional cybersecurity procedures designed for terrestrial systems may not fully work for space systems, and additional measures (both technological and policy) would be required. States have understood (some have experienced) the enormity of the threats and have put in place mechanisms mainly in the form of suggestions to the developers and operators about how to handle the dangers and what precautions the satellite and ground system developers should take. The real challenge is ensuring the regulatory frameworks keep pace with technology evolution. There could be various systemic challenges over here, and it is said that technology would always overtake the regulation mechanisms. Typically, the life of a satellite could be anything between three to fifteen years. Once the satellite is launched with a particular set of security structures, it would be difficult to update it remotely after some years. The technology on board operational satellites and the latest technological developments will always be mismatched. Future satellite system developers need to think about such challenges.

It is a reality that no solutions would guarantee 100% success, but the quest for technological and policy measures should continue. Appropriate international space-cyber regulations are part of the solution, and to ensure better cybersecurity in space systems, stakeholders need to work together. Space systems are the nation's critical infrastructure and all efforts should be made to ensure their safety and security. Human dependence on space has already reached an 'excessive' level, and it is impossible for humans to function without assistance from space systems. Any major and continuous breakdown in space-based services would have significant social ramifications. States need to understand that the weaponization of the space domain is in nobody's interest. Space systems and associated ground infrastructure security are too critical to fail. All efforts should ensure that space and ground systems are not manipulated by cyber means.

“Over the course of time, there has been a substantial increase in human dependence on space systems to facilitate diverse activities ranging from governance to defence. Contemporary applications of satellites encompass meteorology, communications, navigation, and remote sensing, all of which are utilized on a routine basis. Owing to the profound reliance of nation-states on these space systems, they have emerged as alluring targets for military endeavours by adversarial entities. Inflicting physical harm upon outer space systems through conventional means poses significant challenges. Consequently, certain rogue agencies, with or without state support, have turned to cyber methodologies as a means to pose threats to satellites and the associated infrastructure. This pressing reality calls for immediate and dedicated attention towards enhancing the cybersecurity posture surrounding space assets. In this context, the monograph thoroughly examines various aspects pertaining to conceivable cyber threats against space architecture and endeavours to propose potential mechanisms to effectively counter such formidable challenges.”

About the Author

Dr. Ajey Lele is a Consultant at the Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA) in New Delhi. He previously held the position of Senior Fellow at the same institute. His areas of expertise revolve around Weapons of Mass Destruction (WMD), focusing on Chemical and Biological Weapons, as well as Space and Strategic Technologies. Dr. Lele has a rich portfolio of published works, including books such as "Bio-Weapons: The Genie in the Bottle" (Lancers, 2004), "Strategic Technologies for the Military" (Sage, 2009), "Asian Space Race: Rhetoric or Reality?" (Springer, 2012), "Disruptive Technologies for the Militaries and Security" (Springer, 2019), "Institutions That Shaped Modern India: ISRO" (Rupa, 2021), and "Quantum Technologies and Military Strategy" (Springer, 2021). In recognition of his outstanding contributions to the field of strategic and security studies, Lele was honoured with the K. Subrahmanyam Award in 2013. He has also contributed to various publications, including Strategic Analysis, Indian Defence Review, Space Policy, and Astro-politics. Additionally, Lele played a pivotal role in the establishment of the journal CBW Magazine and presently serves on the Editorial Committee of the Journal of Defence Studies.

sspc