CYBER ATTACKS ON SATELLITES: A PARADIGM SHIFT IN ASAT APPLICATION

P A PATIL

The space-faring nations have consistently worked towards exploitation of space technology to acquire an unequivocal advantage in economic growth and national security. The pursuit for eminence in the space sector runs parallel to contesting for space supremacy, fuelling research and development in the fielding of space weapons. Advances in development of space-based weapons get constrained by the technological wherewithal required for launching and managing space assets. Though no space-based weapons have been deployed, space assets are still vulnerable and subjected to a wide variety of attacks. While kinetic energy attacks are limited to military powers with established satellite manufacturing and launch capabilities, the testing and evaluation of Directed Energy Weapons (DEWs) is restricted by the techno-logistic potential of a nation. However, for indulging in space negation efforts, as will be established, access to space is neither a prerequisite, nor mandatory.

Space negation efforts would include physical attacks on ground stations or by exploiting the vulnerabilities in the satellite command, control and communication links. While conventional strikes on the ground segment may not be attempted against a stronger adversary, the more subtle but

Group Captain **P A Patil** is a Senior Fellow at the Centre for Air Power Studies, New Delhi.

Any accidental or deliberate disruption of satellite transmissions can cause catastrophic damage to a nation's economy by affecting the financial institutions, transportation systems, electrical power grids, communication systems and automated services.

equally effective way forward would be sabotaging of satellites' communication links using cybernetic attacks. A satellite in orbit is small but central to the massive ground-based support infrastructure. Any accidental or deliberate disruption of satellite transmissions can cause catastrophic damage to a nation's economy by affecting the financial institutions, transportation systems, electrical power grids, communication systems and automated services. On the military front, it can hamper or result in considerable breakdown of operational capability. Irrespective of the services provided, a breakdown in satellite services directly affects and jeopardises the economy and security of a nation. This growing reliance on satellite services now poses a fundamental threat to nation states as disruption of satellite services and their applications has become feasible by the covert means of cyber attacks.

Satellites being integral to modern warfare are fundamental to the strategic depth of the nation. On the operational front, they comprise a credible force enhancer and form a vital component of force application. Going by the conventional perception and definition of weapon systems, cyber attacks on satellites in a strict sense would be difficult to categorise as Anti-Satellite (ASAT) weapon attacks. While this analogy might have been true in the past, cyber attacks and mitigation techniques are being increasingly utilised in all facets of warfare and are now acknowledged as a new dimension in modern warfare. As modern war-waging equipment relies heavily on information technology for command, control and functionality, cyber warfare now finds itself intricately linked with the operational capabilities of forces fighting in the land, air and sea domains. One may perceive satellites as complex hardwired systems driven by software utilities commanded from the ground to enable precision strikes, improve, and provide for, navigation across the globe, extend communication in otherwise inaccessible terrain and widen the scope of Intelligence, Surveillance, Reconnaissance (ISR) for successful operations. Like all networked infrastructure on the ground and at sea, satellites in orbits and their controlling ground stations are equally vulnerable and susceptible to cyber attacks. The functionality of all space-based assets or objects transiting through outer space rests to a great extent on onboard embedded software (which is subjected to remote command and control) for provision of services and applications. In view of this, and the future war-waging designs eyeing for projection of power towards and from outer space, it seems apt to include cyber attacks on space assets as part of the space weaponisation process.

All satellites are driven by extensive digital controls which are highly vulnerable to interference. The satellite operation rests on the commands relayed from control stations based on the ground, monitoring the satellite response.

CYBER WARFARE AND ITS RELATION WITH SPACE

Prior to establishing the link between cyber warfare and space, it would be prudent to describe what constitutes cyber warfare. Cyber warfare is the unauthorised penetration by, on behalf of, or in support of, a government into another nation's computer or network, or any other activity affecting a computer system, in which the purpose is to add, alter, or falsify data, or cause disruption of, or damage to, a computer, or network device, or the objects that a computer system controls.[1]

When talking of space-based assets, we can say that space and cyber space are closely interlinked and satellites can be viewed as computers placed in orbit with very long and very vulnerable wireless fidelity (wi-fi)-like data links to ground stations and users.[2] All satellites are driven by extensive

[1] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About It* (Harper Collins Publishers), p. 70.

[2] Col M V "Coyote" Smith, "Welcome to the Age of Space and Cyber Warfare", presentation at American Centre for Democracy's symposium on "Energy, Space and Cyber Security-Current and Future Threats," on September 30, 2013, at http://acdemocracy.org/welcome-to-the-age-of-space-and-cyber-warfare/. Accessed on January 13, 2015.

digital controls which are highly vulnerable to interference. The satellite operation rests on the commands relayed from control stations based on the ground, monitoring the satellite response. All satellites use Telemetry, Tracking and Command (TT&C) sub-systems to communicate with ground stations. The TT&C is used to monitor the satellite's health, its overall status and exact location in space. It also accepts the required commands for processing of onboard data and manages the application payloads (imaging, communication, navigation, etc) and, in turn, relays the response to the ground. The TT&C relies extensively on the integrated software which in the modern-day context can be reconfigured as well as updated remotely from the ground. This reliance on software makes the satellites vulnerable to cyber attacks and a number of instances have come to the fore where satellites operations have been interfered with. These occurrences or attempted cyber attacks are not restricted to, or against only, military space assets. Satellites, whether military, civil or commercial, irrespective of their ownership, are susceptible targets for state and non-state actors as well as individuals. The attacks involve effects from temporary irritation to partial or complete breakdown of services. The successful culmination of a cyber attack may involve minimum paraphernalia required, in terms of just a computer and an internet connection. The matter gets complicated as cyber attacks are covert and deceptive in nature. Any cyber attack, whether on a ground system or a space asset would follow similar execution irrespective of the target and would be hard to detect. On detection, ascertaining the time of attack becomes difficult and attributing the attack to any party is extremely challenging as the attacker, by and large, would have covered his tracks.

While interference with satellites, intentional or unintentional, has been common, many instances of hacking of satellites have been reported, with some cases even reporting complete loss of control. As aptly stated by William J. Lynn III, former US deputy secretary of defence, "The willingness of states to interfere with satellites in orbit has serious implications for our national security. Space systems enable our modern way of war. They allow our war-fighters to strike with precision, to navigate with accuracy, to communicate with certainty, and to see the battlefield with clarity. Without them, many of our most important military advantages evaporate."[3]

PRINCIPAL CYBER THREATS TO SATELLITES

Extensive use of satellites in direct support of operations came to the fore with the Gulf Wars and since then there has been an incremental integration of satellite services with the emergence of network-centric warfare amongst the global powers. Moreover, during the Gulf War, instances of blocking satellite services were witnessed and in the aftermath of the war, stray incidences of taking over of the complete controls by unidentified attackers using cyber means have been reported. Cyber attacks are mainly aimed at interfering with, and taking over, the controls of a satellite. While military satellites are obvious targets, commercial satellites also are vulnerable during times of conflict. Cyber attacks on satellites and peripheral infrastructure use the techniques of jamming, evesdropping, hacking and seizing of overall control. The penetration of the cyber and information domains by the hacker community has forced the satellite industry to initiate measures to safeguard satellites and associated sub-systems from cyber threats. While the development of mass-to-target weapons and DEWs continues, new inroads have been made by initiating disruption, degradation or incapacitating a satellite or its services by means of Information Warfare (IW). As new concepts emerge, the developments of IW ASAT capabilities now fall in a very different league of 'silent intrusion systems' and due to the capability of IW in degrading, de-orbiting or making a satellite dysfunctional, the IW attacks can be categorised in the league parallel to kinetic and directed energy weapons. This categorisation of drawing parallels with kinetic weapons and DEWs can be debated, but it must be taken into account that ASAT attacks now ride on the asymmetric applications which no longer demand use of high powered directed energy systems or kinetic kill to impair or damage a satellite. Despite the fact that no satellite has

[3] William J. Lynn III, "A Military Strategy for the New Space Environment," *Washington Quarterly*, 34, no. 3, Summer 2011, pp. 7-16.

been lost or destroyed by cyber means as on date, the occurrence of such an eventuality cannot be ruled out in the future.

Military satellites use hardened protection measures making them difficult to get compromised as compared to commercial satellites that are often dual use in nature, providing support services like communication and reconnaissance. As military or civil satellites come under the category of strategic asset, loss of any satellite or its services is liable to cause economic distress to a nation. Nation states can also resort to obstruction of satellite operations as a coercive measure for political signalling. A cyber attack on a satellite can affect its performance, causing temporary degradation in its services and can extend to cause irreversible permanent damage. These attacks may be blatant or covert in nature. The attacks could be directed at disrupting a particular service and target satellite, irrespective of its orbital altitude. While a number of cyber attacks against non-military satellite services have been reported and documented, a majority of instances of cyber attacks or attempts either go unnoticed or even if noticed, are not made public by the satellite operators for fear of losing their credibility and standing in the international market. On the military front, such attacks would not generally be publicised as the attacker would not be in a position to evaluate the efficacy of his attacks. Only a few cases of cyber attacks and attempts on military satellites have been acknowledged and that too after the required corrective action to mitigate the threat had been put in place.

As will be seen subsequently, most cyber attacks are temporary and reversible in nature. While instances of taking over complete satellite controls have come to the fore, destruction of a satellite by a cyber attack has not been attempted. However, complete takeover of controls may permit the attacker to manoeuvre the satellite, and if need be, the attacker could be in a position to de-orbit the satellite, push it out of orbit into space or manoeuvre it to collide with another space asset.

SATELLITE JAMMING

Satellite jamming is a widespread hacking technique by which the attacker deliberately transmits a signal at the same frequency and with higher power so as to interfere with the legitimate signal between the satellite and the user by means of flooding or overpowering of uplink or downlink transmissions. In fact, jamming a satellite would involve subduing of the actual signal in unwanted noise so that the real signal is no longer legible to the processing circuitry of the receiver system and, thus, cannot reach the user in a comprehensible form. This type of localised jamming would only be of temporary nature and the jamming effects would be negated in time with the removal of the jamming signal. All satellites are installed with a number of transponders which amplify the received signal (uplink signal) and then retransmit it towards the earth at a modified frequency, using frequency converters (downlink signal). Most communication satellites are placed in the geo-synchronous orbit for continuous coverage and use fixed frequencies for uplink and downlink transmissions. A cyber attack could be directed towards the satellite or used to attack the computers and peripheral infrastructure of ground stations. While modern-day military as well as commercial satellites use encoded signals as an anti-jamming technique, a powerful signal at the correct frequency can defeat such protection measures. While many nation states use dedicated military satellites, the dual use commercial satellites are more vulnerable to jamming attacks and can be exploited in crisis situations. There are two types of satellite jamming techniques: orbital jamming and terrestrial jamming.

Orbital Jamming: Here the attacker targets the uplink and overrides the legitimate transmission from the ground terminal to the satellite. Thus, in a real sense, the jamming is directed towards the satellite, preventing the receiver of the satellite from receiving the uplink signal. Further, the efficacy of jamming on a commercial service like communication and television broadcast could be effectively monitored by observing the affected services. This will not be so in the case of a dedicated military satellite as the attacker may not be in a position to process the received signal in the absence of a dedicated configured receiver. As communication and broadcast satellites receive and transmit signals over a wide footprint, it is feasible to carry out cyber attacks on a satellite from any area under its cone of coverage, making it extremely difficult to pinpoint the source of attack. An attacker

Terrestrial jamming is aimed to interfere with the downlink signal of the satellite and enables the attacker to inhibit a useful signal reaching the ground station or receivers, affecting a particular service being provided through the satellite.

jamming the uplink transmission requires the satellite to be visible during the attack. Thus, communication and broadcast satellites would be more vulnerable to such attacks than satellites in Low Earth Orbit (LEO). To target satellites in LEO, the cyber attacks additionally would require tracking equipment as the satellites are moving at higher speeds. Further, the attacker will be forced to plan the time of attack over a short duration in a feasible window of opportunity.

Terrestrial Jamming: Similar to the technique used for orbital jamming, terrestrial jamming is aimed to interfere with the downlink signal of the satellite and enables the attacker to inhibit a useful signal reaching the ground station or receivers, affecting a particular service being provided through the satellite. Unlike the jamming of the uplink, in this, the power requirement is much less, and generally such jammers are positioned in the vicinity of receivers or ground stations. Thus, the source of jamming can be identified and tracked relatively easily. As compared to uplink jammers, downlink jammers are simple and inexpensive. They may be bought off the shelf or easily built by amateurs using instructions available on the internet.

Instances of Satellite Jamming: Satellite jamming has been a common occurrence in the past two decades and has been resorted to by both state and non-state actors, particularly those targeting television broadcasts and communication services for censorship purposes. The cases of jamming date back from the time satellites have been used for television and radio broadcast services. In 1995, the Kurdish satellite channel 'Med TV' was jammed by the Turkish authorities citing that its broadcast supported terrorism and violence. In the present century, we have had instances of countries like Cuba, Iran, Libya and Ethiopia resorting to jamming of satellite communications and television broadcasts originating from Europe and the United States. During the Crimean crisis, Russia had reported that cyber attacks were being originated from western Ukraine to block TV transmissions. In addition to broadcast transmissions, jamming of Global Positioning System (GPS) signals and satellite telephones has now become a common phenomenon worldwide. A comprehensive list of jamming incidents has been compiled by Jason Fritz BS, entitled "Satellite Hacking: A Guide for the Perplexed."[4] These incidents as well as attempts of jamming instances are not only against commercial and civil satellites, but against military satellites as well. Jamming attacks against satellites providing operational support came to the fore in the Gulf Wars and in the Israel-Lebanon War of 2006. As of today, sophisticated technologies for jamming satellite signals are readily available and can be procured 'off the shelf' from the commercial market. The United States has on its inventory a mobile counter-communication system which could be used to selectively and effectively jam satellite communications during a period of conflict, or a period of interest, on a temporary and reversible basis.[5] China has also developed jamming techniques to jam satellite communications.[6]

GPS signals at published frequencies are transmitted from semi-synchronous orbit (~ 20,000 km) in the power range of 50 watts from a satellite. The power received at the ground equipment is not much, thus, making the GPS receivers susceptible to jamming.

GPS Jamming: One of the frequently used jamming attacks is against GPS signals which are critical to operations and navigation. GPS signals at published frequencies are transmitted from semi-synchronous orbit (~ 20,000 km) in the power range of 50 watts from a satellite. The power received at the ground equipment is not much, thus, making the GPS receivers susceptible to jamming. GPS jammers are now widely available –

[4] Jason Fritz BS, "Satellite Hacking: A Guide for the Perplexed", *Culture Mandala: Bulletin of the Centre for East-West Cultural and Economic Studies*, vol. 10, no. 1, December 2012- May 2013, pp.21-50.

[5] Jim Wolf, "US Deploys Space Satellite Jamming System", at http://www.rense.com/general59/jam.htm. Accessed on February 5, 2015.

[6] Brian Bremner, "As China Stalks Satellites, US and Japan Prepare to Defend Them", at http://www.bloomberg.com/bw/articles/2014-07-17/u-dot-s-dot-japan-prepare-to-defend-satellites-from-chinese-attack. Accessed on February 6, 2015.

instructions to build a jammer are available on the internet. Thus, a satellite navigation system which requires investment of billions of dollars can be disrupted with jamming equipment costing only a few dollars. Russia markets jamming equipment of the size of a cigarette packet, which, with a power output of one watt, can deny GPS services in a radius of 80 km.[7]

Space-Based Jamming: Space-based jamming would involve the jammer being placed on a satellite in the vicinity of the target satellite. A jammer placed on a satellite would be effective with much smaller power levels as compared to ground-based jammers. However, pointing the jammer power to the satellite antenna and maintaining the jammer power for a prolonged duration is a difficult proposition. Orbiting the jammer in the same orbit is possible but effective jamming power would be lost. Incidents of space-based jamming have also been reported over contested orbital slots and allocation of frequencies. In 1997, Indonesia used its satellite, Palapa B1, to jam the transponder of the communication satellite APSTAR-1A, leased by the island nation of Tonga from the Hong Kong-based APT Satellite Company over a disputed orbital slot.[8] While many reports termed the incident as intentional jamming, it emerged that the jamming took place due to the two satellites being in near vicinity to each other, owing to disputed orbital slots.[9] Using a satellite platform for jamming equipment does not seem to be a practical proposition as a jamming attack is feasible using ground-based jammers, and any attack planned is bound by the window of opportunity in both time and space.

EAVESDROPPING

Eavesdropping on a satellite would amount to securing unauthorised access to the satellite transmissions without affecting the normal satellite operations and, in a legal sense, would portend stealing of information. This information would be used to decipher the plans of the adversary and could be used effectively

[7] United States Department of Defence, Rumsfeld Space Commission Report, p. 20, Washington, DC.

[8] Fritz BS, n. 4, pp. 21-50.

[9] Jeffrey Lewis, "The Role of Non-State Actors in Outer Space Security", Building the Architecture for Sustainable Space Security Conference Report, March 30-31, 2006, United Nations Institute for Disarmament Research, p.34.

to spoof the transmissions for deceiving the enemy. To avoid eavesdropping attacks, hardened encryption algorithms can be used. However, use of complex encryption standards has its own drawbacks, with escalation in the cost of operations, as well as a drop possible in the overall performance by a margin of 80 percent.[10] Satellite communications without hardened encryption in particular are susceptible to be compromised by off-the-shelf tools and software. One such software called 'SkyGrabber' was sold by a Russian firm, Sky Software, for $26 off-the-shelf and was used by hackers in Iraq and Afghanistan to capture unencrypted video feeds of the Predator Unmanned Aerial Vehicles (UAVs).[11] While the hackers weren't able to interfere in operations, they did use the accessed data to pinpoint areas under military surveillance and the pattern followed by drones for reconnaissance operations for adopting defensive measures.[12] This, in turn, could have helped the insurgents in predicting the position of, and tracking, locating and destroying the Predator drones of the United States during the 2003 invasion of Iraq.[13]

The other type of eavesdropping commonly encountered is the interception of communication of satellite phones and decrypting the messages using commonly available software on the internet. There are more than 100,000 satellite phone (satphone) subscribers worldwide and they are being widely used in disaster relief and military operations which are sensitive in nature.[14] While satellite phones do use encryption algorithms, these encryption algorithms can be broken easily using software tools readily accessible on the internet.[15]

[10] Pierluigi Paganini, "Hacking Satellites… Look up to the Sky", http://resources.infosecinstitute.com/hacking-satellite-look-up-to-the-sky/". Accessed on December 9, 2014.

[11] Pierluigi Paganini, "Satellite Infrastructures: Principal Cyber Threats" at http://www.aofs.org/wp-content/uploads/2013/12/131203-Paganini-Satellite-infrastructures-Principal-cyber-threats_Final.pdf. Accessed on December 3, 2014.

[12] Paganini, n. 10.

[13] Chris Cole, "Rise of the Reapers: A Brief History of Drones", October 6, 2014, at http://dronewars.net/2014/10/06/rise-of-the-reapers-a-brief-history-of-drones/#_ednref22. Accessed on January 20, 2015.

[14] Benedikt Driessen, Ralf Hund, Carsten Willems, Christof Paar, Thorsten Holz, "Don't Trust Satellite Phones: A Security Analysis of Two Satphone Standards", Horst-Goertz Institute for IT Security, Germany at http://gmr.crypto.rub.de/paper/paper-1.pdf. Accessed on January 20, 2015

[15] Ibid.

HIJACKING AND SPOOFING

Hijacking of a satellite involves unauthorised access to the satellite for the purpose of overriding legitimate transmissions with illegitimate transmissions. The attacker's aim is to make use of the available platform to suit his cause by hijacking a particular service or application. While any permanent damage to the satellite and sub-systems is ruled out, the attacker overrides or corrupts the legible signal. A successful hijacking involves eavesdropping and spoofing operations. Spoofing can be perceived as an advanced jamming technique where the jamming signal imitates the characteristics of the actual signal and the content of the jamming signal is replaced with a fake signal for manipulating the contents. Spoofing, thus, would require additional intelligence on the exact characteristics in terms of frequency of transmission and the power with which the signal is expected at the receiver. Signals with gross deviations in the received power levels at the receiver are subjected to be filtered out. A hijacking incident would involve replacement of the original content in a televised or radio broadcast. On the military front, such an attack would be aimed to deceive by planting misleading information and feeds. Hijacking incidents of television and radio broadcast are mainly resorted to as part of psychological warfare and for imposing censorship. For a comprehensive list of occurrences involving hijacking incidents, one may refer to the list of jamming incidents compiled in the work of Jason Fritz.[16]

CONTROL

The attacker in these cases penetrates the Tracking, Telemetry and Control (TT&C) using cyber means and modifies the controlling software to manipulate the services, applications and commands to the satellite. Taking over the function of the satellite by the attacker would entail gaining of complete access to the TT&C link and, thus, enable the attacker to manipulate the controls to manoeuvre or destroy the satellite by de-orbiting it out of its slated orbit. The relatively less serious type of attack is when the control gained is partial, in that the attacker is able to assume unauthorised control of the satellite sub-system. Examples of this type of attack would include

[16] Fritz BS, n. 4, pp. 21-50.

taking over the control of the antenna or shifting the orientation of the satellite, making it unusable to the owner. While manipulation of the signal transmission may not necessarily make the satellite defunct, it can render it useless to the rightful owner for prolonged or indefinite periods. One such incidence came to fore in the year 1998 when the high resolution imager of the US-German ROSAT satellite was destroyed owing to exposure to the sun. Investigations by the National Aeronautics and Space Administration (NASA) revealed that the orientation altered as a consequence of cyber-intrusion at the Goddard Space Flight Centre and the attack allegedly originated from Russia.[17] As of now, while manipulation and taking over of control of satellite services has been witnessed on numerous occasions, there have not been instances of satellite destruction due to hacking. In its report to Congress, the US-China Economic and Security Review Commission (USCC 2011) states that "at least two US government satellites have each experienced at least two separate instances of interference apparently consistent with cyber activities against their command and control systems." The report explicitly brought out the following malicious events experienced by US satellites owing to alleged cyber attacks by Chinese hackers.[18]

- On October 20, 2007, Landsat-7, a US Earth observation satellite jointly managed by NASA and the US Geological Survey, experienced 12 or more minutes of interference. This interference was only discovered following a similar event in July 2008 (see below).
- On June 20, 2008, the Terra EOS (Earth Observation System) M–1, a NASA-managed programme for Earth observation, experienced two or more minutes of interference. The party responsible for this had achieved all the steps required to command the satellite but did not issue the commands.
- On July 23, 2008, the Landsat-7 experienced 12 or more minutes of interference. The party responsible did not achieve all the steps required to command the satellite.

[17] Keith Epstein and Ben Elgin, "Network Security Breaches Plague NASA", at http://www.bloomberg.com/bw/stories/2008-11-19/network-security-breaches-plague-nasa. Accessed on February 2, 2015.

[18] US-China Economic and Security Review Commission Report, November 9, 2011, pp. 215-217.

- On October 22, 2008, the Terra EOS AM–1 experienced nine or more minutes of interference. The party responsible achieved all the steps required to command the satellite but did not issue the commands.

While the hackers were able to gain complete control to command the satellite in the case of the Terra EOS, it is possible that they were assessing the vulnerability of the satellite control system. The likelihood of these attacks originating from an individual hacker could probably be ruled out as no motive was spelled out. That leaves the possibility of the attack being attempted at the behest of government sponsored hackers – a possibility as the attacks were carried out by incorporating measures to obscure the attempts and cover up tracks. Issuance of a command to manipulate the satellite in such a scenario would have amounted to an ASAT attack and thereby subject to international ramifications. This makes it very clear that unless hardened measures and anti-jamming techniques are adopted, the loss of satellite control could allow the attacker to damage or destroy a satellite by steering it out of the slated orbit. Further, the required anti-jamming measures call for specialised hardware and software encryptions which have to be imbedded into the satellite at the design stage itself. Once the satellite is launched, only limited upgrades in software would be feasible. The hacking of controls would make it possible for the attacker to manipulate the services and associated network infrastructure. In the developing network-centric scenario, multiple attacks on a set of satellites could paralyse a nation's network support from space and compromise its operational capability.

Unless hardened measures and anti-jamming techniques are adopted, the loss of satellite control could allow the attacker to damage or destroy a satellite by steering it out of the slated orbit.

CONCLUSION

With cyber attacks, the employment of ASAT technology has not been limited to acts against military satellites alone, nor is it restricted to use by the US, USSR and China. With the advent of information systems across the globe, and growing dependence on satellite services in the commercial and social structures, a cyber attack can take a toll of a nation's economy and break its will to fight a war. Nation states not having the requisite technology and wherewithal for launching of space assets as well as those with not so advanced conventional military power, find themselves alienated from the developments in the field of kinetic and directed energy space weapons. The only option to offset a conventional and technological disadvantage is to adopt an unconventional and asymmetric approach, through the covert means of cyber attacks. Incidents of jamming, hacking and taking over the control of satellites are phenomenal in numbers, and are becoming routine in nature. Many of the cyber attacks on satellites go undetected, and if detected, are not reported. As can be evaluated from the few documented attacks discussed earlier, gaining access to satellite controls would allow an attacker to destroy or damage a satellite, force it to de-orbit, manipulate the transmissions and gain important information on the data collected by the satellite. The technology development in the past had not catered to the new kind of threats as counter-technologies in general never precede new developments. Most nations rely heavily on space-based assets and the vulnerability of these assets necessitates protective measures which at times tend to become aggressive so as to deter the adversary. This would hold in conventional conflicts but may not work against non-state actors engaged in asymmetric attacks. A weaker country with the capability of engaging in cyber attacks can exploit the space dependence of its stronger adversary and create chaos without being traced and detected. Asymmetric warfare of this kind is very much prevalent and is now being actively pursued by both state and non-state actors.

Incidents of jamming, hacking and taking over the control of satellites are phenomenal in numbers, and are becoming routine in nature. Many of the cyber attacks on satellites go undetected, and if detected, are not reported.