71-95

CYBER ATTACK AGAINST SATELLITES

Capt (Dr) Nitin Agarwala, Indian Navy

Abstract

The importance of space sector to life on Earth is difficult to quantify. Everyday services like communication, air transportation, maritime trade, weather monitoring and forecasting, remote sensing, financial services, television, and even defence rely heavily on space infrastructure. As this dependency increases, risk of cyber threats to this infrastructure increases for both the provider and the policymaker. The fact that critical security gaps exist in construction of both old and new generation satellites make the problem even more complex. While old satellites were designed and built with little knowledge about cyber security, new ones are being manufactured to be cheap thereby forcing investment in cyber security to be disregarded.

The resulting cyber vulnerability poses risks to both space-based and ground-based assets. If these vulnerabilities are not addressed, they could impact financial growth and security at the global level. A cyber-attack on a satellite used for communication would result in interruption to communication that could cause panic, and even endanger security of that nation. With countries and private actors acquiring and employing numerous counter-space capabilities, the threat is no longer hypothetical.

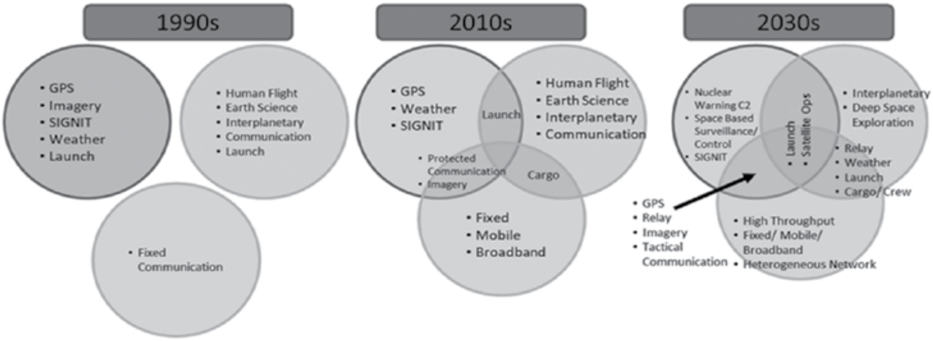
It is with this understanding that this paper aims to look at increasing cyber threat scenarios in the space sector, space infrastructure that requires hardening to address these cyber threats, and challenges and opportunities cyber threat poses to public policy.

INTRODUCTION

Human activities in space increased after the first artificial satellite was launched in 1957. In the last 66 years, 15,946 objects (that include satellites, probes, landers, space station elements, and crewed space-crafts) have been sent into space. Of these 11,330 satellites currently orbit the Earth while others have either fallen back, destroyed in space or orbiting other celestial bodies. Of the orbiting satellites, 6,718 are operational while 3,266 are useless chunks of metals that continue to move around in space. These satellites belong to various countries and have multiple purposes. These include 4,823 for communications, 1,167 for observation of the Earth, 414 for technology development and demonstration, 155 for navigation and positioning, 109 for science and observation of space, 25 for studies of Earth science and 25 for miscellaneous purposes.[1] These satellites may orbit in four main Earth orbits; LEO (Low Earth Orbit – 500 to 2,000 km), MEO (Medium Earth Orbit – 2,000 to just below 35,786 km), HEO (Highly Elliptical Orbit – above 35,786 km) or GEO (Geosynchronous Earth Orbit – exactly at 35,786 km). Small satellites dominate LEO as they are easier to reach while large ones dominate GEO. Due to the distance involved, radio signals travel lesser to reach LEO than GEO and hence satellites in LEO can deliver high-quality internet services and better communication with IoT devices.[2] Accordingly, 84 percent of satellites are found in LEO, 3 percent in MEO and the remaining in GEO.[3] Of the satellites that are operational, 57 percent are used for communication (37 percent for business, 11 percent for civil and 9 percent for military), 9 percent for military and surveillance, 8 percent for navigation, 9 percent for remote sensing and 4 percent for meteorological purposes.

With the number of satellites increasing rapidly, dependence of human life on these space systems has impacted our lives in important and fundamental ways. These activities include trade and commerce; financial transactions; communication; agriculture; transportation; weather assessment and prediction; entertainment; health care to name a few. The convergence of information gathered has been so phenomenal that sectors, products and services are fast amalgamating as seen in **Fig. 1**. Dependence on space has increased so much that if this infrastructure were not available, most of these services would experience a serious degradation or a complete shutdown.

Figure 1: Growing convergence of Sectors, Products and Services (Source: Author, Adapted from NAP, 2016)[4]



Like any other digitised infrastructure, satellites too are vulnerable to cyberattacks. The resulting cyber vulnerability poses risks both to space-based and ground-based assets. If not addressed, the threat could impact global economic development and international security. A cyber-attack on a satellite used for communication would result in interruption to communication that could cause panic, and even endanger security of the nation. With countries and private actors acquiring and employing numerous counter-space capabilities, the threat is no longer hypothetical. As risk of cyber threats to this infrastructure increases, it creates challenges for both the provider and the policymaker.

It is with this understanding that this paper aims to look at the increasing cyber threat scenarios in space sector, space infrastructure that requires hardening to address these cyber threats, and challenges and opportunities cyber threat poses to public policy.

UNDERSTANDING SPACE SYSTEMS AND THEIR VULNERABILITIES

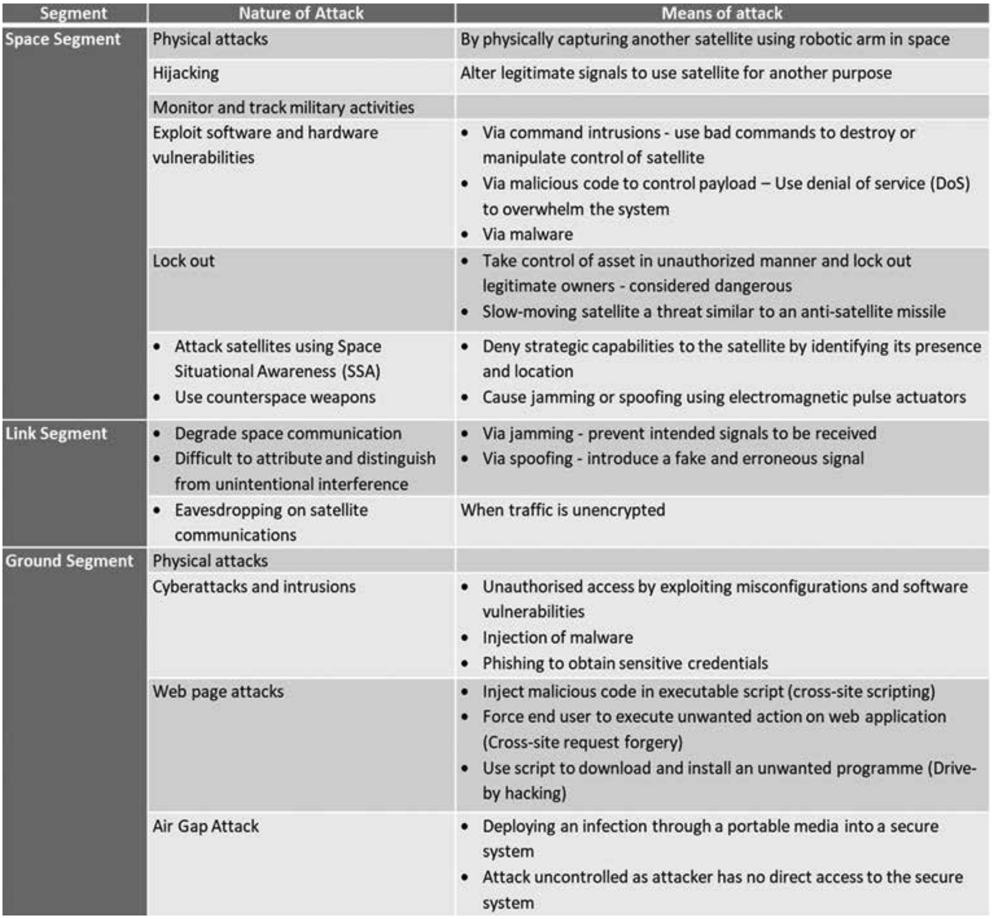
When discussing cyber threat to satellites, it is important to evaluate cyber threat for the entire space system as the satellite is incomplete without the ground and the link segment. Hence, the space system is understood to be made up of three segments. The *space segment* that is made up of the satellite and its launch vehicle, the *link segment* provides a communication channel between two or more satellites and the satellite and ground station, while the *ground segment* is made up of ground elements that provide command and control of the satellite, and management and distribution of data received from the satellite. Since all three segments are digitised, they are susceptible to a range of cyber threats.[5]

A major security gap exists for the *space segment* in satellites of the current and the past generations. While earlier satellites were constructed with little awareness of cyber security, newer ones focus on fast and cheap production and hence funding for cyber security is kept to a minimum. These attacks can be executed through weaknesses in either the ground stations or network components or receivers receiving data from satellites. Expected cyberattacks on the space systems is by giving bad instructions to either destroy or manipulate controls (called command intrusions), by controlling payload (using malicious control such as Denial of Service), through malware (thereby infecting space systems and ground systems) or through spoofing communications to trust the source, or interrupt/delay communication. The consequences of these attacks can be amplified due to growing use of Internet of Things (IoT) devices that are connected to these satellites.

The most common threat to the *link segment* is manipulation of radio signal between the satellite and ground station. Since GPS system is the most important radio signal transmitted by a satellite to the ground station it is susceptible to attack by *jamming* or *spoofing* by disrupting or tampering with the frequency signal. Between these, spooking is more difficult than jamming to achieve but when executed correctly, it can cause greater damage as the victim is unaware of the attack. Yet, another type of attack is to *alter the legitimate signals* so that the satellite can be used for some other purpose. Such an attack is called as broadcast signal intrusion. In this, broadcast signals are hijacked by using signals of higher strength but same frequency. This hijacking can also be achieved by directly breaking into the transmitter to replace the signal.[6] Such a hijack is possible only with unencrypted signal traffic that can be intercepted, eavesdropped and modified conveniently.

The *ground segment* is responsible for collecting data from satellites and hence is exposed to cyber espionage through downloading of malwares and Trojans. These malwares and Trojans when downloaded allow attackers to access and control the satellite.[7] These threats are summarised in **Table 1**.

Table 1*:* Threats Experienced by the Space System



Segment	Nature of Attack	Means of attack
Space Segment	Physical attacks	By physically capturing another satellite using robotic arm in space
	Hijacking	Alter legitimate signals to use satellite for another purpose
	Monitor and track military activities	
	Exploit software and hardware vulnerabilities	• Via command intrusions - use bad commands to destroy or manipulate control of satellite • Via malicious code to control payload – Use denial of service (DoS) to overwhelm the system • Via malware
	Lock out	• Take control of asset in unauthorized manner and lock out legitimate owners - considered dangerous • Slow-moving satellite a threat similar to an anti-satellite missile
	• Attack satellites using Space Situational Awareness (SSA) • Use counterspace weapons	• Deny strategic capabilities to the satellite by identifying its presence and location • Cause jamming or spoofing using electromagnetic pulse actuators
Link Segment	• Degrade space communication • Difficult to attribute and distinguish from unintentional interference	• Via jamming - prevent intended signals to be received • Via spoofing - introduce a fake and erroneous signal
	• Eavesdropping on satellite communications	When traffic is unencrypted
Ground Segment	Physical attacks	
	Cyberattacks and intrusions	• Unauthorised access by exploiting misconfigurations and software vulnerabilities • Injection of malware • Phishing to obtain sensitive credentials
	Web page attacks	• Inject malicious code in executable script (cross-site scripting) • Force end user to execute unwanted action on web application (Cross-site request forgery) • Use script to download and install an unwanted programme (Drive-by hacking)
	Air Gap Attack	• Deploying an infection through a portable media into a secure system • Attack uncontrolled as attacker has no direct access to the secure system

Source: Author from various resources

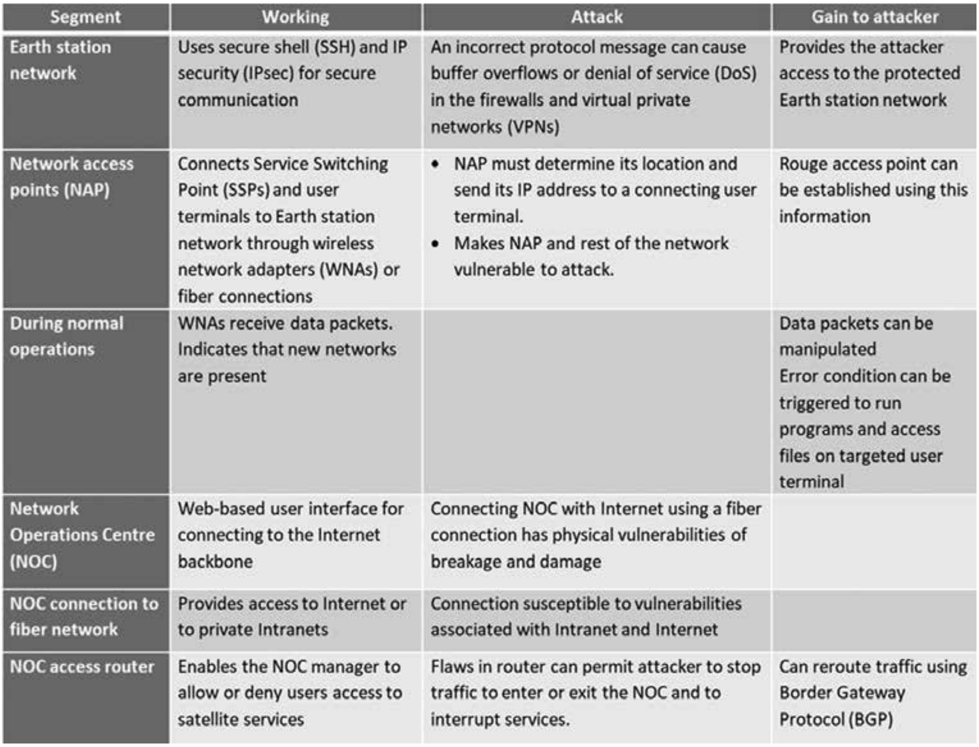
It is important to mention that an unethical attacker is usually looking for financial gains when attacking a civilian satellite. However, when attacking a military satellite, the gains may be direct 'strategic' control or financial gains by 'selling' control to a third party. Of these, the military satellite space system while susceptible to cyberattacks, is better equipped to handle such threats through hardened procedures and hardware, we will limit our discussion to civilian satellites. For such satellites, the most productive attack for an attacker would be on services that relate to financial systems or services for which someone would be ready to pay a ransom. Since the space systems are associated with a variety of services, they are a lucrative target especially since they have the ability to impact a number of systems from a single point. Say, a gas distribution company that relies on satellites for communication for health monitoring of their pipelines if compromised can result in pipe explosion merely by inhibiting maintenance calls. Effectively, the attacker by inhibiting maintenance will be able to impact supply distribution, profits and working of the gas company.

The problem gets complicated due to technology advancement, reducing cost of satellite development due to use of open-source software,[8] use of commercial-off-the-shelf (COTS) products and lack of international or industry security standards governing space systems that does not necessitate high level of cyber security standards and hence makes attack simpler and undetected at times. Furthermore, since no clearly defined procedure exists to discover, analyse risk, mitigate or for remedy of cyberthreats during the lifespan of space systems, detection of a malware may never happen till it causes interruption of services. The situation is exacerbated due to lack of clearly defined responsibility for cybersecurity and management of space systems. With commercial agencies transforming space based capabilities, the need for regulating cybersecurity in this sector cannot be but over-emphasised.

HOW CAN ATTACKS BE CARRIED OUT?

From the discussion in the preceding section one notices that ground segment is possibly the weakest link in the entire space system. This is primarily because ground segment is susceptible to physical attacks and is also approachable. Furthermore, once someone has access to the ground segment, controlling the space segment becomes easy. However, for services such as the Amazon Web Services Ground Station and Microsoft Azure Orbital that connect to satellites from anywhere to provide instant access, attack on ground segment becomes irrelevant. For others, some of the earth segment vulnerabilities are as seen in **Table 2**.

Table 2: Earth Segment Vulnerabilities



Segment	Working	Attack	Gain to attacker
Earth station network	Uses secure shell (SSH) and IP security (IPsec) for secure communication	An incorrect protocol message can cause buffer overflows or denial of service (DoS) in the firewalls and virtual private networks (VPNs)	Provides the attacker access to the protected Earth station network
Network access points (NAP)	Connects Service Switching Point (SSPs) and user terminals to Earth station network through wireless network adapters (WNAs) or fiber connections	• NAP must determine its location and send its IP address to a connecting user terminal. • Makes NAP and rest of the network vulnerable to attack.	Rouge access point can be established using this information
During normal operations	WNAs receive data packets. Indicates that new networks are present		Data packets can be manipulated Error condition can be triggered to run programs and access files on targeted user terminal
Network Operations Centre (NOC)	Web-based user interface for connecting to the Internet backbone	Connecting NOC with Internet using a fiber connection has physical vulnerabilities of breakage and damage	
NOC connection to fiber network	Provides access to Internet or to private Intranets	Connection susceptible to vulnerabilities associated with Intranet and Internet	
NOC access router	Enables the NOC manager to allow or deny users access to satellite services	Flaws in router can permit attacker to stop traffic to enter or exit the NOC and to interrupt services.	Can reroute traffic using Border Gateway Protocol (BGP)

Source: Author; from[9]

KNOWN CYBERATTACKS

It is clear that a space system is susceptible to a range of attacks. However, space systems lack international and industry standards that require assets to protect the system from cyberattacks. Hence, involvement and knowledge of users regarding cyberattacks is limited. This ignorance disallows a mechanism for reporting any attacks on such space systems. To add to this, since space systems have a connection with government activities, little information regarding their being compromised is hard to find. It is interesting to note that with wide proliferation of social media, even videos of how to hack satellites are available for a prize (Hacking Digital Satellite Systems available for $29.95 plus $3.50 for shipping) and advertised regularly in print media.[10]

Research conducted by Ruben Santamarta in 2014 on ten leading SATCOM terminals used by the military and the mercantile marine shows that these systems use weak default passwords. The backdoor used by programmers for data units (for communication control) and control units (for control access) were easily accessible and in default mode and protocols used to communicate between control unit and user interface had a weak authentication mechanism.[47] Another study by the Department of Commerce in August 2014 in the US on security weakness of the ground system of the Joint Polar Satellite System (JPSS) showed them to be 14,000 in 2012 which increased to 23,000 in 2014. This was attributed to complacency in compliance by internal auditors and unwillingness to deviate from scheduled updates.[48] In the following November, the NOAA satellite system was attacked by attackers believed to be from China.[49] These episodes showed that poor cyber practices need to be addressed to avoid a security breach. Notwithstanding ignorance, since space systems are a critical system for economic health and security of a nation, cybersecurity agencies continue to monitor cyberattacks. While many go undetected and hence unreported, there are many others which have been reported albeit many years after attack have occurred. For these, the exact details may be confidential but some such attacks are discussed here to provide importance and relevance of such attacks on space systems. To appreciate the magnitude of these attacks, such events have been arranged chronologically and seen in **Table 3**.

The cases mentioned here provide an idea of how satellites are susceptible to cyberattacks. These cases do not discuss other cyberattacks as they are considered to be beyond the scope of this article. These events are however not considered to be a complete list of such events. A more extensive list for the duration 2006 – 2023 can be found in a publication of the Center for Strategic and International Studies (CSIS).[50]

Table 3: Known Cyberattack Event on Satellites

Year	**Affected**	**Impact**	**Remarks**
Earliest intrusion	Digital video broadcasts	• Information transmitted without encryption. • Can be seen by anyone who can intercept the signals	• Tutorials to intercept signals freely available online[11 12] • Common since 1970s[13]
June 2002	Intercepting signals to view NATO flights over the Balkans	• Internet connection of satellite can be intercepted as signals are unencrypted. • First indication that interceptions could impact military too.[14]	• Attacker can steal IP addresses as shown by Turla attacks. • Can be carried out by Advanced Persistent Threat (APT) groups (HackingTeam, Xumuxu group and Rocket Kitten) • Not widespread. • If spreads, will be a serious problem for security agencies.[15]
1997 - 2013	Cyber espionage against NASA networks was reported 12 times	Chinese nationals including Bo Jiang arrested with technology related information not supposed to be with them.[16]	

1998	ROSAT satellite	Sustained physical damage	• Satellite made to face the Sun by executing a command • Possibly by Russia - as a cyberattack.[17]
2002	SinoSat satellite hacked	Interrupt transmission of China Central TV (CCTV) and China Education TV.[18]	By Falun Gong, a controversial religious group of China
2004	AsiaSat hacked	Disruption of signals for nearly four hours.[19]	
2003 - 2006	DoD, NASA, aerospace contractors & research institutions working on space propulsion, solar panels & fuel systems infiltrated	Coordinated attacks from China under an infiltration campaign named "Titan Rain".[20]	• For APT-One (a cyber-espionage unit of PLA) as reported by Mandiant Technology.[21] • Aerospace industry is second most targeted industry • Satellite industry is fourth most targeted
2006	Libyan nationals	Jammed mobile satellite communications for nearly six months	To control smuggling of contraband from Chad and Nigeria.[22]
2006	Israel-Lebanon war	Al-Manar satellite channel was a target for unsuccessful jamming by Israel.[23]	• To stop Hezbollah leader to reach his followers • Commercial satellites could be potential target during conflict.
2007	Goddard Space Flight Centre was cyber attacked		For data regarding earth observation systems.
2008	NASA satellite Landsat-7 was cyberattacked	Interference for 12 minutes	

2008	NASA satellite, the Terra-EOS AM-1	Interference and loss of control • June - 2 minutes • October - 9 minutes	• Attackers could not command satellite as they did not understand actual commands for satellite manoeuvre.[24] • Some experts believe that this was interference/ jamming radio signals and not cyberattack
April 2007	Hacking of Euro Star 1 and INTELSAT-12	Illegally broadcast radio and TV signals using empty transponder on-board INTELSAT-12.[25]	The Liberation Tigers of Tamil Eelam (LTTE) of Sri Lanka accused of transmitting propaganda
2007	At least two environment monitoring satellites of the US	Cyber attacked from a ground station in Norway	• Hack traced to China • Was possible by using Internet to connect to ground station. • Hackers achieved full control of satellites - no equipment or data were compromised.[26]
2008	The International Space Station (ISS) computers	• Hackers infiltrated mission control computer network of Johnson Space Centre &uploaded a malicious Trojan • Disrupted on-board communications • Did not endanger crew or space flight.[27]	Was possible as computers not receiving software updates

2009	Iraq able to download unencrypted live video stream from American Predator drones	• Used an inexpensive, off-the-shelf software – SkyGrabber • Originally developed to • Receive unprotected satellite TV feed • Gain access to the Internet in areas of Russia	• Hacking allowed insurgents to take evasive action against the planned drone attacks.[28] • Possible because of lack of security in link system between satellite and drone. • Flaw known to designers • Requisite encryption protocols not used - as it made communication ineffective due to reduced speed. • Activity of insurgents categorised as interception hacking. • Data extraction could have been prevented if encryption was used.[29]
2009	BBC broadcast of elections in Iran was jammed	Jamming was accompanied by a cyberattack on the email service of the BBC.[30]	Most probably by Iranian government
Sept 2011	American RQ-170 Sentinel drone	Made it to land in Iran instead of Afghanistan.[31]	GPS signal reconfigured by Iran
October 2011	US Creech Air Force Base (AFB) faced a malware attack on the Predator and Reaper drones	• Attack from infected ground control stations • Earlier compromised using keystroke logger • Attack believed conducted by intelligence services of Russia or China.	• Attack on ground control system that was air gapped • Attack a classic example of air gapping method

March 2012	The BBC	• Disrupt Persian Language Services • Jam two BBC satellite feeds to Iran	
March 2013	Aerospace and defence companies and contractors of the US operating in the South China Sea	Chinese hackers found to be attacking maritime operations and maritime satellite systems, for nearly one year	
February and May 2013	BGP hijacking	Show live evolution of 21 events of Belarus[32]	Broader Gateway Protocol (BGP) hijacking (maliciously intercepting or rerouting internet traffic)
July - August 2013	BGP hijacking.	Show live evolution of 17 events of Iceland[33]	
2014	Crimean Conflict	Ukrainian authorities reported jamming of incoming GPS signals for entire area by the Russian Federation	Jamming caused chaos for navigation system of phones and several aircrafts.[34]
2014	Western companies associated with manufacturing or researching satellites	PLA Unit 61398 was undertaking space surveillance for targeting.[35]	CrowdStrike reported the event
2014		China Telecom repeatedly sent cyber traffic inside Russia from their servers	Not clear if this incident was malicious or accidental routing leak.[36]
2015	Max Headroom Broadcast Signal Intrusion[37]	Powerful microwave signals attackers hijacked satellite signals.	• No one claimed responsibility • Showed that regular TV signals could be hijacked at ground station using microwaves.

2017	GPS system of at least 20 ships spoofed	Shifted destination port 32 km inland making Gelendzhik Airport in the Black Sea as final destination	GPS spoofing was part of new electronic warfare technique being experimented with by Russia.[38]
April – June 2018	Satellite operators, defence contractors, and telecoms companies in the US and Southeast Asia	Infiltrated by Chinese hackers.[39]	Attacks undertaken with an aim of espionage and possible disruption.[40]
November 2018	Trident Juncture exercise of NATO	GPS signals were disrupted and Russia was suspected for doing so.[41]	
2018	US domestic Internet communication	Routed through servers of China Telecom	Possible by manipulating border gateway protocol (BGP) tables from 2015 to 2017
2019	Internet traffic destined for mobile providers in Europe	Rerouted to servers of China Telecom for two hours.[42]	Another incident of BGP manipulation
initial six months of 2020	BGP hijacking	Over 1,430 incidents worldwide, averaging 14 hijackings a day	Mostly involving big financial or telecom companies.[43]
March 2022	Cripple Viasat KA-SAT satellite communication network of Ukraine	Cyberattacks by Russia on the eve of its attack	Attack undertaken using a malware named 'AcidRain viper' that wiped out targeted modems to cripple them.[44]
June 2023	Telecommunication service provider satellite of the Russian FSB and military units	By Ukraine protest group associated with Wagner, a private military corporation.[45]	

August 2023	Starlink with a malware	By GRU of Russia to get Ukrainian troop movement	- Found by State Security Service (SBU) of Ukraine - Verified when SBU found malware on tablets recovered from Russians but originally belonging to Ukrainian soldiers.[46]

Source: Author's compilation

DISCUSSION

While cyberattacks as discussed in the previous section continue to occur the world over on satellites, there is a mixed acceptance about these events being hacking events. One school of thought is that as long as encryption does not exist, reconfiguration would not happen. This means that if functions originally facilitated by the administrator have not been altered, hacking is not deemed to have occurred. The other school of thought is that a hack is a quick fix that provides access to features that were otherwise inaccessible. It is the second school of thought that is usually employed to refer to nefarious activities that are categorised with cybercrime. Similarly, when talking about interception of digital video feeds since these signal are freely available and need only decoding as done by programs such as SkyGrabber, these acts while against the law cannot be considered as a cyberattack.

Before a unanimous decision is arrived at regarding this issue, such security interceptions of satellite signals are important to realise vulnerabilities that exist in this critical infrastructure. It also acts as an eye opener for policy makers and security agencies to ensure that these vulnerabilities are addressed. However, like any other information technology industry, such security controls are never put in place till a serious breach occurs and results into a serious loss. Unfortunately, this has been the operating principle for the industry for years and is considered an acceptable methodology that does not require a change. It is hence not surprising when researchers identify several vulnerabilities in software of GPS receivers belonging to both government and commercial grade or in computers of ground stations that control the satellites.

To date, the focus on providing security against cyberthreats has been to leverage cryptographic protection for data both in transit and at rest using strong encryption algorithms. While this was sufficient till now, capabilities of attackers is rapidly evolving. It is essential that this security gap be closed in future systems, and mitigating procedures adopted for platforms in orbit wherever possible.

Today, Black Hat activities are centred in a few countries and hence major cyberattacks are attributed to them. However, this may not be always true. The fact on ground remains that such activities are mostly undertaken by independent groups and usually not state sponsored. What remains as an area of concern is that as the number of satellites in space increase, their vulnerability is likely to increase since best practices of the IT industry are not implemented in these systems which could have a large and catastrophic impact on our individual lives. As the number of satellites increase, there is a likelihood that the number of players undertaking such attacks would only increase.[51]

It is thus important that information on such attacks is shared within the industry for greater learning and remediation actions and strategies that could possibly prevent another organisation to experience the same fate. In addition, emerging threats need the industry and policymakers to focus on ways and means of hardening the space architecture so that space systems can be protected from cyberattacks. However, use of implementing such technology should be done with due attentiveness to potential challenges and associated costs as the initial investment required for such hardening can be significant. This thus requires a look at the challenges and opportunities that such attacks create for public policy and how this critical infrastructure can be made secure.

CHALLENGES AND OPPORTUNITIES TO PUBLIC POLICY

Policy makers are usually driven by the magnitude of the problem and the acceptable risk that can be permitted to be associated with a given problem. In case of the space industry, since acceptance of given threats is not explicitly defined or very well understood, policy makers tend to distance themselves from the problem at hand. However, as discussed, the need for international and industry standards for cybersecurity of space systems is essential and cannot be delayed. This need is only going to increase with the sector being thrown open to the private sector. It essentially means that if adequate and timely steps in establishing policies for the space sector are not employed, the magnitude of problem may increase many a fold and become cost prohibitive to handle or even difficult to contain.

Hence, policy makers need to look at hardening the three segments of space infrastructure against cyberattack. These include the *space segment* that is considered vulnerable to attacks through command intrusions, payload control or denial of service, the *link segment* that are under threat from interference, and the *ground segment* that are susceptible to physical and virtual attacks alike. This, thus, requires them to look at not only ground stations but also at standards to be followed by satellite manufacturers to provide required hardening of space system infrastructure. The feature of hardening can be incorporated in the space architecture by adopting procedures such as 'Quantum resistance'[52] which is a key theme to achieve hardening for the US which it aims to achieve by 2035.[53] Additionally, military grade encryption such as the gold standard AES (Advanced Encryption Standard) 256 bit and dual tunnel encryption can be used. While Quantum resistance uses immutable laws of quantum mechanics for cryptography, the AES 256 bit encryption makes it difficult for a hacker as they would require 2256 combinations to break the 256 bit encryption. The dual tunnel encryption on the other hand allows data to be encrypted in memory as it moves in an encrypted form to discourage the hacker from stealing information.

Since most of the ground stations are in vicinity of commonly accessibly spaces they are susceptible to malicious intent due to easy access. At times, this intent may be deliberate or accidental. With these ground stations considered as the weakest link in the space system, they need to be made more robust by providing conditioned and generated power, centralised backup facility that is undertaken at varied geographical locations, and implementing standard IT industry norms and functions such as disaster recovery mechanisms and equipping them to withstand electromagnetic pulse and radiological fallout. There is also a need to ensure that human resource engaged in ground stations is adequately trained to understand existing vulnerabilities and impact of downloading unverified information. In addition, physical security of such installations is considered important which could be provided by perimeter fencing, closed circuit security, access control and multiple layer redundancy.

To address interference in the link segment, various types of shielding, filters, training and awareness is considered essential in addition to sharing of root cause analysis of incidents reported to ensure that effective security patches can be developed and disseminated. Furthermore, need to use data encryption including quantum encryption, error protection coding, and use of directional antennas are some other methods that can be effective in reducing interference. To add to these, some features currently being used only by military satellites can be made an industry standard. Methods such as narrowband excision scheme, burst transmission and frequency hopping, antenna side lobe reduction, and nulling antenna systems which observe interference can help address interference and hence cyberattacks on space systems. Though these may increase cost, a balance between cost and security is something that would need to be considered sooner than later. The sector would also benefit if laser based communication, intrusion detection and prevention systems are developed.

It is important to realise that with use of open-source architecture for the satellite industry, this industry is slowly moving towards the traditional IT industry and hence vulnerabilities and solution for such issues employed in the IT industry can be directly employed in the space sector. Since cybersecurity standards, processes, procedures, and methods are already available, there may not be a need for creating new ones. However, their application in the design phase needs to be included to ensure that IT industry standards are effective for which policy making is critical.[54] This additionally requires that hardware used is procured from reliable sources.

With current encryption procedures being challenged, robot encryption for every data transferred to and from any satellite using a VPN solution is a possible way ahead. In addition, to overcome challenges to encryption procedures, network segregation to restrict traffic between segments may be experimented with. A need to monitor networks for suspicious activities using intrusion detection and prevention systems is also considered essential. In addition, an incident response plan to identify, contain, eradicate and recover from any cyberattack is required to be implemented. Additionally, self-healing cyber-physical systems using machine learning can be used. Such system would automatically initiate a reboot if they sense that they are not functioning optimally thereby ensuring that the cyberattack is made ineffective.[55]

TAKE AWAY FOR INDIA

India released its Space Policy in 2023 which aims to enhance space capabilities of the nation by encouraging involvement of the private sector. The policy was released with an aim to increase contribution of the Indian space economy from an existing 2 percent by harnessing the full potential of India's space sector. While the policy has been released, it needs to be followed by legislations and regulations regarding conduct of business. As policy formulation in the space industry is at a nascent stage while cyber threats are well known and looming large, it would be prudent for India to show 'due diligence' towards cybersecurity to become a front runner in this aspect. In this regard work on advanced technological procedures like robot encryption using VPN solution, quantum resistance hardening, and network segregation and monitoring needs to be considered.

It is important to mention that India as a nation is a major contributor to Information Technology Enabled Services (ITeS) industry and hence has requisite knowhow and understanding of needs of cybersecurity for the IT industry. Drawing from this existing knowledge and knowing that the industry standard of future space industry is open-source; India can very well prepare required standards of cybersecurity for the space industry. In the interim, India should work towards establishing 'resilient space best practices' for space companies to develop their cyber protection approaches. These best practices would eventually provide valuable inputs for developing the desired space standards.

Even though naysayers may argue to say that such a step may push the country to costlier systems and hence drive away business in the space sector, this aspect cannot be overlooked. It is an inescapable requirement that should be considered to ensure that the space industry of tomorrow in India is more resilient to cyberattacks and hence is more secure and avoids unintended cost of addressing cybersecurity after launch which would eventually be higher in the long run. As a minimum, this requires that the strategic and technical approach for space systems to combat cyberattacks is incorporated in both old and new satellite space systems. These standards should apply not only to lifecycle stage but also to the development phase including the testing phase and include periodic cybersecurity assessments during development, and before and after launch.

Since the current international space laws (that are underpinned by five international treaties namely, The Outer Space Treaty, The Rescue Agreement, The Moon Agreement, The Liability Convention and The Registration Convention)[56] do not adequately address cybersecurity, there is a need to develop this regime. In doing so, India can engage with the existing intergovernmental organisations but before that it would need to create its own comprehensive domestic systems of cybersecurity for space systems.

This due consideration to cybersecurity is especially important for a nation like India that has limited number of satellites with limited options for meeting requirements through another satellite. Such identifiable satellites can be precision targeted by an attacker if not adequately protected leading to loss of services dependent on these satellites.

CONCLUSION

Space infrastructure is critical to global economic development and international security. However the security of this system has largely been ignored so far due to involvement of governmental agencies in this sector. With increasing dependence on this sector for numerous activities both in the military and the civilian domain, this sector has been subjected to cyberattacks. The problem takes greater importance with an increasing interest of the private sector in space after it was deregulated for them. Accordingly, the paper has discussed cyberattacks, their potential impact on various facets of our daily activities, available opportunities and challenges and takeaway for India.

One realises that as the space sector becomes more commercial, a shift to commercial-off-the-shelf (COTS) items is natural driven by commercial interests. This thus exposes the sector to greater security threats due to cyberattacks usually associated with digitalisation of technology. However, since the sector is critical for economic development and security considerations, it cannot be disregarded and a focused approach to addressing cybersecurity for space systems is essential. Accordingly, hardening using 'Quantum resistance', and using AES 256 bit and dual tunnel encryption are some possible solutions that are being developed. In these efforts, the role of nations such as India who are gaining strength in the global space sector cannot be overlooked.

While India has released its Space Policy in 2023, it needs to work on legislations and regulations. Since cyber threats are here to stay, India can aim to become a front runner in cybersecurity if work on advanced technological procedures like robot encryption using VPN solution, quantum resistance hardening, and network segregation and monitoring are progressed. On the same lines, using its experience and expertise of the Information Technology Enable Services (ITeS) sector India could look at developing 'resilient space best practices' to assist develop desired space standards.

Creating instituting mechanisms and policies to address these cyber threats may be an uphill task as it flouts economics. Since overcoming these cyber threats is an essentiality that cannot be disregarded, it will need to be addressed in future if not now.

Capt (Dr) Nitin Agarwala is a serving naval officer who has authored over 80 articles, papers, book chapters and two books. He was a Research Fellow at the National Maritime Foundation from 2017-2019 and currently a Senior Fellow at the Centre for Joint Warfare Studies. Email: nitindu@yahoo.com; ORCID: https://orcid.org/0000-0003-0916-3044

NOTES

1. Andy, "How many satellites are orbiting the Earth in 2023?" (05 July 2023). https://www.pixalytics.com/satellites-orbiting-earth-2023/. Accessed on 18 March 2024.
2. Z. Qu, G. Zhang, H. Cao and J. Xie, "LEO Satellite Constellation for Internet of Things," in *IEEE Access* 5, (2017): 18391-18401, doi: 10.1109/ACCESS.2017.2735988.
3. NanoAvionics, "How Many Satellites are in Space?," Kongsberg, (04 May 2023), https://nanoavionics.com/blog/how-many-satellites-are-in-space/#:~:text=As%20of%20May%20the%204th,satellites%20in%20various%20Earth%20orbits. Accessed on 18 March 2024.
4. National Academies of Sciences, Engineering, and Medicine, "National Security Space Defense and Protection: Public Report." Washington, DC: The National Academies Press, (2016): 21 https://doi.org/10.17226/23594.
5. Varadharajan, V., and Suri, N., "Security challenges when space merges with cyberspace," Space Policy, (2023), https://doi.org/10.1016/j.spacepol.2023.101600.
6. J. Fritz, "Satellite hacking: a guide for the perplexed," Bulletin of the Centre for East-West Cultural and Economic Studies 10 no 1, (2013): 21–50. [Online], Available: http://www.international-relations.com/CM2012/Satellite-Hacking.pdf. Accessed on 18 March 2024.
7. Sincavage, SM, Carter, N., et al., "Space Based Platforms and Critical Infrastructure Vulnerability (Mccreight)," In Book 7 Nichols (Ed). *Space Systems: Emerging Technologies and Operations.* (KSU – NPP, Los Angeles, CA, 2022).
8. NASA uses cFS as the open source software for its small satellites which is available for free download on GitHub. *See*, Wilmot, J. and Kane, L., "Core Flight System," (2021), [online] cfs.gsfc.nasa.gov. Available at: https://cfs.gsfc.nasa.gov/Introduction.html. Accessed on 18 March 2024.
9. Jessica A. Steinberger, "A Survey Of Satellite Communications System Vulnerabilities," Thesis, (Air Force Institute Of Technology, Ohio, 2008). https://core.ac.uk/download/pdf/288295156.pdf.
10. Scrambling News, "Hacking Digital Satellite Systems Video 2002," Amateur Radio Today, (February 2002): 20. https://www.arimi.it/wp-content/73/02_February_2002.pdf.
11. Adam Laurie, "Satellite hacking for fun and profit," BlackHat, (16 February 2009), https://www.blackhat.com/presentations/bh-dc-09/Laurie/BlackHat-DC-09-Laurie-Satellite-Hacking.pdf.

12. Leonardo Nve Egea, "Playing in a Satellite environment 1.2," Kaspersky, (2015), https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2015/09/20081827/BlackHat-DC-2010-Nve-Playing-with-SAT-1.2-wp.pdf.
13. Judith S. Weinstein, "International Satellite Piracy: The Unauthorized Interception and Retransmission of United States Program-Carrying Satellite Signals in the Caribbean, and Legal Protection for United States Program Owners," Georgia Journal Of International And Comparative Law 15 no. 1, (1985), https://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1774&context=gjicl. Accessed on 18 March 2024.
14. Mark Urban, "Enthusiast watches NATO spy pictures," The BBC News, (13 June 2002), http://news.bbc.co.uk/2/hi/programmes/newsnight/2041754.stm. Accessed on 18 March 2024.
15. Stefan Tanase, "Satellite Turla: APT Command and Control in the Sky," Kaspersky, (09 September 2015), https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/. Accessed on 18 March 2024.
16. J. Fritz, op. cit. p. 33.
17. J. Fritz, op. cit. p. 33.
18. Associated Press, "Falun Gong Hijacks Chinese TV," Wired, (24 September 2002), http://www.wired.com/politics/law/news/2002/09/55350?currentPage=all. Accessed on 18 March 2024.
19. Daly, John C. K., LTTE: Technologically innovative rebels, Wordpress, (18 June 2007), https://lrrp.wordpress.com/2007/06/18/ltte-technologically-innovative-rebels/. Accessed on 18 March 2024.
20. J. Fritz, op. cit. 32.
21. Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," (18 February 2013), p. 24, https://www.mandiant.com/resources/reports/apt1-exposing-one-chinas-cyber-espionage-units. Accessed on 18 March 2024.
22. Space News, "Libya Pinpointed as Source of Months-Long Jamming in 2006," (17 April 2007), https://spacenews.com/libya-pinpointed-source-months-long-jamming-2006/. Accessed on 18 March 2024.
23. Space News, "Inability To Jam Hezbollah Satellite TV Signal Spurs Israeli Research," Space News, (29 August 2006), https://spacenews.com/inability-jam-hezbollah-satellite-tv-signal-spurs-israeli-research/. Accessed on 18 March 2024.
24. J. Fritz, op. cit. 33.
25. Daly, John C. K., op. cit.
26. Charles Arthur, "Chinese hackers suspected of interfering with US satellites," The Guardian, (27 October 2011), https://www.theguardian.com/technology/2011/oct/27/chinese-hacking-us-satellites-suspected. Accessed on 18 March 2024.
27. J. Fritz, op. cit. 33.
28. Mike Mount and Elaine Quijano, "Iraqi insurgents hacked Predator drone feeds, U.S. official indicates," CNN, (18 December 2009), http://edition.cnn.com/2009/US/12/17/drone.video.hacked/index.html. Accessed on 18 March 2024.
29. Ewen MacAskill, "US drones hijacked by Iraqi insurgents," The Guardian, (17 December 2009), https://www.theguardian.com/world/2009/dec/17/skygrabber-american-drones-hacked. Accessed on 18 March 2024.
30. J. Halliday, "BBC fears Iranian cyber-attack over its Persian TV service," The Guardian, (14 March 2012), https://www.theguardian.com/media/2012/mar/14/bbc-fears-iran-cyber-attack-persian. Accessed on 18 March 2024.

31. S. Peterson, "Iran hijacked US drone, says Iranian engineer," Christ Science Monitor. (2011). https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer. Accessed on 18 March 2024.
32. Stefan Tanase, "Satellite Turla: APT Command and Control in the Sky," Kaspersky, (08 September 2015), https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/. Accessed on 18 March 2024.
33. Ibid.
34. T. Harrison, K. Johnson, and T. Roberts, "Space threat assessment 2018," US Center for Strategic and International Studies, (2018). https://csiswebsite-prod.s3.amazonaws.com/s3fs-public/publication/180823_Harrison_SpaceThreatAssessment_FULL_WEB.pdf.
35. Lily Hay Newman, "Report: Another Chinese Military Unit Has Been Hacking U.S. Systems—This Time Satellite Networks," Slate, (10 June 2014), https://slate.com/technology/2014/06/putter-panda-crowdstrike-reports-chinese-military-hackers-have-been-infiltrating-satellite-networks.html. Accessed on 18 March 2024.
36. Dan Goodin, "Citing BGP hijacks and hack attacks, feds want China Telecom out of the US," Technica, (04 October 2020), https://arstechnica.com/tech-policy/2020/04/citing-bgp-hijacks-and-hack-attacks-feds-want-china-telecom-out-of-the-us/. Accessed on 18 March 2024.
37. Katie Serena, "The Story Of The Max Headroom Incident, America's Creepiest Unsolved TV Hack," (15 March 2022), https://allthatsinteresting.com/max-headroom-incident. Accessed on 18 March 2024.
38. Chris Lo, "GPS spoofing: what's the risk for ship navigation?," Ship Technology, (15 April 2019), https://www.ship-technology.com/features/ship-navigation-risks/?cf-view. Accessed on 18 March 2024.
39. Dan Goodin, "China-based hackers burrow inside satellite, defense, and telecoms firms," Technica, (21 June 2018), https://arstechnica.com/information-technology/2018/06/china-based-hackers-burrow-inside-satellite-defense-and-telecoms-firms/. Accessed on 18 March 2024.
40. Threat Hunter Team, "Thrip: Espionage Group Hits Satellite, Telecoms, and Defense Companies," Symantec, (19 June 2018), https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets?API1=100&API2=100017430&SID=100098X1555750Xa111007bba56c9e65774ebf19afaefe9&cjevent=901b335499a011ee82ffc9610a18b8f9&cjid=100017430. Accessed on 18 March 2024.
41. Gerard O'Dwyer, "Finland, Norway press Russia on suspected GPS jamming during NATO drill," Defence News, (16 November 2018), https://www.defensenews.com/global/europe/2018/11/16/finland-norway-press-russia-on-suspected-gps-jamming-during-nato-drill/. Accessed on 18 March 2024.
42. Dan Goodin, 2020 op. cit.
43. Olivier Moli, "Border Gateway Protocol Hijacking - Examples and Solutions," Anapaya, (10 November 2020), https://www.anapaya.net/blog/border-gateway-protocol-hijacking-examples-and-solutions. Accessed on 18 March 2024.
44. Christian Vasquez and Elias Groll, "Satellite hack on eve of Ukraine war was a coordinated, multi-pronged assault," Cyberscoop, (23 August 2023), https://cyberscoop.com/viasat-ka-sat-hack-black-hat/. Accessed on 18 March 2024.
45. AJ Vicen and Christian Vasquez, "Hackers attack Russian satellite telecom provider, claim affiliation with Wagner Group," Cyberscoop, (29 June 2023), https://cyberscoop.com/russian-satellite-hack-wagner-group/. Accessed on 18 March 2024.

46. Gareth Corfield, "Russian spy agencies targeting Starlink with custom malware, Ukraine warns," The Telegraph, (12 August 2023), https://www.telegraph.co.uk/business/2023/08/12/russian-spy-agencies-targeting-elon-musk-starlink-malware/. Accessed on 18 March 2024.
47. Ruben Santamarta, "SATCOM Terminals: Hacking by Air, Sea, and Land," IOActive Security Services, (2014), https://www.blackhat.com/docs/us-14/materials/us-14-Santamarta-SATCOM-Terminals-Hacking-By-Air-Sea-And-Land-WP.pdf.
48. Department of Commerce, "OIG-14-027M: Expedited Efforts Needed to Remediate High-Risk Vulnerabilities in the Joint Polar Satellite System's Ground System." Office of the Inspector General's Report (Washington DC, 21 September 2014): 2-5.
49. Mary Pat Flaherty, Lisa Rein and Jason Samenow, "Chinese Hack U.S. Weather Systems, Satellite Network," Washington Post, (12 November 2014), http://www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellite-network/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e_story.html. Accessed on 18 March 2024.
50. CSIS, "Significant Cyber Incidents Since 2006," (2023), https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents. Accessed on 18 March 2024.
51. Meg King & Sophie Goguichvili, "Cybersecurity Threats in Space: A Roadmap for Future Policy," Wilson Centre, (08 October 2020), https://www.wilsoncenter.org/blog-post/cybersecurity-threats-space-roadmap-future-policy. Accessed on 18 March 2024.
52. Also called as "quantum-safe" and "post-quantum" (PQ) cryptography. Used to describe cryptographic algorithms that can be run on computers to provide resistant against cryptanalytic attacks from both classical and quantum computers.
53. NSA, "The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ," https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF. Accessed on 18 March 2024.
54. Jeffrey Bardin, "Chapter 89 - Satellite Cyber Attack Search and Destroy," Editor(s): John R. Vacca, Computer and Information Security Handbook (Third Edition), (Morgan Kaufmann, 2013): 1173-1181, https://doi.org/10.1016/B978-0-12-803843-7.00089-2.
55. Johnphill, Obinna, Ali Safaa Sadiq, Feras Al-Obeidat, Haider Al-Khateeb, Mohammed Adam Taheir, Omprakash Kaiwartya, and Mohammed Ali., "Self-Healing in Cyber–Physical Systems Using Machine Learning: A Critical Analysis of Theories and Tools," *Future Internet* 15, no. 7 (2023): 244. https://doi.org/10.3390/fi15070244.
56. UNOOSA, "International Space Law: United Nations Instruments," United Nations Office at Vienna, (2017), https://www.unoosa.org/res/oosadoc/data/documents/2017/stspace/stspace61rev_2_0_html/V1605998-ENGLISH.pdf. Accessed on 18 March 2024.