



Centre for Joint Warfare Studies

Room No 301, B-2 Wing, 3rd Floor, Pt Deendayal Antyodaya Bhawan
CGO Complex, Lodhi Road, New Delhi - 110003 (INDIA)

Telephone Nos : 011-24364881, 24366485, **Fax** : 011-24366484

Website : www.cenjows.in, **e-mail** : cenjows@cenjows.in
cenjows@yahoo.com

*Copyright (C) 2021, Centre for Joint Warfare Studies (CENJOWS),
New Delhi
Price in India : ₹250 /-*

All rights reserved

No part of this book may be reproduced, stored in a retrieval system, transmitted or utilised in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the copyright owner. Application for such permission should be addressed to the publisher.

The views expressed in the book are of the author and not necessarily those of the Centre for Joint Warfare Studies/publishers.

Printed in India

Cover Page Image Credit – Image available online & accessed at
<https://dsiac.org/technical-inquiries/notable/technologies-and-strategies-to-protect-satellites-from-cyber-and-electronic-warfare/>

Printed by

Xtreme Office Aids Pvt. Ltd.

Basement Bhanot Building (Below Syndicate Bank)

Nangal Raya Commercial Complex, N.D-110046

Ph.: +91-7982084106

E-mail: xtremeofficeaids@gmail.com

Website: www.xtremeonline.co.in

Space Based Electronic Warfare A Strategic Force Multiplier for India

Lieutenant Colonel Vivek Gopal



Figure 1- Satellite Launch by ISRO [\[1\]](#)

ABSTRACT

The modern challenges of dealing with the high-end capabilities of peer and near-peer adversaries, especially in confrontations requiring operations in Anti-Access/Area Denial (A2/AD) environments, have

brought EW back to the forefront. This means that nations must re-invest in modern EW capabilities, and build enough capacity in these capabilities to compete with peer competitors. India needs to rewrite its EW Doctrine under the newly defined paradigm of Space-based EW. Space with its potential for militarization and with EW in particular needs our immediate attention and aggressive pursuing. Benefits accrued from a COMINT/ ELINT payload in LEO/ MEO has benefits far more enriching than a conventional land-based EW system. This brief intends to address the steps that India needs to take to establish a National Space Operations Strategy leading onto a central apex organization to control and coordinate the militarization of space. While suggesting the roadmap in terms of realizable aims and action points, a global landscape in terms of Space based electronic warfare is also mentioned to put things into a better perspective.

Index Terms - Space, EW, LEO, MEO, COMINT, ELINT, RPO, Defence Space Agency, CASC, PLASSF, KRET

I. Introduction

India is graduating towards a joint theaterized concept of operations which requires the integrated forces (battle groups) to be geared for multi domain operations (MDOs) based on an evolving and dynamic battlefield. Spectrum has become heavily contested and hostilities will always see forces operating in a degraded Electronic Warfare (EW) environment in the future. Ground based EW systems, although necessary and potent suffer from the drawbacks of lack of persistence targeting, limited coverage of the areas of interest and the fingerprint left behind due to emissions (if active). Space EW steps in to augment the ground-based systems by means of overcoming the drawbacks of ground based ELINT systems with the main advantage of persistent targeting and covering a very large footprint with a variety of payloads. India needs to step up

to the challenge by means of devising a ***National Space Operations Strategy*** which will address the issues by means of cross-pollination of ideas and technologies across various domains and work alongside the Defence Space Agency to implement and operationalize the concepts.

Future military operations will be powered by modern, networked C4I systems which are distributable, survivable, secure, resilient and tailorable enabling a more lethal force. This also presents a larger attack surface for EW operations. One cannot expect the future wars to be won using legacy technologies. Spectrum is the new manoeuvre space and has to be safeguarded to ensure furtherance of own operations tactically and strategically.

II. Perspective of Space Operations in India

India's entry into the space age was a consequence of the big commitment to 'Big Science' during the post-independence period under the vision of Nehru. [2] ISRO, the Indian Space Research Organization has been associated with the Indian space program right since inception in 1969 and has focused on the 'soft diplomacy' route with majority projects aimed at constructive civilian use. Courtesy the initiatives by this organization, among the spacefaring nations of the world, India can safely be stratified as a second-generation nation alongside China, Japan, Germany, France and Brazil. Countries such as United States and Russia with their industrial complexes have continued to dominate the space domain situating themselves in the top rung. Australia, New Zealand and UAE are also tailing behind and are the third-generation spacefaring nations. The year 2022 represents a significant milestone for India's space industry as it heralds the fifth decade since the establishment of the Department of Space (DoS). ISRO has led the space related activities from the front and has had several remarkable achievements, including successful space missions and development of technologies to foster India's self-reliance and progress. [3][4]

Technocrats (read NITI Aayog) in the government realized that the growth in the domain of space is directly linked to the growth of the country's economy. To that extent, the Make in India initiative has a strong component of 100% foreign direct investment for satellite construction and operations under the aegis of the Department of Space (DoS) which is the main policy making body. Space industry, with the entry of private players and advances made by various countries is no longer a preserve of a few, leading to democratization of the entire process.

There is an inescapable requirement to engage in cross-domain activities with regards to operations and it is the domain of space which can result in asymmetric advantages against any adversary. Cross-domain synergy has been described in the Joint Operational Access Concept or JOACⁱ as *"The complementary vice merely additive employment of capabilities in different domains such that each enhances the effectiveness and compensates for the vulnerabilities of the others—to establish superiority in some combination of domains that will provide the freedom of action required by the mission."* [5] Among the various domains, space, with its advantages presents itself in the forefront of such fused activities; hence its importance.

"Currently, India's space economy constitutes almost two percent of the global space economy, which is estimated to be worth 423 billion USD." [6] A presentation by Indian delegation to 58th session of STSC - UNCOPUOS Vienna, Austria April 20, 2021[7] brought out the six decades' worth of contributions made in the space domain and the milestones reached in the space programme. To cover a few of these milestones, there were a total of 80 launch vehicle missions, 111 satellites placed in orbit (53 belonging to national requirements) and 342 satellites launched from 34 countries.

ⁱ The Joint Operational Access Concept (JOAC) describes in broad terms the vision for how joint forces will operate in response to emerging anti-access and area-denial (A2AD) security challenges. Version 1.0 of the document was released on 17 January 2012.

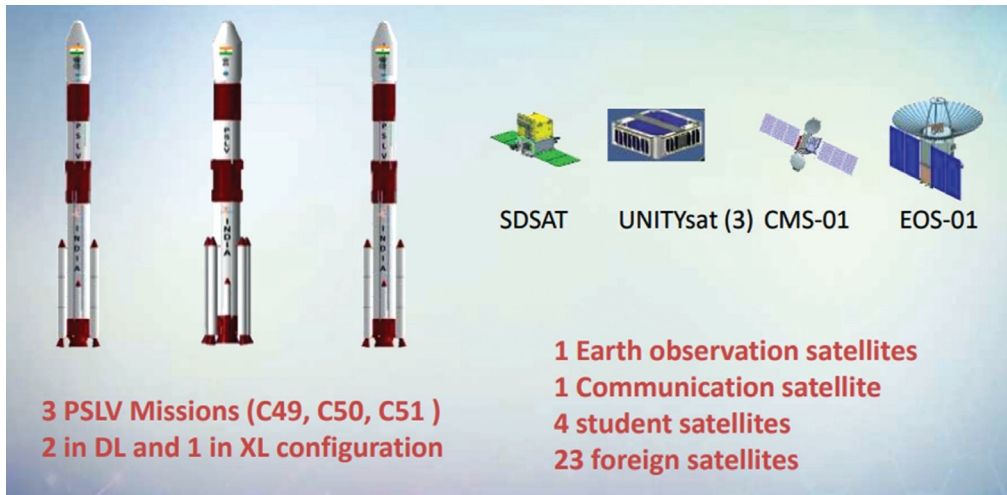


Figure 2- *Missions Accomplished (March 2020 – 21)* [7]

It is evident that the space programme for India is mainly driven by the civil use-cases. Despite the recent segregation of the military programmes under the aegis of the Defence Space Agency, no major endeavour is known towards space-based EW except for ISR capabilities in terms of the CARTOSAT series of satellites.

Space which was earlier a niche domain has now taken the shape of a disruptive arena where safeguarding interests have become paramount. Deterrence in space can only be achieved if one has an aggressively motivated offensive space strategy. While the launch of ICBMs or SLVs can always be assigned motives of tacitly exhibiting aggression, EW in space is one domain where Electronic Support (ES) measures can provide the offensive capability in today's 'information-ised' world. India with considerable space assets has no choice but to protect them by means of developing capability to take punitive action against such misadventures & impose a heavy cost penalty. While the focus should be on dual-use technology, India should always be prepared to tweak the technology for an offensive-defence role when warranted.

This brief aims to bring into perspective the need for space-based EW measured against the global landscape and advances made by the leading spacefaring nations (major focus on USA, Russia, China). To take it further, the paper also presents the way forward to establish a National Space Operations Strategy by focusing on the key areas where impetus is mandatory.

III. Need for Space Based Electronic Warfare

The world's leading military powers are placing increased importance on advancements in technologies and communications, such as artificial intelligence, cyber capabilities, 5G networks, and the Internet of things. EW as a domain too has garnered impetus due to the interplay of all such evolving technologies and space-based EW has reached disruptive significance poised to change the future landscape of military conflict. MDOs will result in parallel engagements on land, sea, air, cyber and space domains. The debate between the semantics involved in Weaponization versus Militarization is historical since the launch of Sputnik by erstwhile USSR. However, EW as a domain in space occupies a place in both the aspects owing its spread in passive as well as active means to achieve the intended aim by definition. How EW is used in the domain of space, can have effects, on the deterrence & escalation dynamics alike.

Modern day EW can be traced back to *Circa* 1904-05 with the Russo-Japanese War. However, if taken in the Indian context, we can go as far back as the *Mahabharata*. To kill *Dronacharya* would have been impossible and hence the deception tactics (rumour/ false propaganda in today's parlance or manipulation of information as part of EW tactics) of spreading the news of the death of *Ashwathama* (an elephant who shared the name of *Dronacharya's* son) exposed his vulnerability had resulted in *Dronacharya's* death. One century later,

EW has resurfaced as the prime contender in today's operations. The contested space domain & ever shrinking EM spectrum has exposed a wider attack surface for EA scenarios. Space as the latest dimension added to warfare has been invigorated with Revolution in Military Affairs (RMA) leading to a Revolution in Space Affairs. EW as a domain, with the advances in technology has transcended into space with countries vying to monitor, control & seize every initiative to achieve ascendancy over the adversaries. A good analysis of how space is helping EW for ground forces has also been done by Mark Pomerleau [8].

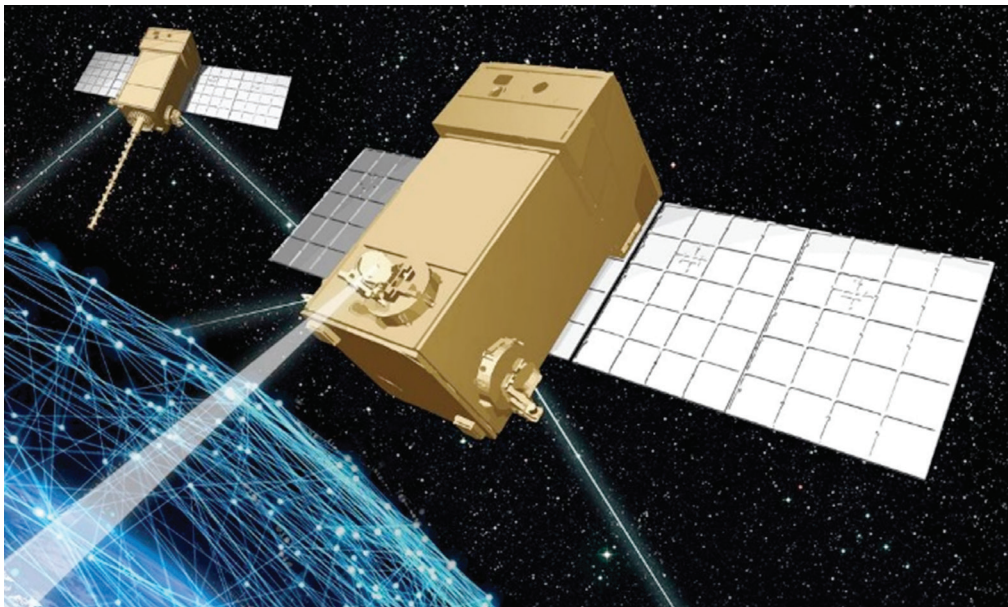


Figure 3- Space-based Sensors for EW [8]

ⁱⁱ Space can be thought to have been Militarized right since the Sputnik era and the launch of the communication satellite. Space weaponization is generally understood to refer to the placement in orbit of space-based devices that have a destructive capacity.

EM spectrum is the new manoeuvre space & freedom of action in this domain while denying the same to the adversary can tilt the balance in favour of the technologically advanced force. Similarly, space EW will ensure the safeguarding of one's space assets which are of prime (national) importance and also portray a nation's might (power projection) in the geo-strategic environment. The need for Space based assets is also greatly influenced by the techno-geo-strategy. Speaking of the theory of offensive realism (propagated by Mearsheimer), China has openly displayed its intent to capitalize on the space domain trying to surpass giants such as USA & Russia. The geopolitical and strategic imperatives to counter the encirclement tactics of China is motive enough to invest time and energy towards developing space assets thereby countering the non-contact warfare approach advocated by the PRC. With Chinese initiatives such as the Beidou constellation (ground station at Ngari in Tibet being the closest to India) and ASAT test in 2007, India needs to adapt its modus operandi to keep pace as well as counter the rise of the dragon as an immediate threat.

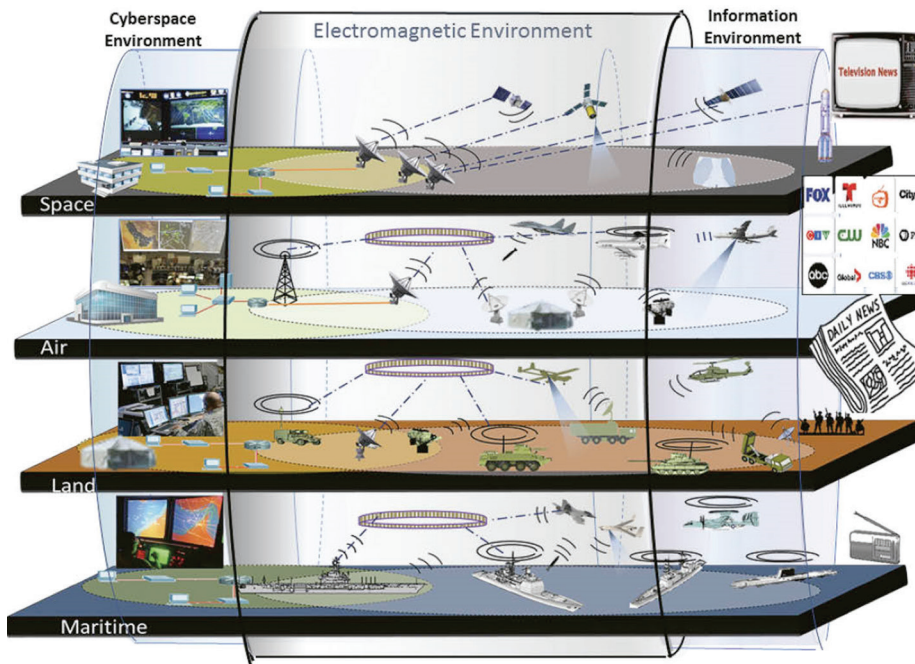


Figure 4- **Contested EM Environment** [9]

Space domination can be graded as one of the pertinent factors in support of foreign policy and national interests, thereby contributing to the overall comprehensive national power. Pakistan's space capability is following the *Circa 2047* vision with an overshadow of 'assistance' by its all-weather ally China [10].

With a growing dependence on space-based operations & proliferation of space-based assets, there is a need to address the challenges being faced with respect to the security of these assets in various orbits. A study [11] by Centre for Strategic and International Studies (CSIS) shows how the space weapons can be categorized viz., Space to Earth, Space to Space & Earth to Space. Drawing a parallel for EW in space, as also shown in the same study, jammers & directed energy weapons (DEW) are capable of effects in all the three categoriesⁱⁱⁱ. Unfortunately, what has been covered are the attack capabilities of EW, while the passive & more potent features of ISR, direction finding & persistent targeting has not been elaborated as part of weaponization. Naysayers & experts may beg to differ on this concept which might seem at a cross with the generic definitions of ES, Electronic Attack (EA) &

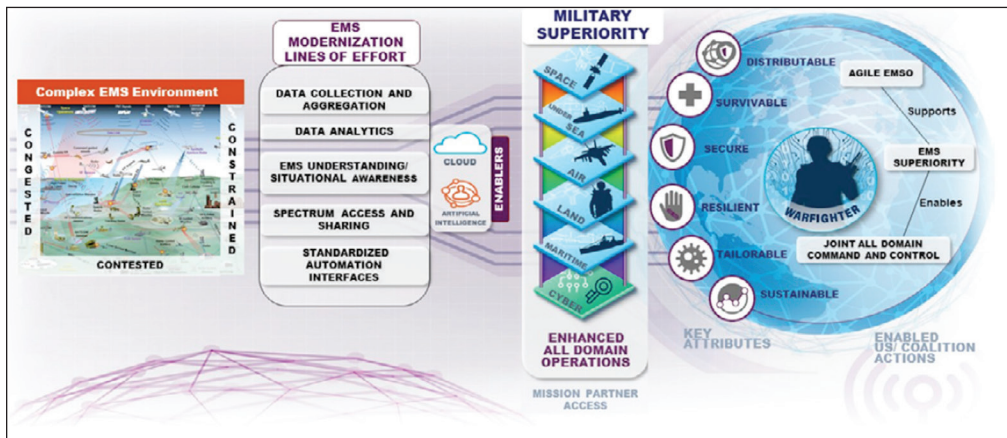


Figure 5- **Electromagnetic Spectrum Operations Visualization** [12]

ⁱⁱⁱ See Appendix 'A' for a table quoted from the same study regarding the electronic weapons in space.

Electronic Protection (EP) or how EA is used as an attack strategy, while ES is merely passive (although passive measures used aggressively can reap immense dividends). One may also give credence to the fact that active defence is not offense.

IV. Global Landscape: Counter Space Capabilities & Space Based Electronic Warfare

“EW is the art of the invisible” [13]. A definition of space electromagnetic warfare as given in a publication [14] by the Defence Technical Information Centre or DTIC is as given below.

“Space Electromagnetic Warfare – Knowledge of spectrum awareness, manoeuvre within the spectrum, and non-kinetic fires within the spectrum to deny adversary use of vital links. Skill to manipulate physical access to communication pathways and awareness of how those pathways contribute to enemy advantage.”

The same DTIC report also mentions the most critical objective of space EW being the gains in the cognitive dimension. *“Decision superiority, deterrence, dissuasion, compellence, and assurance manifest here. Neutralizing an adversary spacecraft offers limited military value if such actions fail to influence the perceptions or decisions of the enemy [14].”*

While counterspace capabilities can be broadly divided into the realms of kinetic physical, non-kinetic physical, cyber and EW, this paper will cover EW and merely touch upon the others. Russia, China and USA have been covered and in addition Australia, France and North Korea.

EW is a viable option for counterspace because of its flexibility: its temporary application at the point of impact and effects on adversary satellite are temporary, unless it employs very high power to burn the

electronics. Also, it does not generate any orbital debris. EW is an extremely attractive option for any space faring in the future intending to protect its assets in space. With greater reliance being placed on ISR and GNSS for operations, EW will be a very potent weapon [15].

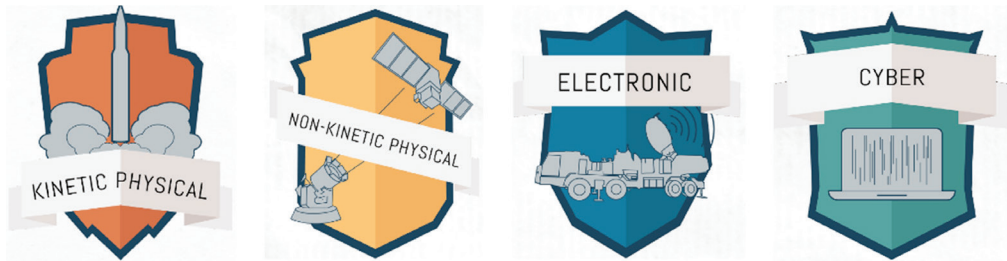


Figure 6- **Symbolic Representation of the Realms of Counterspace Capabilities** [11]

Russia- The birth of Space EW can be traced back in Russia to the era of the US led SDI^{iv} project. OREST-02 was one of the projects which was shelved later. In terms of counter space capabilities Russia has made significant progress. Whether it is RPO^v or EW capabilities, Russia has made investment in jamming PNT^{vi} signals as well as communication uplink



	R&D	Testing	Operational	Use in Conflict
LEO Direct Ascent	●	●	-	●
MEO/GEO Direct Ascent	●	-	-	●
LEO Co-Orbital	●	●	-	●
MEO/GEO Co-Orbital	●	-	-	●
Directed Energy	●	●	?	●
Electronic Warfare	●	●	●	●
Space Situational Awareness	●	●	●	?

Legend: none ● some ● significant ● uncertain "?" no data "-"

^{iv} Strategic Defence Initiative or its popular nickname of the 'Star Wars Programme'.

^v Rendezvous and Proximity Operations

^{vi} Position Navigation and Timing signals

and downlink signals. To counteract the technology prowess by US forces, Russia has made efforts to combine EW into military operations. Russia has also taken several initiatives to drive the EW programme towards significant Space Situational Awareness or SSA capabilities. All its efforts are towards seeking parity with the US forces in this domain. Some examples of the Russian prowess in the field on Space EW can be gauged from the developments of the Peresvet system, Tirada series of satellite EW system and the Bylina systems. Peresvet is the Russian solution to the fourth dimension included in their definition of EW which includes “countermeasures to foreign technical reconnaissance”. Capabilities of Tirada EW system have been covered as part of [16].

In Russian, the name Bylina has been used for a C2 system which are operating in different parts of the radio spectrum (Bylina-KV and Bylina-MM). Open-source information places them as weapons against communication satellites. News released in 2016 talks of another satcom jamming system – KRBSS expanded as “Electronic Warfare Complex to Counter Satellite Systems in Low Circular Orbits”. This system deployed in the Arctic, was probably designed to target LEO satellite constellations such as Iridium, Globalstar, and OneWeb. Krasukha-4 (Russian poisonous plant – *Belladonna* or *Deadly Nightshade*) which has been quite prominent in recent skirmishes is aimed against radar-based surveillance satellites. On-board two Kamaz-650 trucks, both Krasukha -4 and its erstwhile model, Krasukha – 2 are part of the EW complex Moskva -1 (1L267). This project traces its genesis in the 1990s. Another EW Space defence project called the Divnomorye (name based on a Black Sea resort in southern Russia) started development in 2013 and was claimed to be ready for deployment by early 2016. There have been reports of its deployment in 2018. Touted as an improved version of the Moskva -1, it can be used for ELINT as well as a command post [17]. Russia has also constructed three ground-based SIGINT sites intended to pick up and analyze foreign satellite EM emissions over Russia. These will complement the country’s Space Surveillance System (SKKP). These facilities are built under the project name ‘Sledopyt’. Another

such EW complex to protect Russian satellites against EA measures is called the 'Tobol'. Whether the projects have been delayed or have been made operational is not yet known [18]. There have also been rumours surrounding the top-secret nuclear-powered satellite 'Ekipazh' specifically meant for space EW. KRET (Concern Radio-Electronic Technologies), is under the Rostec State Corporation, and is the largest holding in Russia's EW industry. Important stakeholders in the Russian EW systems are Vladimir Design Bureau of Radio Communications (VKBR) with its subcontractors i.e. Vladimir Radio Equipment Factory, the Radio Research and Development Institute (NIIR), NPP Istok, the Moscow Radiotechnical Scientific Research Institute (MNIRTI), and NPO PM-Razvitiye. REB-K units in the Russian defence forces are the operators of Russian EW systems.

China- The PRC space capabilities and developments would require a separate paper to do justice, however, the noteworthy EW related aspects are covered subsequently. The PLA experimented with electronic reconnaissance satellites in the mid-1970s. The satellite was launched from



	R&D	Testing	Operational	Use in Conflict
LEO Direct Ascent	●	●	●	●
MEO/GEO Direct Ascent	●	●	-	●
LEO Co-Orbital	●	?	-	●
MEO/GEO Co-Orbital	●	-	-	●
Directed Energy	●	●	-	●
Electronic Warfare	●	●	●	?
Space Situational Awareness	●	●	●	?

Legend: none ● some ● significant ● uncertain "?" no data "-"

Jiuquan in July 1975 on an FB-1 launch vehicle, which was specifically designed to meet the weight and orbital accuracy requirements of

“Space attack and defence operations are [a type of] direct military confrontation activity carried out mainly in outer space by the opposing sides. Space warfare takes military space forces as the main operational strengths, takes the opposing sides’ direct attack and defence as the basic form of expression, and takes seizing and maintaining dominance of outer space over a certain scope and within a certain time as the basic goal. It is the form of space-domain military struggle sharpest in confrontation and highest in intensity.”

[21]

electronic reconnaissance platforms. The FB-1 launched two more experimental satellites in December 1975 and August 1976. For unknown reasons, the program was discontinued. Publications by the Chinese Academy of Military Sciences bring out the fact often professed by the PLA – Those who can rule space, will rule the Earth. The data available in open source suggests of several developments that have been undertaken by China in terms of Counter Space capabilities. SSA is one of the many functions where impetus has been laid down in China. The reconstitution & reconfiguration of the PLA giving rise to the PLASSF with cyber & EW domains included is a major step highlighting the inclination of PLA towards defensive (active defence) and offensive capabilities. The tests (RPO) which took place after the launch of the ‘SJ’^{vii} series of satellites can be extrapolated for military use, mainly jamming capabilities of adversarial space vehicles. The DIA report of 2019 [19] also brings out the Chinese SATCOM and SAR jamming capabilities. Similar analysis has been done in an ORF occasional brief [20].

vii The notorious Chinese inspector satellite, dubbed Shijian-17 (SJ-17), was relatively quiet this past year but did make a few stops near other satellites as it moved around the GEO belt. According to CSIS analysis, SJ-17 performed three enduring rendezvous proximity operations (RPOs) nearby other Chinese satellites, Chinasat 6B, SJ-20, and Gaofen 13 (GF 13).

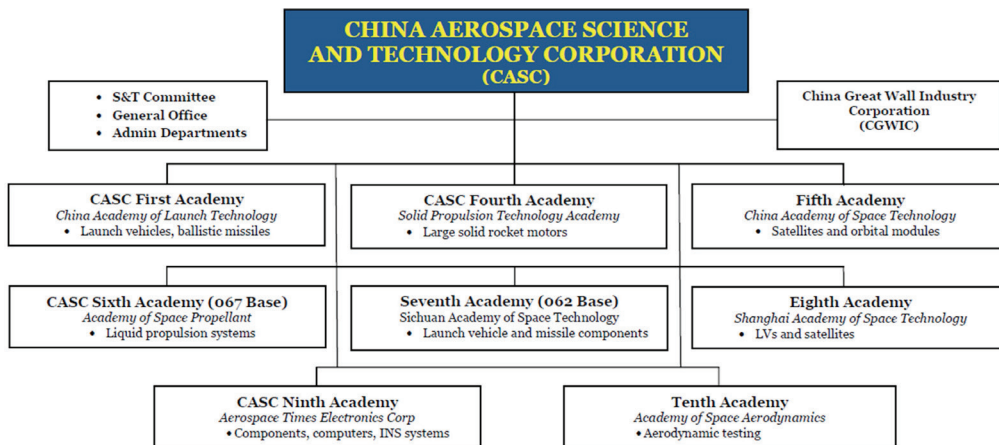


Figure 6– **China Aerospace Science& Technology Corporation** [22]

Open-source data also confirms of the PLA utilizing TDOA^{viii} based techniques for geolocation using clusters of three to four satellites. CASC^{ix} 509th Institute and SWIEE^x have accounts of PLA direction finding and tracking methodologies. While information is sparse, indications exist that at least some funding has been dedicated toward developing a space based ELINT capability as China clearly believes that to exert itself regionally, it has to develop capabilities in electro-optical, SAR and ELINT. Further details regarding the military satellites, stealth satellites and ELINT are covered in papers published by the Chinese Journals. [23] [24] [25]

Chinese and Russian military doctrines present the view of space as an inseparable part of modern warfare and view counterspace capabilities as a means to reduce adversarial military effectiveness. While US established the Space Force, both these countries reorganized their militaries in 2015 to provide impetus to space operations. [26] [27]

viii Time Difference of Arrival – a direction finding method used commonly in EW

ix China Aerospace Science & Technology Corporation

x Southwest Institute of Electronic Equipment

China in the domain of EW is gaining near-parity with the US forces. This includes both soft and hard kill measures as part of the EM spectrum dominance strategy under the umbrella of the overarching ‘informationised’ & ‘intelligent-ised’ concept of integrated network and electronic warfare [28]. Integration between these domains has been professed as “the only way to simultaneously ‘decapitate and blind’ the adversary while ‘crushing their bones and damaging their body’ to sustain the People’s Liberation Army’s advantage and accelerate the operational tempo.” [29] A high-level spectrum policy is also being formulated as per certain reports [30]. The exploitation of space by China in terms of EW can be sensed from reports where scepticism has been seen with activities related to China in space [31] [32] [33] [34]. Another wholesome account of Chinese ELINT & SAR/ Optical imagery capabilities has been covered in the article at [35].

United States (USA) - Through the EW Counter Space System (CSS) and the Navigation Warfare (NAVWAR) programme, US forces are presumably at the top when it comes to EW employed in various domains including space.



	R&D	Testing	Operational	Use in Conflict
LEO Direct Ascent	●	●	-	●
MEO/GEO Direct Ascent	-	-	-	●
LEO Co-Orbital	●	?	-	●
MEO/GEO Co-Orbital	●	?	-	●
Directed Energy	●	●	?	●
Electronic Warfare	●	●	●	●
Space Situational Awareness	●	●	●	●

Legend: none ● some ● significant ● uncertain “?” no data “-”

Defensive and offensive space control are amalgamated into the SSA programme for USA and investments have been made right since the 1960s towards developing a substantial capability. Very little information is available on NAVWAR in the open domain, however, it is estimated that since its inception in 1990s, heavy investments have been made to bolster the capabilities as part of SSA and counter space activities. Similar is the case for the CCS established in 2003. US forces have also conducted various exercises in which activities were done in a GPS denied environment. The US forces are taking the lead and making an all-out effort to ensure that all space assets get unified under a central agency and that the parochial attitudes of individual services are set aside. The setting up of the Space Force (erstwhile US Airforce Space Command) with a Title 10 role (*Title 10 of the United States Code **outlines the role of armed forces in the United States Code.** It provides the legal basis for the roles, missions and organization of each of the services as well as the United States Department of Defence*). amplifies the point [36]. The United States has employed its technological prowess for the development of several weapon systems to maintain ascendancy over adversarial forces in all domains. US forces are heavily reliant on PNT signals and network centrality, even for expeditionary forces. It is launching several satellites every year to extend its military capabilities. In December 2020, the US launched the NROL-44 satellite as part of the plans of the US National Reconnaissance Office (NRO)^{xi}. The Advanced Extremely High Frequency Spacecraft (AEHF-5)^{xii} was earlier launched in 2019 [37]. U.S. Space Force now controls the GPS Block III satellites aimed to provide resilient PNT signals for its forces worldwide. “*The newest satellite from the latest generation of more accurate systems is among a larger group of 24 GPS payloads on orbit that are capable of using a new military PNT signal, M-code.*” [38]

xi The NROL-44 is a geosynchronous signals intelligence (SIGINT) satellite weighing more than 5 tons and is outfitted with a huge parabolic antenna, which unfolds to a diameter of more than 100 meters in space.

xii The AEHF-5 provides jam-proof communications, including real-time video streaming between the control and the deployed forces.

Space Delta-3, formerly the 721st Operations Group, at Peterson Airforce Base, is the unit which controls Space-based EW for the US forces to dominate the space domain. *“Space Delta 3 includes both offensive and defensive space control operations. Offensive space control is intended to prevent an adversary’s hostile use of space capabilities, while defensive space control focuses on identifying and geolocating interference with U.S. capabilities, thereby protecting space capabilities from attack or interference.”*[\[39\]](#) The U.S. military also relies on satellites for SIGINT, and is reported to have up to three giant ‘Mentor/Orion’ satellites parked in GEO for the purpose of collecting radio emissions with radio reflecting dishes estimated to be 100 meters in diameter.[\[40\]](#)



France - France too has made the transition of the satellite control to their military and delinked it from their civil space programme. They have a well-defined Space Defence Strategy.

Iran - Islamic Revolutionary Guard Corps (IRGC) conducted two major exercises in 2020, which Iranian sources claim included “space operations” using jamming drones and radar units from the IRGC Aerospace Force. In February 2021, Aerospace Force Brigadier General Mehdi Hadian hailed Iranian electronic warfare capabilities in recent exercises, with a focus on offensive and counter electronic warfare against enemy air power [\[41\]](#). In March and May 2020, there were reports of Iranian GPS circle spoofing. GPS circle spoofing differs from other spoofing attacks in that it causes transponders to show various erroneous positions forming odd ring-like patterns around a central location. Previously observed in China, the March 2020 incident involved a potential GPS spoofing device in operation at Iran’s Army Command and Staff College [\[42\]](#). The May 2020 incident also involved the circling phenomena with GPS-based reporting systems from vessels and fitness trackers in Tehran. Iran has publicly claimed in the past to have the capability to spoof GPS receivers.

North Korea - U.S. Army published a new manual titled North Korean Tactics in July 2020 which details North Korea's electronic warfare organizations, capabilities, techniques, and tactics. [43] North Korea continues to exercise its downlink jamming capabilities. In April 2020, North Korea announced that it was preparing to deploy a new "GPS jamming device" for use against South Korea. [44] Many open-source reports in the past year highlight jamming focused on commercial radio broadcast frequencies and civilian GPS signals rather than military targets. The report at [43] also highlights the Electronic Warfare Jamming Regiment focused on electronic jamming and signals reconnaissance.

UK - The United Kingdom continues to integrate space into its military structure. In 2021, the country announced building the Royal Air Force Space Command in Scotland. The first commander of the United Kingdom's Space Command was also announced in February 2021 and the command is scheduled to be operational and capable of launching its first rocket by 2022.

Australia - As part of the Project 9358 (includes the JP 9102 Australian Defence SATCOM System project), Australian Defence Forces are exploring options of the deployment of ground-based EW sensors. After the 2020 Defence Strategic Update, this project aims to fill the void in capabilities in EW related to space. Australia's military use of the space domain rests on communications between Earth and satellites. The country's armed forces use satellites for navigation, communications and Signals Intelligence (SIGINT). Central Australia is home to the Pine Gap Earth Station near Alice Springs. Pine Gap receives raw SIGINT from US satellites as they pass over Asia and the Middle East. These SIGINT satellite constellations include Advanced Orion, Improved Trumpet, Mercury and the Space-Based Wide Area Surveillance System. Not surprisingly, no information appears in the public domain on the datalink frequencies used to transmit raw SIGINT to Earth. [45] [46] The Wide Area Space Surveillance (WASS) system of the Australian Defence Forces [47] is how ground stations can be used to monitor

the space activities. The capability consists of using over the horizon radar network to keep track of orbital debris and satellites in LEO. Called the Jindalee Operational Radar Network or JORN, radars are placed at three locations manned by BAE and controlled by the Australian Airforce Number 1 Remote Sensor Unit.

The not so very distant Nagorno-Karabakh conflict drives home some pertinent aspects as regards space-based EW. “First, an integrated air-defence system is critical; Second, the role of electronic warfare should be accentuated; and third, the human factor is key, and it underpins the other two factors.” [48]

V. Space EW Strategy Development Matrix

Since the First Gulf War, Space has gained prominence in executing operations and is a reflection of the foreign policy and strategic interests of a nation [49]. Similar views as regards strategy for Space has been echoed by IDSA in their policy brief [50] which states that geostrategic viewing of the space related activities links it closely to a projection of a nation’s comprehensive power & extension (read symbolic) of foreign policy. Emphasis is therefore necessary to develop capabilities for satellite hardening as well as EW measures to safeguard these national assets in orbit. Strategy, and in turn policy, will be a derivative of the questions asked which underscore the requirement of EW in Space. To quote from an AFCEA^{xiii} whitepaper [51], a wonderful set of intriguing questions put forth have been replicated as under:-

- (a) What are the implications of a contested space environment on ISR developers and users?

xiii AFCEA - Armed Forces Communication and Electronics Association

- (b) Are we treating Space and our use of Space correctly?
- (c) Are the future requirements for the use of space by both the Intelligence Community and Defence Department driving us to the same position on Space ISR or to radically different positions?
- (d) Should we adopt a strategy and policy position that approaches space differently, for instance, as a kinetic or non-kinetic warfighting domain?
- (e) What are the implications of continuing with the current Space posture and not making a change?
- (f) What shorter term actions should we take within our current bounds?

Based on the questions posed earlier, certain strategic goals come to fore when it comes to formulating and implementing a Space EW strategy. To state a few, not in order of precedence are as follows:-

- (a) **Agility** - Developing agile EW options aiding EM spectrum operations. These agile options include the development of state-of-the-art ES and EA measures.
- (b) **Resilience** - Enhance the delivery of own signals in the contested domain. Robust EP measures will ensure that our own forces are not hampered by the adversarial attempts to eavesdrop into our communication and PNT signals. Case in point of the resilient GPS signals by the Block III satellites of the United States.
- (c) **Transparency** - Provide an integrated picture at the theatre level. This will ensure coordination of the resources at the highest level and the judicious employment of EW resources which are not

too proliferated owing to the cost prohibitive technologies involved. Tools such as the EW planning and Management Tool or EWPMT^{xiv} are a great asset in this effort.

(d) **Synchronize** – All sensors to be in sync to help in the analysis of the emerging operational scenario. The endeavour undertaken as part of the ‘Project Convergence’^{xv} by the United States is a glaring example of this synchronization.

(e) **Establish** - A National Space Operations Strategy thereby transition from outdated technology towards seizing high ground with novel sensors and technology.

(f) **Accelerate and Innovate** - Accelerate the deployment of Space based EW assets and innovate by rapid prototyping of payloads.

(g) **Develop** - A conducive environment for development partners to nurture the capability and grow at an accelerated pace. This development can be aided by the correct fusion of military-academia-industry. There is an inescapable need to innovate,optimize and cultivate talent.

The **Terminal Objective** of such an exercise of strategizing should yield in establishing policy and procedures for enabling Space-based EW components and assets. Work towards commonality in operating procedures and equipment which helps to leverage the advantages accrued out of the space-dimension of warfare.

xiv Provide a suite of software tools and applications by delivering six capability drops (CD) that enhance the manoeuvre commander’s cyber-electromagnetic activities (CEMA) element’s ability to plan, coordinate and synchronize electronic warfare (EW), spectrum management (SM), and Cyber operations (CO) across the 2/3/6 staff sections.

xv Project Convergence is the US Army’s campaign of learning, experimentation and demonstration aimed at aggressively integrating the Army’s weapons systems and command and control systems with those of the rest of the Joint Force

VI. Way Ahead for India

Indian activities in space underwent a metamorphosis after March 2019, when the then Prime Minister announced to the world about India's Anti-Satellite Test (ASAT). This heralded the inclusion of India within the gamut of select nations after United States, Russia & China. The latent capabilities existing with India were transformed into a harbinger of the materialization of a strong deterrent capability. Project Shakti as it was dubbed resulted in a change in the way the world viewed India and the message conveyed was that of a transition towards a Space hard power wielding nation [52].

Space domain is the characterized by a Disruption in Military Affairs which has had connected effect on the C4ISR capabilities transforming to C6ISR (including Cyber and Combat Intelligence) [53]. These capabilities, based on their resilience drive the military decision-making process in consonance with enhanced situational awareness – hence, the importance of Space-based EW as a pivotal counterspace capability and the measures to preserve the assets in orbit. Nearly 15 military satellites presently are being used for varied purposes by India, the last being the GSAT-7.

Air Marshal Chaudhari, Vice Chief of Air Staff while addressing the ***e-Symposium on 'Space Technologies for National Defence'***, organized by FICCI, in association with Society for Aerospace, Maritime and Defence Studies (SAMDeS), brought out the need for an independent military space programme which so far has been dependent on ISRO's civil space programme [54]. It was also mentioned that indigenous capability to observe, track and identify non-cooperative objects in outer space is an inescapable requirement looking towards developing a common operating picture. This accentuates the requirement of SSA or Space Domain Awareness of which EW is a key component.

The electromagnetic environment has become exceedingly dynamic. Nations are pushing the envelope when it comes to developing

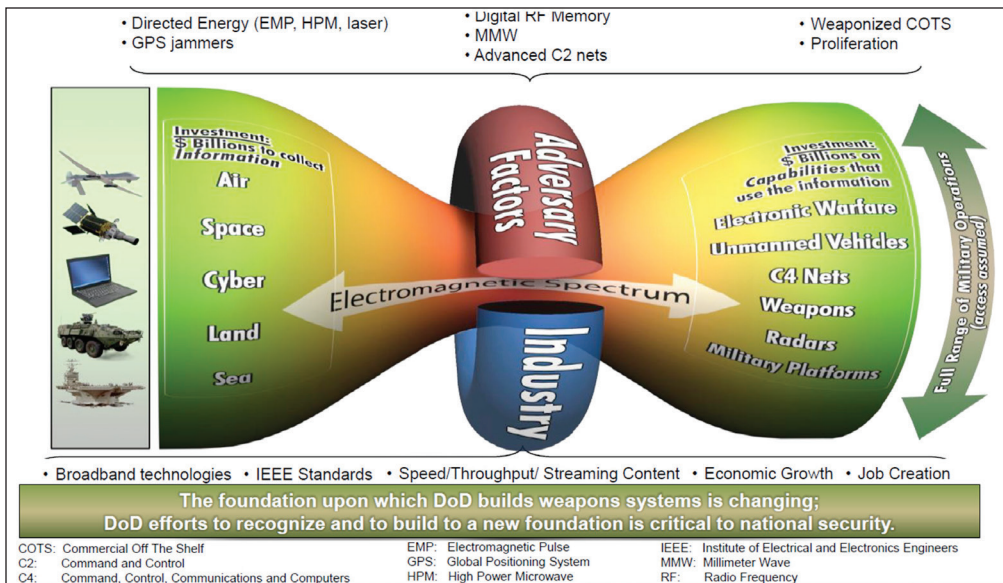


Figure 7– **Rapidly Changing EM Environment** [57]

advanced C4ISR capabilities and are become more reliant on PNT signals and satellites for operations. India too is trying to keep pace with these advances. Defence Space Agency in India has issued a RFI in January 2021 to look at collaborations to thwart threats in this niche domain of Space-based EW [55] [56].

The steps for the way towards attaining parity in the EW domain in the long run will involve meeting certain aims which can be listed as follows:-

- (a) **Aim 1-** Develop Agile Electromagnetic Spectrum Operations.
- (b) **Aim 2 -** Enhance the Delivery of Resilience of Position, Navigation, and Timing (PNT) Information. How much the anti-jamming properties of NavIC (IRNSS – Indian Navigation Constellation) can be utilized is yet to be seen.
- (c) **Aim 3 –** Formulate a Single Point National Level Organization Authority. Establishing a Spectrum Warfare Wing

has been proposed in a Centre for Land and Warfare Studies or CLAWS occasional brief [58].

(d) **Aim 4** – Develop and Provide state-of-the-art Communication Capabilities. This will involve accelerated and proliferated use of software defined radios and a resilient waveform [59] to name a few.

(e) **Aim 5** - Accelerate and Synchronize Fielding of Satellite Systems with Variable Payloads. These payloads in LEO can help in ISR capability along with direction finding EW satellite payloads. ELINT and SAR payloads also need to be increased in number alongside the constellations of cubesats.

(f) **Aim 6** - Develop a Regional Electromagnetic Spectrum Information System on the lines of the U.S. developed GEMSIS^{xvi}. [60]

VII. Implementation Strategy

Having seen the strategy and aims, it is the implementation part of the entire process which is going to bear fruit or lead us to a sustainable end state. Some pointers towards the implementation of the Space-based EW strategy are covered in the succeeding paragraphs.

Action Point I - Like any other domain, alignment with the other doctrines already in place is a necessity which brings us to the fact that there is an emergent need to revisit the EW concepts and **evolve a doctrine** which encompasses the future battlefield scenarios and ways to fight. Space based operations will see a flux with the cyber operations (read cloud-based and Artificial Intelligence), termed as Cyber Electromagnetic Activities (CEMA) interplaying with the classical EW domain. Organizations such as Defence Space Agency, Cyber Command and a

^{xvi} Global Electromagnetic Spectrum Information System (GEMSIS)

dedicated EW organization need to come together to fuse the capabilities thereby aligning the objectives. As a recommendation, the taxonomy of a proposed Space Doctrine/ Publication may be adapted from the Joint Publication 3-14 of the US Forces, issued in October 2020.

Action Point II - Space is a contested, congested and competitive domain. No longer is it the sole playing field for a select few nations. Establishing an 'Aerospace Command' has been marred with a myopic view by the stakeholders. The powers that be, should take cognizance of the similar verticals established in the leading space faring nations to **migrate to a well-structured, agile & responsive organization**. With the lack of established and fundamental doctrine, India must look inwards to other organizations to establish doctrinal principles to enable the space warfare plans, execution, and assess training for the same.

Action Point III - Technology absorption which involves the subsets of **funding research and development**, reverse engineering, developing infrastructure and a wholesome contribution by the military-industry and academia.

Action Point IV - Industry Participation for Research Collaborations and Building Technological Capabilities is inescapable. India has set up the autonomous body, Indian National Space Promotion and Authorisation Centre (IN-SPACE) under the Department of Space (DoS). **IN-SPACE** will act as a link between the ISRO and private sector companies, assessing how best to utilise India's space resources and increase space-based activities. Similarly, the recently established **ISpA** or the Indian Space Association is a positive step towards nurturing private sector participation in Space. ISpA, IN-SPACE along with **NSIL** or the New Space India Limited concern of ISRO can together with joint effort (consortium approach) augur well for the future in this domain. **Incentivization as done for the drone sector** by means of **production linked incentives** should be catered for the Space industry.

Action Point V - Establish programmes such as the **school and college level** NASA space challenges and Grand challenge programme by the NITI Aayog to foster talent in the domain of satellite technology. Simultaneously **invigorate the start-ups**. Measures that have been initiated to invigorate the Space industry including startups is surely going to provide a ray of hope for a new strategic trajectory for India. Reliance on nanosatellite constellations to achieve what the cost-prohibitive smallsats or the 1000 kg satellites cannot. **Rapid prototyping using fast track procedures and faster launch capabilities** are the hallmarks of a well-established Space domain. Programmes such as **Rapid Agile Launch Initiative**, that is, use small satellites to test sensor capabilities.

Action Point VI - Developing an EW Mindset. One of the most essential facets towards developing an EW force lies in mentally and cognitively training the mind to understand the concepts and implement ideas in unorthodox and out-of-the-box ways.

Action Point VII - Partnership with International Space Agencies. Despite the skepticism surrounding the military utility of the Quad, the collaboration between the members for developing better payloads, miniaturization and sharing of research work and data can immensely benefit the cause.

Action Point VIII - Use of Disaggregated Systems – This would entail the stratification of assets at the strategic & tactical/ operational levels and act as a major countermeasure to widespread EA activity by the adversary.

VIII. Conclusion

Military space power is the ability to accomplish strategic and military objectives through the control and exploitation of the space domain. Security, deterrence, and violent competition are the signs of a warfighting force, and military space forces are no different. Progress in the domain of Space EW will reconfigure the rules of deterrence & alter the dynamics during a heightened skirmish. It is high time that we had a comprehensive National Space Operations Strategy to cater to a rainy day in space.

Unlike doctrines, ancient treatises & eponymous texts such that of Sun Tzu which have compiled generations of military experience into comprehensible learnings, space as a domain is new. However, it should always be recalled that the underpinnings remaining the same, it is the application of these learnings that have to be translated into actionable steps extending to the domain of space. Space requires an unprecedented forward-looking approach & out of the box thinking to apply concepts; to forge its own future, while being costly, safeguarding the outer space & the world as we know it against untoward & irresponsible actions. Space has emerged as an inescapable warfighting domain & EW within space inseparable for continued asymmetric advantage & psychological preponderance.

Like China, there is a need to have a national agency to coordinate all the activities pertaining to the militarization of Space. By leveraging the power of Space-based operations, India can afford to exert its presence much beyond its shores in-line with the aim of graduating to become a regional power by complicating the regional dynamics (read China). Over the next decade India must aim at advanced precision strike assets, integrated with persistent space-based surveillance. India's external behavior is characterized by exerting itself as a potent regional power while always preparing itself for a two-front war. The

developments of the recent past have tilted the attention focus towards China while the Af-Pak issue continues to simmer.

Do we want to take the lead, be up there with the leading nations or merely be reactive? This is something we need to answer and decide now. EW has always aimed at developing technology that causes entropy to set in thereby imposing a cost penalty of the adversarial forces. A reactive force will always have catching-up to do. Space with its potential for militarization and with EW in particular needs our immediate attention and aggressive pursuing. Benefits accrued from a COMINT/ ELINT payload in LEO/ MEO has benefits far more enriching than a conventional land-based EW system. Naysayers may be skeptical with respect to the costs involved in development, as budget involved is substantially more due to the complexities involved in micro-electronics, launch costs and associated overheads. However, if we are to keep in mind the ***'Nothing Ever Goes Unnoticed'*** paradigm of EW, then the space-based operations are to be viewed as a life-insurance policy which pays dividends when life is at stake.

Appendix 'A'

Types of Attack	Electronic		
	Uplink Jamming	Downlink Jamming	Spoofing
Attribution	Modest attribution depending on mode of attack	Modest attribution depending on mode of attack	Modest attribution depending on mode of attack
Reversibility	Reversible	Reversible	Reversible
Awareness	Satellite operator will be aware; may or may not be known to the public	Satellite operator will be aware; may or may not be known to the public	May or may not be known to the public
Attacker Damage Assessment	No confirmation of success	Limited confirmation of success if monitoring of the local RF environment is possible	Limited confirmation of success if effects are visible
Collateral Damage	Only disrupts the signals targeted and possible adjacent frequencies	Only disrupts the signals targeted and possible adjacent frequencies	Only corrupts the specific RF signals targeted

Types of Counterspace Weapons

Source: T. Harrison, K. Johnson, and M. Young, "Space Threat Assessment 2021," *Csis.org*, 2021. <https://www.csis.org/analysis/space-threat-assessment-2021> (accessed Oct. 14, 2021).

References and Endnotes

- [1] India, "Title: India a World Leader in Space Technology: Jitendra Singh | Technology News," *Google.com*, 2011. (accessed Sep. 14, 2021).
- [2] Y. S. Rajan, "Development of space technology: Indian experience and future prospects on JSTOR," *Jstor.org*, 2021. https://www.jstor.org/stable/24094541?read-now=1&refreqid=excelsior%3A6ff997983c9518bd65a5389f5e4e9104&seq=1#page_scan_tab_contents (accessed Sep. 14, 2021).
- [3] "Chapter 10. India's Space Enterprise — A Case Study in Strategic Thinking and Planning," *Anu.edu.au*, 2021. <http://press-files.anu.edu.au/downloads/press/p34191/mobile/ch10.html> (accessed Oct. 20, 2021).
- [4] "vikaspedia Domains," *Vikaspedia.in*, 2013. <https://vikaspedia.in/education/childrens-corner/science-section/space-programmes-of-india#:~:text=The%20Indian%20Space%20Research%20Organisation,formed%20on%20August%2015%2C%201969.&text=Since%20inception%2C%20the%20Indian%20space,transportation%20system%20and%20application%20programmes>. (accessed Sep. 14, 2021).
- [5] "JOINT OPERATIONAL ACCESS CONCEPT (JOAC)," 2012. Accessed: Oct. 20, 2021. [Online]. Available: https://dod.defense.gov/Portals/1/Documents/pubs/JOAC_Jan%202012_Signed.pdf.
- [6] C. Giri, "India's Catalytic Reforms for Space 2.0 Era," 2021. [Online]. Available: <https://media.defense.gov/2021/Mar/07/2002595035/-1/-1/1/GIRI.PDF>.
- [7] "Indian Space programme: 2020 Updates & Priorities Presentation by Indian delegation to 58 th session of STSC -UNCOPUOS Vienna, Austria," 2021. [Online]. Available: <https://www.unoosa.org/documents/pdf/copuos/stsc/2021/tech-06E.pdf>.
- [8] M. Pomerleau, "Here's how new space tech is helping electronic warfare forces on the ground," *Defense News*, Apr. 13, 2021. <https://www.defensenews.com/electronic-warfare/2021/04/13/heres-how-new-space-tech-is-helping-electronic-warfare-forces-on-the-ground/> (accessed Oct. 23, 2021).

- [9] M. V. Spreckelsen, "Electronic Warfare – The Forgotten Discipline | Joint Air Power Competence Centre," *Joint Air Power Competence Centre*, Dec. 13, 2018. <https://www.japcc.org/electronic-warfare-the-forgotten-discipline/> (accessed Oct. 23, 2021).
- [10] A. Minhas, "Space Weapons: A Rapidly Evolving Threat to South Asian Strategic Balance," 2018. Accessed: Oct. 04, 2021. [Online]. Available: <https://ndu.edu.pk/ndu-journal/2018/16-Space-Wpns.pdf>.
- [11] T. Harrison, K. Johnson, and M. Young, "Defense Against the Dark Arts in Space: Protecting Space Systems from Counterspace Weapons," *Csis.org*, 2021. <https://www.csis.org/analysis/defense-against-dark-arts-space-protecting-space-systems-counterspace-weapons> (accessed Oct. 04, 2021).
- [12] A. Rosner, E. Coyle, and K. Pugh, "Agile Electromagnetic Spectrum Operations," presented at the Agile Electromagnetic Spectrum Operations -Increasing the Agility of Spectrum Maneuver for DoD, Dec. 2020, [Online]. Available: https://disa.mil/-/media/Files/DISA/News/Events/2020-Virtual-Experience/AFCEA_Agile_EMSO_Rosner_Coyle_Pugh_11-3-20_Final_PAO_Approved.ashx (accessed Oct. 20, 2021)
- [13] K. Atherton, "What's the frequency, Putin? 5 questions about Russia's EW capability," *C4ISRNet*, Jun. 04, 2018. <https://www.c4isrnet.com/electronic-warfare/2018/06/04/whats-the-frequency-putin-5-questions-about-russias-ew-capability/> (accessed Oct. 27, 2021).
- [14] SPACE FORCE WASHINGTON DC, "Space Capstone Publication: SPACE POWER. Doctrine for Space Forces," *DTIC*, 2020. <https://apps.dtic.mil/sti/citations/AD1129735> (accessed Oct. 27, 2021).
- [15] "Global Counterspace Capabilities | Secure World," *Swfound.org*, 2021. <https://swfound.org/counterspace/> (accessed Oct. 27, 2021).
- [16] "Российские военные смогут подавлять враждебные спутники с Земли," *Interfax.ru*, Jan. 04, 2018. <https://www.interfax.ru/russia/594392> (accessed Oct. 23, 2021). Translated as "Russian military will be able to suppress hostile satellites from Earth" comments on the Tirada system.

- [17] “The Space Review: Russia gears up for electronic warfare in space (part 1),” *Thespaceview.com*, 2020. <https://www.thespaceview.com/article/4056/1> (accessed Oct. 23, 2021).
- [18] “The Space Review: Russia gears up for electronic warfare in space (part 2),” *Thespaceview.com*, 2020. <https://www.thespaceview.com/article/4060/1> (accessed Oct. 23, 2021).
- [19] Defence Intelligence Agency, “Challenges to Security in Space,” January 2019, p. 20, http://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf.
- [20] Kartik Bommakanti, “‘Soft Kill’ or ‘Hard Kill’? The Requirements for India’s Space and Counter-Space Capabilities”, *ORF Occasional Paper No. 224*, November 2019, Observer Research Foundation.
- [21] ChinaAerospaceStudiesInstitute, “In Their Own Words: Foreign Military Thought Science of Military Strategy,” 2013. [Online]. Available: https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2021-02-08%20Chinese%20Military%20Thoughts-%20In%20their%20own%20words%20Science%20of%20Military%20Strategy%202013.pdf?ver=NxAWg4BPw_NylEjxaha8Aw%3d%3d.
- [22] Project 2049 Institute, “China’s Evolving Space Capabilities: Implications for U.S. Interests,” *Project2049.net*, Apr. 26, 2012. <https://project2049.net/2012/04/26/chinas-evolving-space-capabilities-implications-for-u-s-interests/> (accessed Oct. 24, 2021).
- [23] Huang Hanwen, “Conceptual Study on Stealth Satellites [卫星隐身概念研究], *Aerospace Electronic Countermeasures* [航天电子对抗], June 2010, pp. 22-34.
- [24] For space-based electronic reconnaissance systems, see Yuan Xiaokang, “Satellite Electronic Reconnaissance, Antijamming,” *Shanghai Hangtian*, October 9, 1996, pp. 32-37, in *FBIS-CST-97-011*; and Yuan Xiaokang, “Some Problems of Space Electronic Reconnaissance,” *Hangtian Dianzi Duikang*, March 1996, pp. 1-5, in *CAMA*, Vol. 3, No. 4.

[25] Pan Changpeng, Gu Wenjin and Chen Jie, “An Analysis on the Capabilities of Military Satellites to Support an ASBM in Offense and Defense Operations” [军事卫星对反舰导弹攻防作战的支援能力分析], 2006, No. 5.

[26] “Challenges to Security in Space.” [Online]. Available: https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf.

[27] V. Samson and W. Office, “Global Counterspace Capabilities: An Open Source Assessment,” 2020. [Online]. Available: https://swfound.org/media/206970/swf_counterspace2020_electronic_final.pdf.

[28] M. Clay, “To Rule the Invisible Battlefield: The Electromagnetic Spectrum and Chinese Military Power - War on the Rocks,” *War on the Rocks*, Jan. 22, 2021. <https://warontherocks.com/2021/01/to-rule-the-invisible-battlefield-the-electromagnetic-spectrum-and-chinese-military-power/> (accessed Oct. 22, 2021).

[29] Office of the Secretary of Defense, “Office of the Secretary of Defense annual report to congress: Military and security developments involving the people’s republic of china i,” 2020. [Online]. Available: <https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF>.

[30] 张思远, “余志锋: 为打赢信息化局部战争冲锋, 再冲锋 - 中国军网,” *Wwww.81.cn*, 2020. http://www.81.cn/201311/jxjhh/2020-06/08/content_9830067.htm (accessed Oct. 22, 2021). - Yu Zhifeng, associate professor of the School of Electronic Warfare, National University of Defence Technology an influential scholar warrior is key to the “Development Strategy in the Field of Electronic Warfare”.

[31] Reuters Staff, “China denies it is behind hacking of U.S. satellites,” *U.S.*, Oct. 31, 2011. <https://www.reuters.com/article/us-china-us-hacking-idUSTRE79U1YI20111031> (accessed Oct. 21, 2021) - “At least two U.S. environment-monitoring satellites were interfered with four or more times in 2007 and 2008 via a ground station in Norway, and China’s military is a prime suspect, according to the draft report to Congress.”

[32] Reuters Staff, “China denies it is behind hacking of U.S. satellites,” *U.S.*, Oct. 31, 2011. <https://www.reuters.com/article/us-china-us-hacking/china-denies-it-is->

behind-hacking-of-u-s-satellites-idUSTRE79U1YI20111031 (accessed Oct. 04, 2021).

[33] TZVI JOFFRE, "U.S. warns of GPS interference, communications spoofing in Persian Gulf," *The Jerusalem Post* | *JPost.com*, 2019. <https://www.jpost.com/middle-east/us-warns-of-gps-interference-communications-spoofing-in-persian-gulf-597998> (accessed Oct. 04, 2021).

[34] Y. BUTT, "Effects of Chinese Laser Ranging on Imaging Satellites," *Science & Global Security*, vol. 17, no. 1, pp. 20–35, Jun. 2009, doi: 10.1080/08929880902864376.

[35] ANI, "China's eye in the sky: An Analysis of China's satellite surveillance," @ *bsindia*, Oct. 30, 2019. https://www.business-standard.com/article/news-ani/china-s-eye-in-the-sky-an-analysis-of-china-s-satellite-surveillance-119103000151_1.html (accessed Oct. 24, 2021).

[36] M. Donovan, "US military must avoid a 'Kasserine Pass' failure for space power," *C4ISRNet*, Jul. 19, 2021. <https://www.c4isrnet.com/opinion/2021/07/19/us-military-must-avoid-a-kasserine-pass-failure-for-space-power/> (accessed Oct. 22, 2021).

[37] AEHF Satellite - N. Strout, "Space Operations Command takes over final AEHF satellite," *Defense News*, Dec. 08, 2020. <https://www.defensenews.com/battlefield-tech/space/2020/12/08/space-operations-command-takes-over-final-aehf-satellite/> (accessed Oct. 23, 2021).

[38] N. Strout, "Space Force declares operational acceptance of fifth anti-jamming GPS III satellite," *C4ISRNet*, Jul. 15, 2021. <https://www.c4isrnet.com/battlefield-tech/space/2021/07/15/space-force-declares-operational-acceptance-of-fifth-anti-jamming-gps-iii-satellite/> (accessed Oct. 23, 2021).

[39] "Space Delta 3 focuses on electromagnetic spectrum," *Peterson Space Force Base*, Feb. 16, 2021. <https://www.peterson.spaceforce.mil/News/Article/2504236/space-delta-3-focuses-on-electromagnetic-spectrum> (accessed Oct. 23, 2021).

[40] "Jonathan's Space Report," No. 369, August 22, 1998, www.planet4589.org/space/jsr/back/news.369

- [41] T. Harrison, K. Johnson, and J. Moye, "April 2021 A REPORT OF THE CSIS AEROSPACE SECURITY PROJECT." [Online]. Available: https://aerospace.csis.org/wp-content/uploads/2021/03/CSIS_Harrison_SpaceThreatAssessment2021.pdf.
- [42] D. Goward, "GPS circle spoofing discovered in Iran - GPS World," *GPS World*, Apr. 21, 2020. <https://www.gpsworld.com/gps-circle-spoofing-discovered-in-iran/> (accessed Oct. 28, 2021).
- [43] "ATP 7-100.2 NORTH KOREAN TACTICS Headquarters, Department of the Army," 2020. Accessed: Oct. 28, 2021. [Online]. Available: <https://irp.fas.org/doddir/army/atp7-100-2.pdf>. – See Chapter 9 on Electronic Intelligence Warfare (EIW) or *chonja chinungjon*
- [44] Editor, "N. Korea readies deployment of new GPS jamming device / Link to funeral prep - Daily NK & IBT - RNTF," *RNTF*, May 2020. <https://rntfnd.org/2020/05/01/n-korea-readies-deployment-of-new-gps-jamming-device-link-to-funeral-prep-daily-nk-ibt/> (accessed Oct. 28, 2021).
- [45] Dr. Thomas Withington, "Space Savers - Armada International," *Armada International*, Sep. 09, 2021. <https://www.armadainternational.com/2021/09/space-savers/> (accessed Oct. 23, 2021).
- [46] C. Kadib, "Defence launches new project to guard space domain," *Defenceconnect.com.au*, Jul. 29, 2021. <https://www.defenceconnect.com.au/intel-cyber/8486-defence-launches-new-project-to-guard-space-domain> (accessed Oct. 23, 2021).
- [47] R. ACT, "Department of Defence," *Defence.gov.au*, 2021. <https://www1.defence.gov.au/project/wide-area-and-space-surveillance> (accessed Oct. 22, 2021).
- [48] B. Ho, "The Second Nagorno-Karabakh War: Takeaways for Singapore's Ground-Based Air Defense," *Air University (AU)*, Aug. 25, 2021. <https://www.airuniversity.af.edu/JIPA/Display/Article/2743721/the-second-nagorno-karabakh-war-takeaways-for-singapores-ground-based-air-defen/> (accessed Oct. 06, 2021).
- [49] Admin PSF, "Space Weapons: A Rapidly Evolving Threat to South Asian Strategic Balance (Review) - Pakistan Strategic Forum," *Pakistan Strategic Forum*, Jan.

14, 2021. <https://pakstrategic.com/2021/01/14/space-weapons-a-rapidly-evolving-threat-to-south-asian-strategic-balance-review/> (accessed Oct. 24, 2021). – Original article written by Ahmed Saeed Minhas, ISSRA National Defence University, Pakistan and available online at https://ndu.edu.pk/issra/issra_pub/articles/ndu-journal/NDU-Journal-2018/16-Space-Wpns.pdf

[50] “India’s Space Security Policy: A Proposal | Manohar Parrikar Institute for Defence Studies and Analyses,” *Idsa.in*, 2016. https://idsa.in/policybrief/indias-space-security-policy_alele_280416 (accessed Oct. 27, 2021).

[51] “Space ISR in a Contested Environment.” Accessed: Oct. 4, 2021. [Online]. Available: https://www.afcea.org/mission/intel/documents/AFC_FallIntel_WhitePaper_R4.pdf

[52] Shounak Set, “India’s Space Power: Revisiting the Anti-Satellite Test,” *Carnegie India*, 2019. <https://carnegieindia.org/2019/09/06/india-s-space-power-revisiting-anti-satellite-test-pub-79797> (accessed Sep. 14, 2021).

[53] Kapoor, Lt Gen Anil. “Joint C6ISR and Exploitation of Space Domain - A Roadmap to Address the Capability Gaps.” *Cenjows.in*, CENJOWS, Aug. 2021, cenjows.in/upload_images/pdf/Synergy_%20August%20-2021_Final.pdf. Accessed 23 Sept. 2021.

[54] “Press Release: Space Technology for National Defence | SAMDeS INDIA’S BLOG,” *SAMDeS INDIA’S BLOG*, Sep. 08, 2021. https://www.samdesindia.in/blog/press-release-space-technology-for-national-defence/?_ga=2.90344670.590392948.1635025414-1598202995.1635025414 (accessed Oct. 23, 2021).

[55] Chethan Kumar, “To counter China, India’s DSA begins scouting for star wars technology,” *The Times of India*, Feb. 23, 2021. <https://timesofindia.indiatimes.com/india/india-begins-scouting-for-star-wars-technology/articleshow/81163698.cms> (accessed Oct. 28, 2021).

[56] “Reportlinker’s Space-Based C4ISR Market – Growth, Trends, COVID-19 Impact, And Forecasts (2021 – 2026) – SatNews,” *Satnews.com*, Mar. 29, 2021.

<https://news.satnews.com/2021/03/29/reportlinkers-space-based-c4isr-market-growth-trends-covid-19-impact-and-forecasts-2021-2026/> (accessed Oct. 23, 2021).

[57] A. Rosner, E. Coyle, and K. Pugh, "Agile Electromagnetic Spectrum Operations," AFCEA, Dec. 2020. https://disa.mil/~media/Files/DISA/News/Events/2020-Virtual-Experience/AFCEA_Agile_EMSO_Rosner_Coyle_Pugh_11-3-20_Final_PAO_Approved.ashx (accessed Oct. 03, 2021).

[58] Lieutenant Colonel Vivek Gopal, "Electronic Warfare Capability: Establishment of Spectrum Warfare Wing and Roadmap for India – Centre for Land Warfare Studies (CLAWS)," *Claws.in*, Jun. 28, 2021. <https://www.claws.in/publication/electronic-warfare-capability-establishment-of-spectrum-warfare-wing-and-roadmap-for-india/> (accessed Oct. 27, 2021).

[59] Vivek Gopal, "Joint Waveform Interoperability System - COMMON TACTICAL DATA LINKS FOR THE FORCE OF 21ST CENTURY," *Centre for Joint Warfare Studies (CENJOWS)*, 2021, doi: 10.13140/RG.2.2.23398.55362.

[60] "Global Electromagnetic Spectrum Information System (GEMSIS)." Accessed: Oct. 24, 2021. [Online]. Available: <https://www.disa.mil/~media/Files/DISA/Services/DSO/GEMSISpectrumCapabilities.pdf>