CENTRE FOR LAND WARFARE STUDIES

ISSUE BRIEF

No. 287 May 2021

Space and Cyber Warfare: An Umbilical Bond

Lt Gen PR Kumar PVSM, AVSM, VSM (Retd), served in the Indian Army for 39 years. He was the DG Army Aviation, before superannuating from the appointment of Director General of Military Operations (DGMO) in end 2015. His area of interests comprises international & regional geo-political issues and also security & strategic issues.

Key Points

- Niche and disruptive technologies especially in the field of electronic and cyber counter-space capabilities has enabled a wider range of actors, including states and non-state actors to target and disrupt space eco-systems, including both military and civilian satellites.
- While a kinetic space war has not yet started, the non-kinetic space war is already underway, which can even cause a nuclear 'Armageddon'.
- The existing regulatory framework (OST) does not cover the threat to space systems posed by electronic and cyber capabilities— specific and appropriate measures that define norms of behaviour and rules of engagement in these domains, are urgently required before it is too late.

Introduction

During the 70's, many declared 'Space' as the 4th and final frontier of warfare. Today, however, the 5th dimension–a virtual dimension of cyber and electromagnetic spectrum (EMS) is ubiquitous, and we all are involved in an information and cyber war (competition and confrontation) to safeguard our strategic space in a multi-polar and multi-domain war. Space and cyber systems together form a potent mix which is both advantageous to mankind but at the same time can also destroy it—there exists an 'umbilical bond' between them. Outer space is crowded, with more than eighty countries either owning or operating satellites. It is no longer a preserve only of states, but an increasing variety of players including many non-state actors, private sector enterprises and academic institutions, are jostling for access.

This article focusses on non-kinetic military capabilities in space and counter-space that seeks to prevent "an adversary from exploiting space to their advantage".[1] These capabilities enable a space power to maintain "a desired degree of space superiority by the destruction or neutralisation of enemy forces".[2] Kinetic capabilities, which involves physical destruction

of a space object, are difficult to hide from the international community, however it could prove difficult to establish identity of attacker. Electronic and cyber-attacks are much harder to detect because it is difficult to distinguish between a 'non-intentional failure' or a 'malfunction'. More importantly, such capabilities can be developed and deployed or even used without detection—such attacks are already taking place.

Current Space Status

During the Cold War, outer space utilisation was primarily for strategic operations, such as strategic intelligence gathering, early warning of nuclear attack and executing arms control agreements. [3] Space eco-systems have become far more innovative, technologically advanced, congested, and confrontationist, which paradoxically has made access to outer space much cheaper for governmental and private actors alike. Today most states view space from the prism of security, and it plays a pivotal and often decisive role in conventional military operations, and contributes substantially towards tilting the balance of power. Offensive or defensive counter-space operations impacts not only the security sector, but also the social and economic sectors across continents because of large-scale civilian dependency on space-based applications. Being vital to both civilian and military operations, the probability of inadvertent escalation and conflict gets heightened, for instance, a disruption or denial of service (DOS) during period of heightened tensions creates unnecessary panic, even if the incident was a natural incident or due to a mechanical failure.

Space is getting Crowded and Competitive

The brief post-Cold War lull was broken with a sudden surge in interest and emphasis on hard power capabilities in outer space. Since 2007, several States have begun to test anti-satellite (ASAT) capabilities, after an unofficial moratorium that lasted for more than two decades. USA has set up space forces, and many nations including Russia, China, France and even India (Space Command) have plans for a similar force. Space has become another domain where geo-politics and competition are playing out. The trillion-dollar commitment made by President Obama and further enhanced by Trump for modernisation of the entire US nuclear eco-system will mainly impact space infrastructure and communication (ESM), and has already activated an intense nuclear and space race, mainly due to its impact on second strike capabilities of nations.[4] The current India-China military standoff finds a reflection in space domain. [5] Outer space capabilities have become critical to comprehensive national power (CNP) of a Nation.

Expanding Counter Space Capabilities

Niche and disruptive technologies, and capabilities to use offensive and defensive counter-space capabilities has become a strategic imperative for global powers, leading to increasing instances of electronic and cyber warfare. Multipolar (nationalism, nation first, authoritarianism, religious, social and economic asymmetry, global warming), multi-domain characteristics of competition, confrontation and even conflict is providing an impetus for a space arms race as major spacefaring powers seek new military space capabilities. While the norm to 'not test' ASAT weapons is seldom breached, there are indications that other norms, such as non-interference in satellite operations, is weakening. It is a truism that whenever more actors/competitors enter an established field, rules/SOPs are challenged and violated especially when some find it convenient to create/maintain an edge, resulting in acceleration of the race to dominate the electromagnetic and cyber domains.

Types of Counter-Space Capabilities

There are four types of counter-space capabilities vis. kinetic physical, non-kinetic physical, electronic and cyber.[6] Similarly, RAND Corporation in their study have classified 'space-based weapons" into several distinct classes of weapons[7] vis. kinetic-energy weapons against missile targets and against surface targets; space based conventional weapons against surface targets; and directed energy weapons (first three kinetic and last non-kinetic).

- ***Kinetic physical operations and capabilities.*** These cause permanent and irreversible destruction of a satellite or to ground support infrastructure through force of impact by an object or detonation of a warhead. These technologies include direct-ascent ASAT missiles and co-orbital systems. ASATs are typical kinetic weapons.[8]
- ***Co-orbital systems (non-kinetic physical).*** These systems are satellites placed on similar orbits and can be directed to intercept or interfere with other satellites through close orbital rendezvous operations.
- ***Electronic Warfare (EW).*** Electro-magnetic pulses or directed-energy weapons (laser beams or microwave bombardments) interfere with or jam communications to or from satellites, but do not cause any permanent physical damage.
- ***Cyber Warfare Technologies.*** Includes the usage of software and network techniques to compromise, control, interfere or destroy computer systems linked to satellite operations.

Use of electronic and cyber means have become preferred methods of attack especially in grey zone operations as attribution, intention and even the final impact is difficult to discern, thereby, making proportional responses problematic. Such counter-space capabilities can be used to deny, degrade, disrupt, or destroy space systems. Additionally, the requisite technology for electronic and cyber warfare is becoming ubiquitous and diverse, accessible even to non-state actors.[9] Each form of attack and methodology used, operates in different ways, is suitable for different kinds of targets, has different response times, and requires different numbers of weapons (in orbit) to achieve the degree of responsiveness required to reach a particular target when needed.

Nuances of EW Capabilities: Jamming, Spoofing and Other Methodologies

Jamming is an electronic attack that interferes with radio frequency communications by creating noise in the same frequency band and within the field of view of the antenna of the satellite or receiver it is targeting, thus disrupting communications. Jamming is temporary and reversible. A number of different jamming options are available including proactive, function-specific or hybrid-smart jamming to produce the most effective results.[10] Spoofing refers to electronic attack whereby fake signal is produced by the attacker's device. In this case, if the spoofing attack targets the downlink data from a satellite to the ground, then it could end up feeding false or corrupt data into the ground receiver system. Lasers have also been used to blackout reconnaissance satellites and have been found to be quite successful. This is called dazzling, and several States are reported to be investing in this capability.[11] However, the power requirements for significant effects are still a challenge.

Global Positioning System (GPS) satellites have proven to be particularly vulnerable to jamming— by blocking users from acquiring useful and accurate positioning, navigation and timing data from the satellites. But jamming is primarily restricted to civil GPS signals, as military signals are more robust. The global dependence on GPS data, have made GPS systems more vulnerable to be used to cause widespread disruption. Such actions, if not controlled through new rules or norms, could reduce the utility of outer space for providing services. It could also lead to a general dilution of the norms of behaviour in outer space, thereby, increasing security competition that could have a longer-term impact on the peaceful utilisation of space. Today, effective counter-systems are being developed, deployed and activated to 'geo-locate and characterise enemy jammers'— making enemy systems vulnerable to destruction and damage. Enemy electronic systems "could be destroyed, avoided, and negated via adaptive, real-time filtering or otherwise defeated by other electronic protection tactics like increasing transmitter power".[12]

Instances of Use

Though rarely reported, some instances of EW are as follows:

- The US has the technical knowhow to undertake jamming of Global Navigation Satellite System (GNSS) receivers, such as GLONASS or Beidou, in a small restricted area of operation to avoid those systems being used by adversaries.
- In an incident in 2006, China reportedly made efforts to blind US spy satellites flying over Chinese territory using high-powered lasers. US officials claim that China has this capability and has 'exercised it'.[13]
- There are reports of Iran engaging in electronic warfare activities. In a specific case, Iran was accused of jamming certain news broadcasts of BBC's Persian TV in order to prevent Western media from reaching domestic viewers. This jamming was evident during coverage of the 2009 Iranian presidential elections and the 2011 Arab Spring revolts.[14] Recently (2020), Iran has reportedly jammed the GPS Navigation System to divert ships into Iranian territorial waters to bypass detection from the space satellites. Similarly, in the Middle East, Russian forces have jammed the GPS System including those of advanced F-22 and F-35 US fighters near the Iranian airspace.[15]
- In November 2018, Russia was suspected of disrupting GPS signals in northern Norway and Finland as the two nations participated in NATO's Trident Juncture exercise.[16]

Nuances of Cyber Warfare

The accessibility and affordability of cyber warfare systems, has led to its increased presence in space —both in quality and quantity; less advanced states, have also been able to develop space-cyber warfare capabilities. Due to strategic and security considerations, the number of reported cyber interference are few. Many states apart from the big three (US, China and Russia), like Iran and North Korea have demonstrated their capabilities and willingness to carry out cyber-attacks against non-space targets.

In December 2019, NATO Foreign Ministers formally declared space as an 'operational domain,' thereby, extending the alliance's range from land, sea, air and cyberspace to operations in space.[17] As cyber warfare and hybrid threats become the 'weapon of choice' for state and non-state actors, and as global economy and daily life is increasingly becoming dependent on space, therefore, space systems may well become the next front in cyber conflict.[18] While satellites are attractive targets, an attack on them could have serious

unintended consequences and has the potential to lead to a serious conflict. Naturally, commercial space satellites may be more vulnerable compared to military assets. Cyber warfare capabilities will become the biggest challenge in the coming years as it can be developed and deployed much faster than an ASAT and is much cheaper. In 2017, a senior US military official went on record to state that cyber-attacks are the "No 1 counter-space threat". The Director of US National Intelligence, James R. Clapper, made similar observations.[19] Interference with communication satellites could affect the integrity of military operations in addition to creating disruptions with capabilities that are used for airline safety, security and cargo vessels in the high seas.[20]

Cyber warfare is a more direct form of attack than electronic warfare measures as it targets the transmitting radio frequency signals. It warrants more sophisticated capabilities and expertise, but the availability of large number of independent hackers makes it easier for states to outsource operations to mercenary individuals or groups and at the same time maintain deniability. Currently, states can prosecute variety of cyber-attacks, creating tactical and strategic impacts through 'theft, alteration, or denial of information, as well as control or destruction of satellites, their subcomponents, or supporting infrastructure'.[21] With greater number of space programmes using 'more advanced on-board processing, all digital components, software-defined radios, packet based protocols, and cloud enabled high performance computing, the attack surface for cyber-attacks is also increasing".[22]

Amplifications of Cyber Threats to Space Assets

Space systems are usually divided into three technological and operational segments, which are responsible for different functions and are therefore exposed to different cyber threats vis. the ground segment, the space segment, and the link segment.[23]

- ***The ground segment*** consists of all the ground elements of space systems and allows command, control and management of the satellite itself as well as the data arriving from payload and delivered to the users. Due to their role in collecting data, the ground stations and terminals are exposed to the threat of cyber espionage from state and non-state actors. Moreover, the military importance of satellites renders them prime targets for hostile takeover, disruption and shutdown. Most cyber-attacks on the ground segment exploits web vulnerabilities wherein the ground station personnel are 'deceived' into downloading malwares and Trojans, that corrupts the computers. Infiltrating the ground station's network can allow the attackers to access the satellite itself. Hostile access could enable the attacker to execute a Denial of

Service (DoS) attack and may also involve the taking over of Industrial Control Systems (ICS) in order to control the satellite and damage it.

- ***The space segment*** comprises of the satellites. Cyber threats to space segments are usually derived from the vulnerabilities in ground stations, in network components, and in the receivers, that receives the data from the satellite, thus allowing the attacker to infiltrate into the network and still remain undetected. Another threat may involve the introduction of a malware into the satellite's hardware in the supply chain, in order to attack the ground units at a later stage. Consequences of cyber-attacks on satellites could also be aggravated due to the rising connection and use of Internet of Things (IoT) devices. An attack on a communication satellite could cause wide disruptions to communication channels across countries, causing panic and endangering national security.
- ***The link segment*** comprises the electromagnetic spectrum between the satellite and the ground station, as well as between satellites, and also the aspects of jamming, spoofing and dazzling.

Instances of Use

- In 2014, the US National Oceanic and Atmospheric Administration confirmed that one of its satellites had been hacked, however, none of its data was compromised.[24]
- A group of Russian-speaking hackers, with possible links to the Russian government, has been reported to be using malware named 'Turla' for attacking the communication satellites that use unencrypted data links.[25]
- In October 2018, systems of the US National Aeronautics and Space Administration were hacked, and personal data of current and former employees were found to be compromised.[26]

Outer Space Regimes: 1967 Outer Space Treaty[27]

The Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (referred to as Outer Space Treaty, or OST) is the foundational treaty regulating outer space activities.[28] The OST and four subsidiary legal instruments– the Rescue Agreement of 1968, the Space Liability Convention of 1972, the Registration Convention of 1976, and the Moon Agreement of 1979– have largely maintained the sanctity of outer space. Article III of the OST has a direct reference to the Charter of the UN, wherein it states that all States Parties "carry on activities in the exploration and use of outer space, including the moon and other celestial bodies, in

accordance with international law, including the Charter of the United Nations, in the interest of maintaining international peace and security and promoting international cooperation and understanding". Article IX of OST amplifies that any activity in outer space which would cause potentially harmful interference, shall undertake appropriate international consultations before proceeding with any such activity or experiment". Concurrently those states affected have a right to ask for consultation. Although the treaty prohibits the placement of weapons of mass destruction (WMD) in outer space, it does not explicitly ban weapons other than WMDs in outer space. This is increasingly being interpreted to suggest that "non-WMD armaments in space do not violate international law".[29] Another limitation is that, forbidding weapon placement in space does not necessarily forbid use of weapons in space such as ASATs. Therefore, lack of clarity and different interpretations of key concepts like 'peaceful use (can be interpreted as 'non-military' or 'non-aggressive' use)', 'defensive use' and 'space weapon' represents a challenge for the OST. This has many a time led to offensive interpretation, because of fear that other States may have already interpreted and acted accordingly.

EW and Cyber Domains: Complicating Space

Ambiguity becomes acute while dealing with cyber and EW due to difficulty in detection and attribution. States also engage in probing electronic and cyber defences of potential adversaries, but it is unclear if this would constitute an actual attack— a problem that becomes even more serious if non-state actors are employed to front such attacks. The presence of non-state actors further aggravates these issues because it is unclear if an attack on a non-state actor, like a private corporation, can be considered as an attack by one State on the other.

Umbilical Bond: Space and Cyber

- ***Risk of Nuclear Response to Cyber-attacks.*** All nuclear weapon states (NWS) and their allies rely on space-based systems to provide early warning of a nuclear attack. The very existence of space weapons threatens the security structure of any Nation, causing apprehension and increasing risk of nuclear retaliation. While currently this is more applicable to the big three, the same is valid for India-China-Pakistan. Increase in space weapons will trigger development of space-based defences and ASATs. These in turn, would endanger all adversarial nations' early warning (EW) systems, impair intelligence efforts, and increase uncertainty. All NWS would become unsure of their own second strike capabilities including the US, thereby, increasing the risk of an accidental nuclear weapons attack. The perceived vulnerability of EW systems will

force nations to adopt destabilising countermeasures, such as advanced ASAT weapons.[30] Therefore, reliability on space EW systems is vital and must continue. The qualitative and quantitative asymmetry in space, nuclear and cyber capabilities between China and India is so vast that it could lead to 'unintended escalation'.

- ***Cyber Attacks in Space and its Implications.*** A joint study by think tanks from the US and China concluded that cyber-attacks on nuclear systems could trigger conflict, with both the Nations underestimating the risk. This three-year study by the Shanghai Institutes for International Studies (SIIS) and the Carnegie Endowment for International Peace (CEIP) found that the major powers not only lacked an effective mechanism to deal with the risk of an attack on nuclear systems escalating into conflict, but were also not fully aware of the persisting threat.[31] As per Lu Chuanying, the Director of the International Cyberspace Governance Centre at SIIS , the use of cyber operations for intelligence gathering 'are relatively inexpensive, non-lethal, often effective, and not clearly illegal; because they seem, and often are less destructive, more temporary in their effects, and generally less provocative than the use of human spies and certainly kinetic weapons— cyber operations hence poses a lower risk of escalation'. However, Gen Alexander who was the Director of National Security Agency (NSA) and US Cyber Command when questioned during confirmation hearings by senators in the Congressional Committee about cyber-attacks responded that the President would be the judge of what constituted cyber war; if America responded with force (including in cyberspace) it would be in keeping with the rules of war and the "principles of military necessity, discrimination, and proportionality".[32] NWS do not currently have a strong motivation to build a risk-reduction mechanism together, as they are not yet fully aware of the potential risk. Hence, the best solution would be to enter into an agreement (specially NWS) prohibiting cyber-attacks on each other's nuclear systems—but trust deficit between them makes it very hard to reach such a deal.
- ***Response to Cyber Threats*.** In response to the rising cyber threats to space systems, many state agencies, contractors and commercial companies have started developing new technologies, or upgrading existing ones which were not secured by design. In December 2018, Lockheed Martin was awarded a US Air Force contract to modernise GPS ground control systems to support an anti-jamming GPS signal named M-Code, which will allow the Air Force to continue operating the GPS3 constellation with existing ground systems until 2025.[33] In January 2019, NASA announced that it would start testing an open-source Blockchain platform in order to address potential issues of privacy and to prevent spoofing, DoS and other attacks.[34] In March 2019, Lockheed Martin announced that it had developed a new software-

defined satellite architecture called SmartSat as a space segment solution, which will enable more capabilities and greater control of in-orbit satellites for ground operators. It would provide greater precision in diagnosing problems such as cyber incidents, as well as to allow satellites to back each other up. Operators will also be able to update on-board cyber defences to address new threats.[35] While these will mitigate specific cyber threats, a comprehensive problem requires a comprehensive, unified and systematic policy solution to guide the efforts of protecting space assets and services.

Recommendations

Notwithstanding the loopholes and functionality of the OST, it will be difficult to draft a comprehensive Treaty or Agreement, and more importantly bring all the nations together on a common platform, given the current geo-politico-security environment. This dilemma was evident at the UN Group of Governmental Experts (UNGGE) on the Prevention of an Arms Race in Outer Space, which met in Geneva in 2018–19. The UNGGE's inability to reach a consensus and produce an outcome report in its final session provides evidence of the difficulties in space governance and the lack of consensus among the major powers on defining the vital space security concepts—what a space weapon is? what constitutes an armed attack in outer space? and the application of the right to self-defence. Two opposing perspectives prevails on global governance in outer space— first, the belief that legal measures are necessary to resolve the problems being faced by the current space regime, and the second, that given the contemporary political climate, traditional transparency and confidence building measures (TCBMs) or norms are more practical goal. A better approach could be something in between.[36] This could take the form of a legally binding TCBM that encompasses new outer space codes of conduct. While TCBMs are traditionally construed as political measures rather than treaties, legally binding TCBMs could be a useful middle ground. It is pertinent to mention that India which has emerged as a reckonable and technologically capable space nation, can make a difference with its considerable geo-political stature and soft power capabilities, and can be the driver to expedite the dialogue for a modern holistic space regime. Some major recommendations are as follows:

- The UN Disarmament Commission (UNODA) which is the multilateral body in Geneva responsible for international arms control negotiations, including for outer space should get revitalised. If a workable outer space policy is not instituted expeditiously, then countries will be forced to rely on deterrence to protect their assets in outer space. This approach would be inherently destabilising and would

have a cascading effect— if one country relies on deterrence, others will be forced to follow, making further negotiations difficult.

- The OST has served as a useful instrument in ensuring safe and secure access to outer space, however, the development of counter-space capabilities including EW and cyber warfare measures is a major threat that needs to be dealt with more holistically in a fresh/reviewed OST. The revised OST must include a prohibition on all weapons in space, both offensive and defensive, as they are hard to distinguish.
- Definition and interpretations of terms such as 'space weapon', 'weaponisation of space' and 'peaceful uses of space' needs to be clearer and more precise if the challenges of counter-space technologies, especially electronic and cyber warfare technologies, are to be dealt with in an effective manner. 'Weapons' would have to be defined for the purposes of this treaty which distinguishes between space objects with a peaceful purpose and items that are not relevant to the objective of preventing space weaponisation.
- While charting the new OST, the process needs to be more inclusive. An inclusive process over drafting a treaty or a TCBM, gives states' a sense of ownership, brings stakeholders together, ensures wider acceptability, increased legitimacy and thus compliance.
- Concurrently, multi-lateral and bilateral TCBMs should be encouraged and forged, leading slowly to global acceptance of space norms.
- Status of non-state actors, needs to be clearly studied. UN Security Council resolution 1540 provides a potential solution because it mandates each State to control the actions of citizens and individuals within its borders (including into outer space).[37]

Conclusion

Events in this century has clearly demonstrated, that if dangerous weapons and technologies (vis. NBCW) are to be controlled for the safety and security of all, then it must be done early, before the systems become entrenched. Prevention of weaponisation of space is pivotal to world stability; deployment of such weapons even by a single nation will provoke counter-measures—active, passive and reactive. Treaties like the Non-proliferation Treaty (NPT) and even the OST have worked to a large extent, but needs to be reviewed and refreshed regularly as per the prevailing geo-political situation. It is absolutely clear that a 'workable and durable' Space Treaty needs political will of all nations and statesmanship of all spacefaring nations. The repercussions can be devastating if countries no longer consider

outer space as global commons and make it free for all. The World led by the big three supported by India better act now before it is too late.

End Notes

[1] JB Sheldon, "Threats to Security in Space from Counter-Space Technologies", ASEAN Regional Space Security Workshop, *Hoi An, Vietnam*, 06–07 December 2012. Accessible at http://aseanregionalforum.asean.org/files/Archive/20th/ARF%20Workshop%20on%20Space%20Security,%20Hoi%20An,%206-7December2012/Annex%205%20- %20Spa ce%20Security.pdf. Accessed on 02 April 2021.

[2] Air Force Doctrine Document 1, *Air Force Basic Doctrine*, September 1997, p.47. Accessible at https://apps.dtic.mil/dtic/tr/fulltext/u2/a341711.pdf. Accessed on 02 April 2021.

[3] B Weeden and V Samson(eds), "Global Counterspace Capabilities: An Open Source Assessment", *Secure World Foundation*, April 2018. Accessible at https://swfound.org/media/206118/swf_global_counterspace_april2018.pdf. Accessed on 04 April 2021.

[4] Philip Ewing, "Obama's Nuclear Paradox: Pushing for Cuts, and Agreeing for Upgrades", *NPR*, 25 May 2016. Accessible at https://www.npr.org/sections/parallels/2016/05/25/479498018/obamas-nuclear-paradox-pushing-for-cuts-agreeing-to-upgrades. Accessed on 04 April 2021.

[5] India focuses more on its space race with China than China does, since China sees itself in competition with the United States. But there are elements of mutual competition such as undertaking Moon and Mars missions.

[6] T Harrison, K Johnson and TG Roberts, "Space Threat Assessment 2018", *Center for International and Strategic Studies*, April 2018. Accessible at https://csisprod.s3.amazonaws.com/s3fs/public/publication/180823_Harrison_SpaceThreat_Assessment_FULL_WEB.pdf. Accessed on 04 April 2021.

[7] Bob Preston, Dana J Johnson, Sean JA Edwards, Michael Miller, Calvin Shipbaugh, "Space Weapons Earth Wars", *Project Air Force*, (RAND CORPORATION, 2002) Accessible at https://www.rand.org/content/dam/rand/pubs/monograph_reports/2011/RAND_MR1209.pdf.Accessed on 06 April 2021.

[8] BS Kuplic, "The Weaponization of Outer Space: Preventing an Extra-terrestrial Arms Race", *North Carolina Journal of International Law and Commercial Regulation*, vol. 39, no. 4, 2014. Accessible at https://scholarship.law.unc.edu/cgi/viewcontent.cgi?referer=https://www.google.co.in/&httpsredir=1&article=2011&context=ncilj. Accessed on 06 April 2021.

[9] N.1

[10] K Grover, A Lim, and Q Yang, "Jamming and Anti-Jamming Techniques in Wireless Networks: A Survey", *International Journal of Ad Hoc and Ubiquitous Computing*, vol.17, no.4. Accessible at http://www.cs.montana.edu/yang/ pa per/j amming.pdf. Accessed on 06 April 2021.

[11] B Sutherland (ed), "Militarising Space", *Modern Warfare, Intelligence and Deterrence:The Technologies That Are Transforming Them*, 2014, pp. 142–143; PC Saunders and CD Lutes, "China's ASAT Test Motivations and Implications", *National Defense University*, *Institute for National Strategic Studies*, Washington DC, 2007. Accessed on 10 April 2021.

[12] L Bonner, "Defending Our Satellites: The Need for Electronic Warfare Education and Training", *Air & Space Power Journal*, November–December 2015. Accessible at

https://www.airuniversity.af.mil/Portals/10/ASPJ/journals/Volume-29_Issue- 6/SEW-Bonner.pdf. Accessed on 10 April 2021.

[13] F Harris, "Beijing Secretly Fires Lasers to Disable US Satellites", *The Telegraph*, 26 September 2006. Accessible at https://www.telegraph.co.uk/news/worldnews/1529864/Beijing-secretly-fires-lasers-to-disable-US-satellites.html. Accessed on 11 April 2021.

[14] "BBC Fears Iranian Cyber-Attack over its Persian TV Service", *The Guardian*, 14 March 2012. Accessible at http://www.theguardian.com/media/2012/mar/14/bbc-fears-iran-cyber-attack-persian; P Horrocks, and "Stop Blocking Now", *BBC News*, 14 June 2009. Accessible at http://www.bbc.co.uk/blogs/theeditors/2009/06/stop_the_blocking_now.html. Accessed on 11 April 2021.

[15] Neeraj Aarora, "Cyber Warfare will Dominate Space & Physical War" 2020, *Cris*, 30 June 2020. Accessible at https://cyberpandit.org/?article_post=cyber-warfare-will-dominate-space-physical-war. Accessed on 18 April 2021.

[16] Woody C, "Finland and Norway are telling airline pilots to be ready to fly without GPS, and some think Russia is up to something", Business Insider. Accessible at https://www.businessinsider.com/finland-norway-tell-pilots-to-fly-without-gps-and-some-blame-russia-2018-11, 9 Nov. 2018. Accessed 18 April 2021.

[17] 'Foreign Ministers take decisions to adapt NATO, recognize space as an operational domain', *NATO News*, 20 November 2019.Accessible at https://www.nato.int/cps/en/natohq/news_171028.htm. Accessed on 18 April 2021.

[18] Ms Gil Baram and Mr Omree Wechsler, "Cyber Threats to Space Systems: Current Risks and the Role of NATO",*Joint Air Power Competence Centre*, 2020. Accessible at https://www.japcc.org/cyber-threats-to-space-systems/. Accessed on 18 April 2021.

[19] K.Pollpeter, "Testimony Before the US-China Economic and Security Review Commission: Hearing on China's Advanced Weapons", CNA, February2017. Accessible at https://www.cna.org/CNA_files/PDF/CPP-2017-U-014906-Final.pdf; https://www.dni.gov/index.php/newsroom/congressional-testimonies/item/1845-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community and https://www.dni.gov/files/documents/Newsroom/Testimonies /2018-ATA---Unclassified-SSCI.pdf. Also see JP Clapper, statement before the US Senate Select Committee on Intelligence, "World-wide Threat Assessment of the US Intelligence Community, Senate Select Committee on Intelligence", 09 February 2016. Accessible at https://www.dni.gov/files/documents/SSCI_Unclassified_2016_ATA_SFR%20_FINAL.pdf.

[20] Andrea Gini, "Cyber Crime from Cyber Space to Outer Space", *Space Safety Magazine*, 14 February 2014. Accessible at http://www.spacesafetymagazine.com/aerospace-engineering/cyber-security/cyber-crime-cyber-space-outer-space/ and read T Harrison, K Johnson and TG Roberts, Space Threat Assessment 2018, Center for International and Strategic Studies, April 2018, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180823_Harrison_Space Threat_Assessment_FULL_WEB.pdf. Also see R Santamarta, "A Wake-up Call for SATCOM Security", *Technical White Paper*, IO Active, 2014, available at https://ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf, accessed on 19 April 2021.

[21] B Weeden and V Samson (eds), "Global Counterspace Capabilities: An Open Source Assessment", *Secure World Foundation*, April 2018. Available at https://swfound.org/media/206118/swf_global_counterspace_april2018.pdf. Accessed on 20 April 2021.

[22] Andrea Gini, "Cyber Crime from Cyber Space to Outer Space", *Space Safety Magazine*, 14 February 2014. Accessible at http://www.spacesafetymagazine.com/aerospace-engineering/cyber-security/cyber-crime-cyber-space-outer-space/. Accessed on 20 April 2021.

[23] Referred to Wikipedia and Encyclopaedia Britannica, and also N.18. Accessed on 20 April 2021.

[24] "Chinese Military Suspected in Hacker Attacks on US Satellites", *Bloomberg*, 27 October 2011. Available at https://www.bloomberg.com/news/articles/2011-10-27/chinese-military-suspected-in-hacker-attacks-on-u-s-

satellites; "China Denies It Is Behind Hacking of US Satellites", *Reuters*, 31 October 2011, available at https://www.reuters.com/article/us-china-us-hacking-idUSTRE79U1YI20111031; L Johnson, *"Sky Alert: When Satellites Fail*", 2013,p 37; MP Flaherty, J Samenow, and L Rein, "Chinese Hack US Weather Systems, Satellite Network", *Washington Post*, 12 November 2014. Available at http://www.washingtonpost.com/local/chinese-hack-us- weather-systems_satellitenetwork/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e_story.html. Accessed on 21 April 2021.

[25] AL Johnson "Turla: Spying Tool Targets Governments and Diplomats", *Symantec Security Response*, 7 August 2014. Accessible at https://www.symantec.com/connect/blogs/turla-spying-tool-targets-governments-and-diplomats; S Khandelwal, "Russian Hackers Hijack Satellite to Steal Data from Thousands of Hacked Computers", *The Hacker News*, 10 September 2015. Accessible at https://thehackernews.com/2015/09/hacking-satellite.html. Accessed on 21 April 2021.

[26] J Bachman, "NASA Says Hackers Stole Employee Information", *Bloomberg News*, 19 December 2018. Accessible at https://www.bloomberg.com/news/articles/2018-12-19/nasa-says-hackers-stole-employee-information; M Peterson, "China Charged with Hacking NASA,45+US Tech Firms and Govt Agencies", *iDrop News*, 21 December 2018. Accessible at https ://www.i dropnews.com/news/fast-tech/china-charged-with-hacking-nasa-45-u-s-tech-firms-and-govt-agencies/90222/. Accessed on 21 April 2021.

[27] Paraphrased and content taken the Treaty itself (see Note 28) and Rajeshwari Pillai Rajagopalan, "The Outer Space Treaty: Overcoming Space Security Governance Challenges", *ORF Commentaries*, 23 February 2021. Accessible at https://www.orfonline.org/research/the-outer-space-treaty/. Accessed on 28 April 2021.

[28] "Treaty on Principles Governing the Activity of States in the Exploration and Use of Outer Space, including the Moon and other Celestial Bodies" by *UN Office for Outer Space Affairs*, 2021. Accessible at https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html. Accessed on 28 April 2021.

[29] BS Kuplic, "The Weaponization of Outer Space: Preventing an Extra-terrestrial Arms Race", *North Carolina Journal of International Law and Commercial Regulation*, vol. 39, no. 4, 2014. Accessible at https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=2011&context=ncilj&httpsredir=1&referer=. Accessed on 30 April 2021.

[30] Thomas Graham Jr, "Space Weapons and the Risk of Accidental Nuclear War", *Arms Control Association*, April 21. Accessible at https://www.armscontrol.org/act/2005-12/features/space-weapons-risk-accidental-nuclear-war. Accessed on 30 April 2021.

[31] Rachel Zhang, "US-China tensions raise risk of nuclear reaction to cyberattacks", *South China Morning Post (SCMP)*, 17 April 2021. Accessible at https://www.scmp.com/news/china/diplomacy/article/3129764/us-china-tensions-raise-risk-nuclear-reaction-cyberattacks. Accessed on 30 April 2021.

[32] Hearings before the Committee on Armed Forces United States Senate One Hundred Eleventh Congress Second Session, 15 April 2010. Accessible at www.fas.org. Accessed on 30 April 2021.

[33] S Erwin "Air Force to upgrade existing GPS ground control system while next-generation OCX lags". *SpaceNews*, 09 January 2019. Accessible at https://spacenews.com/air-force-to-upgrade-existing-gps-ground-control-system-while-next-generation-ocx-lags/. Accessed 30 April 2021.

[34] N Kaur "NASA adopts Blockchain to battle aerospace cyber-attacks", *CryptX*. Accessible at https://www.express.co.uk/news/science/1073236/nasa-bitcoin-blockchain-crypto-cyber-attacks. Accessed on 30 April 2021; Tom Fish, "NASA embraces bitcoin BLOCKCHAIN tech to battle aerospace cyber-attacks". Express,

16 January 2019. Accessible at https://www.express.co.uk/news/science/1073236/nasa-bitcoin-blockchain-crypto-cyber-attacks, 16 Jan. 2019. Accessed 30 April 2021.

[35] J Hill, "Lockheed Martin Accelerates Transition to Software-Defined Space", *Via Satellite*, 21 March 2019. Accessible at https://www.satellitetoday.com/innovation/2019/03/21/lockheed-martin-accelerates-transition-to-software-defined-space/. Accessed 30 April 2021.

[36] Rajeswari Pillai Rajagopalan, "The Outer Space Treaty: Overcoming Space Security Governance Challenge", Council on Foreign Relations (CFR), 23 February 2021. Accessible at https://www.cfr.org/report/outer-space-treaty. Accessed on 30 April 2021.

[37] "UN Security Council Resolution 1540", *UN Office for Disarmament Affairs*, 2004. Accessible at https://www.un.org/disarmament/wmd/sc1540/. Accessed on 30 April 2021.

CENTRE FOR LAND WARFARE STUDIES (CLAWS)
RPSO Complex, Parade Road, Delhi Cantt, New Delhi 110010
Tel.: +91-11-25691308, Fax: +91-11-25692347, CLAWS Army No. 33098; Email: landwarfare@gmail.com
Website: www.claws.in