# Protecting 'Space' from 'Cyber': A Case for Cybersecurity in Space Systems

*Khyati Singh*

Contemporary literature of security heavily revolves around the need to protect 'critical infrastructure'. The US Department of Homeland Security identified 16 areas comprising critical infrastructure. The list includes Chemical, Commercial Facilities, Communication, Critical Manufacturing, Dams, Defence Industrial Base, Emergency Services, Energy, Financial System, Food and Agriculture, Government Facilities, Healthcare, Information Technology, Nuclear Reactors, Materials and Waste, Transportation System, and Water Systems. However, the crucial sectors among these rely on Space systems for functioning. Space Systems comprise assets that are present in Outer Space, suborbital or ground control systems. Sectors like transportation rely on global positioning systems (GPS) satellites, or the defence sector relies on intelligence satellites. While there have been tremendous debates on protecting this critical infrastructure from cyberattacks, relatively less attention has been given to the unfolding domain of cyberattacks in space.

Ms **Khyati Singh** is a Research Associate at the Centre for Air Power Studies, New Delhi.

## THE CASE FOR SPACE

Space assets had a similar trajectory like other technical devices that entered the security domain. They were initially analogue devices and did not have the same cybersecurity concerns as today because they lacked the vulnerabilities that can be exploited. However, with the digitalisation of the systems, and transformation of technology, the space aspect became vulnerable to cybersecurity. They became a point of failure for crucial industries. For instance, to attack the financial system of a state, it is easier for a hacker to target a satellite operator that provides connectivity to sale/credit systems instead of attacking big corporate houses.

A single space system that can be compromised and cause harm to several systems is a desirable target. Additionally, there are numerous attack vectors for every space system. The manufacturer of the space asset equipment, the operator or management firm of the space systems, the producer of test equipment used to test spacecraft components, subsystems, and systems, and the supply chain of hardware and software for the space system are a few examples of attack vectors.[1]

Space assets are unique in that they are highly refined systems that rely on a broad supply chain and whose handlers have complete control over a number of crucial system components. A space mission could be destroyed by a minor error, or satellites could malfunction. A part of the problem has been the lack of regulations and standards for space cybersecurity.

Space systems like satellites are extremely sophisticated devices that consist of radiation hardening, communication, and computing needs. Despite this, there is no governmental organisation that oversees cybersecurity requirements for space assets. In contrast, the Federal Energy Regulatory Commission

[1] William Knowles, et al., "A survey of cybersecurity management in industrial control systems", *International Journal of Critical Infrastructure Protection*, 9 (2015). Accessed on July 28, 2023.

(FERC) regulates other businesses, such as electric networks. Satellite regulation is comparatively weak.[2] The International Telecommunication Union (ITU), an organisation under the United Nations, controls satellite communication frequencies to prevent any interference in communication along with registering the orbits of satellites, but they are not sufficient. There is no overarching governing body that monitors the specific usage of satellites. This vacuum allows for exploitation of satellites to launch cyber operations.[3]

Although the absence of standards for such crucial systems is concerning, hackers are also drawn to these systems due to the complexity of the supply chain needed to build them. For some systems, many manufacturers with different expertise will be required to create multiple technologies, and a system integrator will be needed to combine all the parts into a cohesive whole. There is no single manufacturer that produces all of the specialised components required for space assets. In fact, to reduce costs, NASA and other space technology developers buy parts from recognised suppliers' catalogues all around the world. A hacker has more chances to compromise a satellite with each new vendor.[4] The approval procedure for these vendors is more concerned with physical quality control than it is with cybersecurity vetting criteria. Significant cybersecurity risk is introduced by this lack of understanding. In addition to vendors being weak points in the system supply chain, space asset organisations frequently collaborate with a number of research institutions that could be weak points as well. Collaborations involving several parties

[2] Federal Energy Regulatory Commission, "What FERC Does", 2018, at https://www.ferc.gov/about/ferc-does.asp. Accessed on July 28, 2023.

[3] International Telecommunications Union, "ITU Radio Regulatory Framework for Space Services", 2016, at https://www.itu.int/en/ITU-R/space/snl/Documents/ITU-Space_reg.pd. Accessed on July 28, 2023.

[4] Michael Sampson, "NASA Parts Selection List. NASA Electronic Parts and Packaging Program", 2016, at https://nepp.nasa.gov/npsl/. Accessed on July 28, 2023.

make potential security problems worse. It can be difficult to determine who should be operationally and financially in charge of a system's cybersecurity at different stages of the life cycle of a space asset due to complex supply chains associated to space assets. The intricacy of the creation, administration, use, and ownership of space assets is what makes the space asset supply chain difficult. Space assets are not owned by the same organisations that administer the infrastructure, which raises problems about who would be responsible if they were attacked, unlike most critical infrastructure sectors. India though has started to stress on '*Atmanirbharta*' (self-reliance), it is yet to achieve it in all dimensions. Hence, outsourcing crucial elements is also a loophole that cyber bullies exploit. The development lifetime of a space asset involves a large number of stakeholders, and the asset itself has a long and complicated lifespan. Space missions can endure for decades, and because of this, unpatched legacy systems may increase security risks. Similar to industrial control systems, space assets are made to last, and since they are mission-critical and operate in the field for such extended periods of time, system downtime is not an option. This makes it challenging, if not impossible, to correct any uncovered security issues in space assets.

## LOW-COST SOLUTION WITH HIGH-COST RISK

All these concerns would call for deployment of advanced security protocols but not every satellite has the same level of sophistication. To bring down the cost of satellites, commercial off-the-shelf (COTS) technology is being used. In such low-cost solutions, components like open-source operating systems mounted with security vulnerabilities are used. They altogether bring a new dimension to the security of satellites. The wide availability of COTS allows the hackers to extensively analyse and exploit the vulnerabilities of these devices. Moreover, COTS demands regular upgradation for security along with active maintenance, a concern often overlooked by its users. Since they are generally based on open-source systems, the software can be deliberately planted by the hackers to have a certain edge beforehand. Hence, it is important to introduce low-cost solutions that are equally safe as they are effective.

An estimate in 2017 signalled that there are nearly 700 such CubeSats in orbit, mainly launched by companies to streamline their operations but by this they end up introducing vulnerabilities into their IT systems.[5] The concern runs similar for governments who lease bandwidth on commercial satellites, this paves the way for introducing vulnerabilities into government agencies, military, and IT ecosystems if the linked CubeSat is not completely secured. In addition, these CubeSats can be hacked to attack or collide with a satellite. They have increasingly become a known phenomenon.[6]

## CYBERATTACKS ON SPACE SYSTEMS

Nation states and criminal organisations have already compromised space assets. The most famous assaults were launched on government and commercially supported space assets. These attacks show that even well-funded space projects lack the necessary cybersecurity to protect themselves from cyberattacks.

In order to conceal their cyberespionage activities against nations like the US and the former Eastern Bloc, Turla, a Russian cyberespionage group, gained access to a satellite internet provider, according to Kaspersky Labs. Turla was able to establish a TCP/IP connection from a stolen IP address by utilising a ground

[5] Leonard David, "Sweating the Small Stuff: CubeSats Swarm Earth Orbit", *Scientific American*, 2017, at https://www.scientificamerican.com/article/sweating-the-small-stuff-cubesats-swarm-earth-orbit. Accessed on July 28, 2023.

[6] Hugh G. Lewis, et al., "An assessment of CubeSat collision risk", 2014, at https://eprints.soton.ac.uk/369583/1/IAC1%252CA6%252C4%. Accessed on July 28, 2023.

antenna to find users of satellite internet who were using stolen IP addresses. By using the stolen IP satellite address, Turla can conceal their malicious activities.[7] Because the espionage operation does not necessarily affect the performance of the innocent user, it is impossible to tell if a hacker and a valid user are both using the same IP address at the same time. Attacks of this nature can be used to target remote electric substations and can inject the data on the users' systems that is connected to that IP address.

Another virus launched into space jeopardised GPS systems, which rely on satellites to establish precise locations on Earth. A GPS receiver on Earth may not be able to deliver a reading if noise is introduced into the GPS satellite's receiver spectrum. This method is referred to as 'Jamming'. To prevent US missiles from entering its airspace, Russia has installed GPS jammers on over 250,000 cell towers.[8] While GPS jamming assaults have been utilised in the past and are not necessarily regarded as cyberattacks, GPS spoofing is because the GPS signal is being altered. As the GPS appears to be operating as intended, GPS spoofing is much riskier than GPS jamming.

A GPS satellite can be impersonated in numerous ways. One method involves breaking into the satellite receiver and changing the signal that the satellite outputs. Using a software-defined spoofer or a GPS signal emulator, an adversary can launch a fake data injection assault to spoof the GPS satellite. It is safer to use software-defined spoofers. They operate by hiding a hardly perceptible false signal behind the real signal. The phoney signal's

[7] Stefan Tanase, "Satellite Turla: APT command and control in the sky", Kaspersky, 2015, at https://media.kaspersky.com/pdf/SatTurla_Solution_Paper.pdf. Accessed on July 28, 2023.

[8] Andrew Dalton, "Russia Hopes to Block Cruise Missile Attacks with Cell Towers", *Engadget*, 2016, at https://www.engadget.com/2016/10/17/russia-jamming-cruise-missile-attacks-with-cell-towers/. Accessed on July 29, 2023.

strength gradually rises to the point where the receiver mistakenly believes it to be the real signal.

The first GPS spoofing attempt against more than 20 ships in the Black Sea was reported in 2017 by the US Maritime Administration. One of the impacted vessels' communications with their command centre reveals that during the strike, the GPS position shown on their navigation tool occasionally indicated "lost GPS fixing position".[9] During the attack, the ship's fake location briefly indicated that it was close to the Gelendzhik airport when it was actually 25 nautical miles away. Anecdotal allegations of spoofing are prevalent in Russian waters, claims an organisation, Resilient Navigation and Timing, which keeps track of GPS incidents.[10]

It is commonly believed that Iran launched a different strike of this nature in December 2011 to seize a US drone. Iranians claimed to have perfected a new method of using GPS spoofing to compromise aeroplanes in September 2011. By rerouting the GPS signal's coordinates to cause the drone to land in Iran rather than its base in Afghanistan, they were able to successfully capture an American RQ-170 Sentinel drone.[11] The US military attributed the drone's capture to a malfunction but was unable to explain how the Iranians managed to get hold of the drone intact.

[9] Dana Goward, "Mass GPS Spoofing Attack in Black Sea?", *The Maritime Executive*, 2017, at https://www.maritimeexecutive.com/editorials/mass-gps-spoofing-attack-in-black. Accessed on July 29, 2023.

[10] Lisa Vaas, "Suspected Mass-Spoofing of Ships' GPS in the Black Sea", *Naked Security*, 2017, at https://nakedsecurity.sophos.com/2017/09/26/suspected-mass-spoofing-of-ships-gps-in-the-black-sea. Accessed on July 29, 2023.

[11] Scott Peterson, "Exclusive: Iran Hijacked US Drone, Says Iranian Engineer", *The Christian Science Monitor*, 2011, at https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer. Accessed on July 29, 2023.

## MITIGATION TECHNIQUES FOR CYBERATTACKS

To mitigate cyberattacks of all nature, it is important that space agencies establish stricter access control schemes and policies among all its service providers and engineers. Phishing has been a common practice; NASA introduced a programme called 'Spot the Phishing Email' to cure this.[12] India, too, should have similar programmes in place along with cyberproofing the system at all levels.

India needs to have specialised teams in its Space centres and allied wings that specifically work with the security of their missions and systems. NASA's Jet Propulsion Laboratory (JPL) established the Cyber Defense Engineering and Research Group (CDER). It aims at protecting mission systems which have specific cybersecurity requirements. It is possible to defend these space assets in ways that typical security teams protecting computers and data cannot by creating specialised teams with specialised knowledge in mission systems. To cut expenses and security operations, some of CDER's work focuses on creating tools and processes that function across many mission systems. India can establish Cyber Excellence centres that do not work in isolation, rather have a direct link to space stations and their security requirements.

Furthermore, data encryption during transfer and while in stores is an important safety measure. Encryption allows for private communications that are accessible only to cryptographic key holders. Encryption at this level works as the first line of defence in the face of an attack that is aimed at hijacking the Deep Space Network.[13]

[12] Office of the CIO, *IT Talk*, National Aeronautics and Space Administration (NASA), 2012, at https://www.nasa.gov/pdf/666064main_ITTalk_JUL2012_final.pdf. Accessed on July 29, 2023.

[13] Sharon Gaudin, "NASA installs VPN to protect Deep Space Network", 2016, at https://www.computerworld.com/article/3150973/space-technology/nasa-installs-vpn-to-protect-deep-space-network.html. Accessed on July 29, 2023.

While external security procedures can be put in place, it is crucial to foster a security culture amongst the community. While the systems continue to digitalise and technology advances, the people are not catching to the developments at the same pace as the attackers. For this, a behavioural change is needed. Likewise, working in vacuum approach would not bear good results. Space agencies should actively collaborate with educational centres like IITs to conduct security tests as an educational venture especially for those systems that are working on mission system software.

## CYBERSECURITY PRINCIPLES FOR THE WIN

Different stakeholders and agencies would require a different set of principles to operate safely in cyber ‘space’. There are plenty of best practices and standards available for developers but they may not apply to specific technologies of space systems. To remedy this, it is important that Space asset organisations develop specific standards that are consistent across all the organisations. This should also include vendors that provide for space assets, and there should be explicit testing and demonstrations of these components.

The most crucial criticism that has been mounted against India’s cyber strategy has been its reactive approach. This should be replaced with a more proactive one. The agencies and policymakers should not look forward for an attack to have institutions, laws, and defences in place, rather it should take note of the developments around the world and curate the best policies and practices for its organisations.

While the internal structure improves, the need to upgrade and cyberproof the existing infrastructure is also required. Space systems should be considered an essential critical infrastructure unit, and should be dealt with in the same manner. Moreover, there must be proper channel and responsibility assigned for cyber breach and failure. At present, India has numerous agencies dealing with the same issue but it never reaches a solution, and rather complicates the problem at hand. Therefore, there must be a sole central agency with specific departments demarcated and designed for specific agencies and their cyber needs.

## CONCLUSION

The majority of the critical infrastructure is supported by space assets. The cybersecurity of vital infrastructure is a growing concern for academics, legislators, and engineers, but they neglect to take into account the space assets that support these systems. As technology develops, cybersecurity concerns will only get worse since hackers usually look for the weakest link to break into a target system. Assets in space are currently the weakest link. There are various steps that might be performed to safeguard their systems without regulatory guidance, thus space asset organisations should not wait for legislators to act on this issue.

Protecting Space from cyberattacks is going to be more challenging with the arrival of Artificial Intelligence and its collaboration with cyber, and the possibilities of damage have become endless. Thus, it is the need of the hour to look for solutions at every go and ensure safety measures that are not just physical in nature, but cyber in approach.