POLICY BRIEF NO. 116/2023-24

CHINA ENTERING THE AGE OF SPACE WARS

SHANTANU K. BANSAL

Founder of IADN. He has more than 10 years of experience in research and analysis. An award-winning researcher, he writes for the leading defence and security journals, think tanks and in-service publications. He has been a senior consultant to the Army Training Command (ARTRAC), Shimla and the Helicopter Training School (HTS), Indian Air Force.

The near-space has emerged as the most active frontier of human activities, with the emergence of small reusable rocket infrastructure, miniaturisation of space technologies and the prevalence of small groups of satellites providing better services compared to conventional heavy-weight satellites, human dependence on space is going to increase by many folds. Space is also an enabler of national power. Space assets have been used since the Cold War period to support both civil, military and commercial applications in the domains such as remote sensing, communication, navigation, oceanography, meteorology and more.

Space assets are dual-use in nature, which means they can simultaneously cater to civil and military needs. All major spacefaring countries have been actively searching for opportunities to support military infrastructure utilising space assets for reconnaissance, communication, target identification, weapon guidance, fire direction and command and control of the battlefield enabling Net-Centric Operations (NCO) and seamless integration of military assets at land, air, sea and undersea. China has been an active spacefaring nation with an extensive focus on the utilisation of space assets for military functions.

During the past 10 years, China has doubled its launches per year and the number of satellites in orbit. Last year in 2022, China conducted 64 space launches, including two space launch failures. The successful launches resulted in over 150 satellites successfully placed into different orbits and the launch of one orbital and one suborbital spaceplane was also conducted.

China far exceeds India in utilising the space domain to fulfil its power aspirations. Space is becoming China's key domain of interest as it enables 'fighting wars under informatized conditions', which is the People's Liberation Army's (PLA) main doctrinal guidance. From utilising space assets for near real-time monitoring of the South China Sea (SCS) to gaining capabilities to target space assets with the use of a wide variety of Anti-Satellite weapons (ASATs). China has been increasingly focusing on utilising space to enable sensors to shooter loop, all-weather remote sensing and mapping, image/video surveillance, electronic reconnaissance, anti-ballistic missile sensors, encrypted quantum communications, laser communication, Wide Area internet connectivity, and more for varied military roles with equal focus on counter-space weapons. In 2016, on the first China 'Space Day', Chinese President Xi Jinping directed his government and the military to become the "*foremost global space power by 2045*."

*The **United States** was the first country to **develop** an **ASAT** weapons system*

China's space and anti-space programmes are largely focused towards the U.S. which China considers as the prime opponent. A *Xinhua* (Chinese media website) in one of its article reads that "*for countries that can never win a war with the US by using the method of tanks and planes, attacking the US space systems may be an irresistible and most tempting choice*." As the US Armed Forces largely rely on space assets for conducting its operations, overseas. Since US Armed Forces are known to undertake expeditionary missions; it is highly dependent on space assets as terrestrial communications remain weak and susceptible to interdictions that make

US opponents more interested in counter-space systems or formally known as Anti-satellite (ASAT) technology. As per some estimates, more than 60 per cent of all global civil space expenditure and 80 per cent of the world's military activity is undertaken by the USA. The United States was the first country to develop an ASAT weapons system. While the US-China competition in space is to intensify in coming years, as a result, China is heavily focusing on building space support and counter-space capabilities.

UNDERSTANDING CHINA'S INTENT TOWARDS MILITARISATION OF SPACE

China has been an active spacefaring nation with an extensive focus on the utilisation of space assets for military functions. However, China's space programme provides great emphasis on military purposes while in comparison India's space programme is largely dedicated to civilian purposes. China far exceeds India in utilising the space domain to fulfil its

defence and security agendas. Space is becoming the key domain of interest for China as it enables '*fighting wars under informatized conditions*' which is the People's Liberation Army's (PLA) main doctrinal guidance.

The last National Defence White Paper of China was published in the year 2019 majorly addressed the U.S. as a priority threat to its national security and India got very little attention. The earlier 2015 White Paper gave a directive to the PLA to prepare for "*winning local wars under high-technology conditions*", it further directs the PLA to "*win informatized local wars*" with emphasis on the struggle in the maritime domain. These phrases have been adjusted twice, once in 2004 and again in the 2015 Defence White Paper which is largely taken from 1993 guidelines to PLA. Chinese military science sources describe key modernization efforts as driven by an "*information system–based system-of-systems*" approach, akin to U.S. Network-Centric Warfare (NCW) program.

The 2013 Lectures on the Science of Army Campaigns provides updated PLA thinking on campaigns. An informatized military would experience greater offensive advantages than in the past in conducting sudden, concealed indirect attacks with dispersed forces to disrupt the cohesion of the enemy's defensive system. Informatized systems like reconnaissance, communications, navigation and positioning satellites can support concealed assembly, deployment, manoeuvre and attack. Today, China has in place the full spectrum of space military capabilities to fight and win local wars under informatized conditions as enunciated by its leaders in past.

Such modernised force could better conduct multi-dimensional manoeuvres and multi-directional feints to confuse and stress the defender, seize key terrain, and achieve a deep attack against the opponent state. The PLA also believes that informatized logistics and equipment support can overcome many of the difficulties posed by the complex environment. Ultimately, the PLA seeks to turn itself into a modern, network-enabled fighting force, capable of undertaking swift annexation of Republic of China (ROC) Taiwan, projecting sustained power far throughout the Pacific region.

The PLA sees space, cyberspace and the electromagnetic domain as critical '*strategic frontiers*' and the 'commanding heights' of future warfare. PLA is concentrating on 'information operations' that include space warfare, cyber warfare, electronic warfare and information warfare capabilities. The establishment of the PLA Strategic Support Force (SSF) in 2015 integrated the PLA's space, cyber, electronic and information warfare capabilities in order to enhance its capability to achieve dominance in these "*new commanding heights*" of future warfare as part of PLA's "*unrestricted warfare strategy*" to use public opinion warfare, psychological warfare, legal warfare, economic warfare, financial warfare, and other asymmetric/irregular components of warfighting which might not have any direct significance on the battlefield but can be of valuable support to achieve strategic objectives during a war or No War No Peace (NWNP) scenario.

*Today, **China** has in place the **full spectrum** of space **military capabilities** to fight and win **local wars** under **informatized conditions***

In particular, the PLASSF could advance the PLA's capability to provide information support to joint operations. As it is responsible for engaging in intelligence, surveillance and reconnaissance within the space, cyber, and electromagnetic domains, acting as an "information umbrella" for the PLA as a whole, the SSF would thus serve as a critical enabler of the PLA's ability to project power, not only to conventional but perhaps also in support of its nuclear force – PLA Rocket Force (PLARF). It may also ensure counter-space, cyber and EW attack capabilities.

Given the perceived dominance of offensive attacks in this domain, the PLA is believed to prefer seizing the initiative through a "*first-strike*." Increasingly, the PLA considers cyber capabilities a critical component in its overall integrated strategic deterrence posture, alongside space and nuclear deterrence. In 2015 China's Defence White Paper also called to expedite the development of a Cyber Force. Besides the cyber domain,

China has one of the most diverse space-based ISR capabilities second to the U.S. and one of its stated missions includes achieving near-real-time image and communication coverage throughout the Earth.

China's space missions perpetually help the PLA '*informatization*' dream. China's Space White Paper which was publicised in December 2016 states *"to explore the vast cosmos, develop the space industry, and build China into a space power is a dream we pursue unremittingly*." China space papers have always advocated the peaceful use of space but China's growing interest in counter-space weapons proves otherwise.

China** is heavily focusing on building **space support** and **counter-space capabilities

CHINA'S INTEREST IN COUNTER-SPACE CAPABILITIES

Potential Susceptibility of Indian Space Systems to Chinese Counterspace Activities

Evolving Chinese Counterspace Systems	Indian Space Systems						
	Telemetry, tracking, and command stations	Communications satellites	Earth observation satellites (electro-optical/ infrared)	Earth observation satellites (synthetic aperture radar)	Navigation satellites	Electronic intelligence satellites	Science and research satellites
Cyber attacks	✓						
Space-based jamming	✓	✓		✓			✓
Ground- and air-based jamming		✓	✓	✓	✓	✓	✓
Ground-based directed energy weapons			✓	✓		✓	✓
Space-based high-power microwave weapons			✓	✓		✓	✓
Direct ascent interceptors		✓	✓	✓	✓	✓	✓
Co-orbital attack satellites			✓	✓		✓	✓
Co-orbital "service" satellites			✓	✓		✓	✓
Ground attack	✓						
Nuclear/ electromagnetic pulse attack	✓	✓	✓	✓	✓	✓	✓

Credits: Centre for Strategic and International Studies (CSIS)

Space above the *Karman line* 100 km above sea level is considered a global common where no country can put its territorial claim. While the "Outer Space Treaty" of 1967 and the supplementary treaty Prevention of Arms Race in Outer Space (PAROS) to some extent prohibit placing Weapons of Mass Destruction (WMD) in space, no treaty prohibits space assets from being attacked using non-nuclear Kinetic Kill Vehicles (KKVs), or electronically, with Directed Energy Weapons (DEWs) or other non-kinetic ASAT systems.

At present, China has the capability to target Low-Earth Orbit (LEO) satellites with KKV, the LEO accounts for the majority of surveillance satellites like Earth Observation, and Electronic Intelligence, and by some accounts, about 80 per cent of surveillance satellites are placed in LEO. The Medium Earth Orbit (MEO) accounts for the majority of navigation satellites and the Geostationary Earth Orbit (GEO) accounts for the majority of communication satellites with the exception of geostationary electronic and imagery surveillance satellites. Chinese defence academics often publish on counter-space threat technologies.

These scholars stress the necessity of "*destroying, damaging, and interfering with the enemy's reconnaissance and communications satellites*," suggesting that such systems, as well as navigation and early warning satellites, could be among the targets of attacks designed to "*blind and deafen the enemy*." The US Senate Armed Services Committee in 2022 that the goal of the Chinese military is to "*blind and deafen*" the enemy by crippling reconnaissance, communications, navigation, and early warning satellites.

The People's Liberation Army Strategic Support Force (PLASSF) has consolidated the management and control over space assets for military use with a Space System Department (SSD) under the PLASSF; it may also have command over China's ASAT systems. In the near future, China might give more emphasis on developing space war capabilities as the U.S. has already taken steps to use space as a tool to push its hard power with the formulation of a separate U.S. Space Force branch at par with its – army, navy, marine corps, coast guard and air force. The competition between the three major powers – US, China, and Russia – and the increased international footprint in space could further provide impetus to counter-space weapons or even pave the way towards the weaponisation of space.

*In the near future, **China** might give more emphasis on developing **space war capabilities***

CHINA'S KINETIC COUNTER SPACE CAPABILITIES

The relevance of ASATs has been there since last at least 60 years. The development of ASAT weapons was bolstered in the background of the cold war period marked by the US and Russia rivalry. The first ASAT was tested in October 1959. According to the Federation of American Scientists, an "air-launched ballistic missile" was fired from a B-47 bomber of the US Air Force at an Explorer VI satellite. The ASAT weapon "apparently came within four miles of its target"; the programme was called *'Bold Orion'*. The Soviet Union first tested the *Polyot* interceptor in 1963 and successfully tested an orbital anti-satellite (ASAT) weapon in 1968. In contrast to the United States and China, Russia has largely preferred the co-orbital type of ASAT systems with its own weapons development and testing dating back to the 1960s. The *Istrebitel Sputnikov* (IS) or known as "satellite destroyer" but the programme came to an in 1983.

A 'miniature' ASAT missile that could be carried on the then MiG-31 fighter was later on revealed by Russia in the 1980s. In 1985, the United States Air Force conducted a test of a similar air-launched weapon system called the ASM-135 ASAT. China first tested a direct-ascent ASAT system in 2007, which was later assessed as a result of the US withdrawal from the 1972 Anti-Ballistic Missile Treaty (ABMT) in 2002. This was followed by February 20, 2008, American ASAT test, where a Standard Missile-3 (SM-3) from a US Navy Aegis destroyer took out a USA-193 reconnaissance satellite. India conducted its first ASAT test in 2019 under the *Mission Shakti*.

On 15 November 2021, Russia conducted a direct-ascent ASAT test by destroying a defunct Cosmos-1408 satellite. In April 2020 U.S. pledged to no longer conduct direct-ascent ASAT missile testing with a call on other nations to follow and establish this as an international norm although as of 2020, US has stood out as a nation to conduct the maximum number of ASAT tests: U.S. (30), Russia (28), China (10), India (1).

TYPES OF KINETIC-KILL ASAT WEAPONS

1. **Direct-Ascent ASAT:** Direct-ascent ASAT systems (Aka. Kinetic Hit-to-kill Vehicles) involve launching a ballistic missile or projectile directly at the target satellite. The missile follows a trajectory that intercepts the satellite in space. Upon reaching the target, the missile can employ various means to disable or destroy the satellite, such as through a kinetic impact or an explosive warhead. This type of ASAT system typically requires precise targeting and guidance similar to Ballistic Missile Defence (BMD) interceptor to ensure a successful interception of satellites which could be launched from land, air and sea.
2. **Co-Orbital ASAT:** Co-orbital ASAT systems differ from the direct-ascent systems in the ASAT family as they place a dedicated satellite or spacecraft in a similar orbit to the target satellite. The co-orbital ASAT then uses its proximity to the target satellite in order to execute its mission. This type of ASAT system can employ different methods to disable or destroy the target by using direct kinetic impact, explosive

charges, or even space arms. These systems can potentially offer advantages in terms of flexibility and the ability to track and engage multiple satellites for effective Space Traffic Management (STM).

THE DOWNSIDE OF LETHAL ASAT WEAPONS

- The space debris which is generated by a kinetic hit can really be dangerous as they travel at a speed of up to 30,000 km per hour, which turns even tiny piece of junk into deadly shrapnel that can damage satellites, space shuttles and even space stations which severely restrict this option.
- Disabling a satellite through a kinetic-kill vehicle/Direct Ascent (DA-ASAT) could cause a chain reaction in space which can blow multiple satellites once a single satellite gets hit as per Kessler syndrome unless course correction measures are taken by the satellites in response to the immediate situation.
- Kinetic ASATs are expensive and may cost the same amount as what a normal space rocket would cost.
- Military satellites orbit at about 800 km above sea level and move at 7.5 km/s and are difficult to intercept for which missile will require accurate guidance in the terminal phase.
- While ASAT missiles can cover LEO but the GPS and communications satellites orbit at much higher altitudes of 20,000 to 36,000km putting them out of range of most of the solid-fuelled ICBMs.

*The **U.S.** has stood out as a nation to conduct the **maximum** number of **ASAT tests***

CHINA'S KINETIC HIT-TO-KILL VEHICLES (HTK)

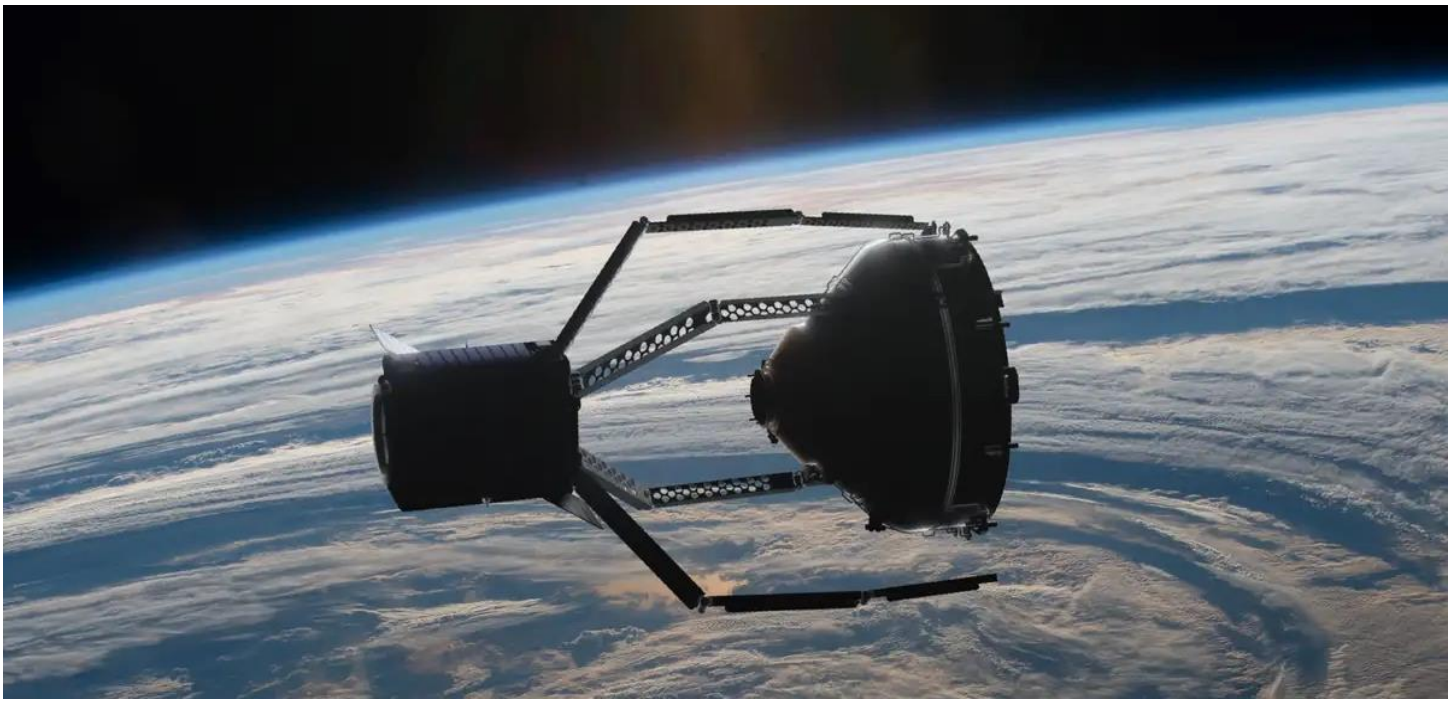
Both direct-ascent and co-orbital ASAT systems have been developed and tested by various countries. China codenamed the *Direct Fire Systems* which refer to the instrumentalities required for a land or vehicle-based missile to strike a satellite. It is a Kinetic Kill system designed to physically destroy or damage a satellite in a '*Hit to Kill*' mode. China has proclaimed that it has tested such systems multiple times but the most prominent test was in 2007. The former GAD and China Aerospace Science and Industry Corporation (CASIC) demonstrated a space intercept KKV in January 2007 in which SC-19 or DN-1 ASAT missile was used to strike a retired *Fengyun* series weather satellite. Given the test was done in 2007; *Dong Neng*-1 (DN-1) ASAT missile must be operational in some numbers in the PLA inventory.

As per some accounts, the advanced version of Dong Neng hit-to-kill kinetic ASAT, the DN-2 ASAT missile of China might be capable of hitting MEO satellites and the successor DN-3 is capable of hitting the GEO-based satellites. The experts believe that in order to target satellites in

geostationary or geosynchronous orbit, China would need to have Intercontinental Ballistic Missile (ICBM) sized interceptors. China has been conducting secret Direct Ascent ASAT (DA-ASAT) tests from time to time.

In May 2013, China's DN3 reached 10,000 Km in space and release a barium cloud to study the magnetosphere. The US contradicted this and said that the rocket had a ballistic trajectory close to geosynchronous orbit in other words it was intended to knock out a target in a geostationary orbit by actually ramming it. Again in 2013, China conducted another ASAT test at an altitude above 30,000 km (almost reaching geosynchronous orbit). The US DoD labelled this new rocket as DN-2 and estimated that it may reach operational status by 2020-2025. It has also been reported that China has been developing *Kaituozhe* KT-1, KT-409, KT-2, KT2A, KT-3, and other KT versions of ASAT. China may have also been developing sea-based DA-ASAT like JL-2 Submarine Launched Ballistic Missile (SLBM) is said to have ASAT capability. Further, China may also have been developing air-launched DA-ASAT similar to US ASM-135 27 or Russian *Kontakt*.

***Dong Neng-1** (DN-1) **ASAT** missile must be operational in some numbers in the **PLA** inventory*



CHINA'S CO-ORBITAL ATTACK VEHICLES

Another form of Kinetic-ASAT is the use of Mini, Micro, Nano and Pico satellites which can weigh even less than 1 kg, it is defined as any object orbiting the earth that has a mass of about 10 kg. Although even a single stone can be as deadly as the satellite orbiting the Earth, such small satellites are primarily peaceful, they can be easily weaponised because of a satellite's high relative velocity to another satellite, any collision would destroy the targeted satellite(s), and micro-satellites have the advantage of being cheaper, more manoeuvrable and harder to track thus deception is possible.

In 2008 the BX-1 micro-satellite released by the People's Republic of China (PRC) passed dangerously close to the International Space Station (ISS) at a relative speed which would have destroyed both objects had they collided. This close call raised awareness of the PRC's ability to use micro-satellites as a kinetic-kill ASAT system. These systems are not acknowledged by the PRC as being strictly ASAT, but they are capable of destroying or disabling a satellite.

China has launched multiple satellites to conduct scientific experiments on space maintenance technologies and it is conducting space debris clean-up research. The US Defence Intelligence Agency (DIA) in February 2019 stated that *China is developing capabilities for inspection, repair, and space debris removal that may also be used as a weapon but did not specifically state that any Chinese co-orbital activities were a weapons test. It is reported that China's Shi Jian SJ-12, SJ-06F SY-7 and TJS-3 satellites have some sort of rendezvous capabilities*. In 2013, the Shiyan-7 (SY-7) released an object that performed manoeuvres and tested a telerobotic arm.

__China__ is developing capabilities for __inspection__, repair, and __space debris__ removal that may also be used as a __weapon__

In June 2016, the PLASSF launched the Aolong-1 spacecraft—which included a robotic arm—on a space debris-related mission. Between November 2016 and August 2018, the *Shi Jian*-17 carried out rendezvous and proximity operations with Chinese satellites in geostationary orbit, ostensibly for the purposes of monitoring space debris. In 2022, a Chinese *Shi Jian*-21 spacecraft docked with a defunct Beidou-2 navigation satellite and towed it into a graveyard orbit above the geostationary orbit.

Reportedly, the US and China have shown interest in developing a "Swarm of Satellites" and India is also planning to launch 20 Cube Satellite (CubeSat) Swarm in LEO for remote sensing mission. The weaponization of swarm satellites is well within reach of the present military space capabilities. China has launched some ten experimental Co-orbital (Aka. scavenger satellites).

The scavenger satellite is a technology which the European Space Agency (ESA) and the United States have been developing as well for Space Traffic Management (STM) for debris removal. They are also referred to as co-orbital "service" satellites which can be used for orbital satellite inspection and repair but they can be weaponised as they can be designed not to collide with their targets but to either manipulate their trajectory or physically damage them through interference by mechanical means such as robotic arms, thereby rendering the spacecraft inutile to its possessors without causing any debris. In 2019, French officials announced plans to study concepts such as swarms of nano-satellites that would patrol a few kilometres around French satellites, a ground-based laser system to blind snooping satellites, and perhaps even machine guns on board some satellites.

*The **U.S.** and **China** have shown interest in developing a "**Swarm of Satellites**" and **India** is also planning to **launch***

CHINA'S NON-KINETIC COUNTER-SPACE CAPABILITIES

Since physically destroying satellites generates debris, there is a greater emphasis on Soft-Kill techniques. As the chances of the usage of the Soft Kill Method are more in ASAT operations as compared to Hard Kill Method like Kinetic Attack. India will need to look beyond Hard Kill ASAT weapons. The Hard Kill Ability also known as a Conventional Kinetic Energy Weapon is simply a weapon which can have Hit-to-kill (HTK) ability or a proximity detonation to take the space-based asset out completely. Reportedly, China is also working on a non-nuclear Electromagnetic Pulse bomb which can be used as an ASAT weapon without creating a debris problem.

Non-nuclear EMP (NNEMP) has been the subject of substantial research and development (R&D) by the Chinese for developing usable weapons that can target rival electronics and electrical infrastructure both space and ground-based. As per US DIA report in 2022, *the PLA routinely incorporates in its exercises jamming and anti-jamming techniques that probably are intended to deny space-based communications, radar systems, and GPS*

navigation support to the military movement and precision-guided munitions.

TYPES OF NON-KINETIC ASAT WEAPONS

Non-lethal ASAT systems can act as a deterrent by providing a credible capability to disrupt or disable adversary satellites without causing permanent damage or generating space debris. Instead of resorting to irreversible destruction or generating space debris with the use of kinetic kill ASATs, non-lethal ASAT capabilities can be used to temporarily disrupt or disable adversary satellites, and for peacetime operations, the Non-lethal ASAT systems can contribute to Space Traffic Management by selectively targeting malfunctioning or derelict satellites, removing them from operational orbits, and reducing the risk of collisions.

1. **Laser dazzling:** Non-kinetic ASAT systems can use lasers to temporarily blind or "dazzle" optical sensors on satellites. This can impair the satellite's ability to gather visual information or track targets accurately, thereby affecting its operational capabilities.
2. **Jamming (EW):** Non-kinetic ASAT systems can involve jamming the communication signals of satellites. By emitting powerful radio frequency signals, the ASAT system can disrupt or block the satellite's ability to send or receive signals, rendering it ineffective or causing temporary communication loss.
3. **Spoofing:** Non-kinetic ASAT systems can employ spoofing techniques, where false signals are broadcasted to deceive or confuse the satellite's navigation or communication systems. By impersonating legitimate signals or providing incorrect information, spoofing can disrupt satellite operations and compromise their effectiveness.
4. **Cyberattacks:** Non-kinetic ASAT techniques can include launching cyberattacks against satellites' command, control, and communication systems. By exploiting vulnerabilities in the satellite's software or network infrastructure, hackers can disrupt operations, compromise control, or even take unauthorized control of the satellite.

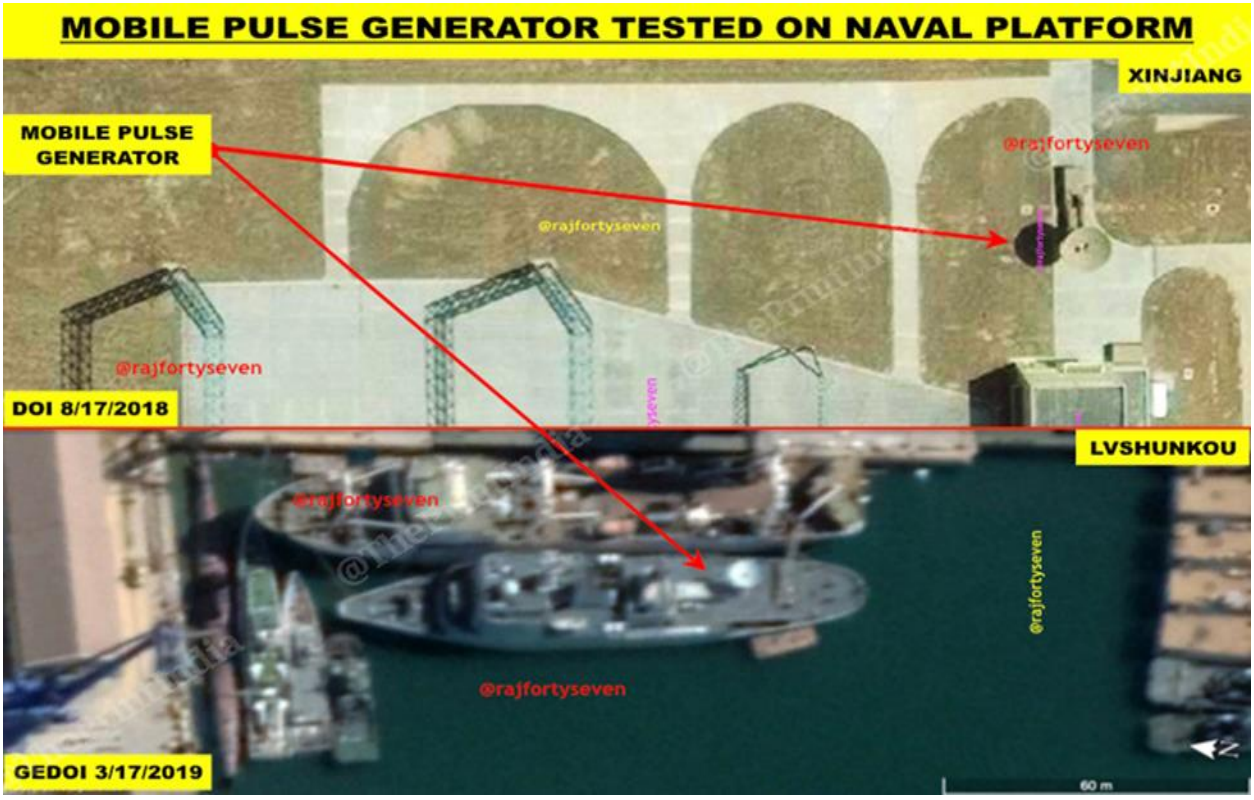
CHINA'S MICROWAVE SPACE-ATTACK CAPABILITIES

Unlike kinetic-kill vehicles, cleaner space kills would be through the development of microwave, EMP, or laser weapon systems. In the area of 'soft kill' techniques, China is trying to develop Directed Energy Weapon (DEW), which is a high-powered laser or microwave weapon designed to either disrupt or electrically damage a satellite. Reportedly, China's ally Russia has developed DEWs long-back during the Cold War period, weapons like the *Kalina*, *Peresvet*, and the *Zadira* laser dazzlers are in active service.

China has been working on ASAT DEW technology though no country has, so far, fielded an ASAT DEW system. Though, as reported that China's first tested a ground-based non-kinetic ASAT weapon even before the DN-1 kinetic-ASAT missile test, against a U.S. spy satellite in 2006. It is reported that China is developing DEW since 1995 and reportedly tested the same on orbiting US satellites in 2006. Laser Orbital Debris Removal (LDOR) to burn up in the debris in orbit as part of Space Traffic Management (STM) is possible solution for cleaner space, the LDOR was studied by NASA in the 1990s under *Project Orion* ASAT programme. An airborne system called

Sokol-Eshelon has been under development since 2001, *Sokol-Eshelon* is a Soviet/Russian laser weapon–based anti-satellite system. It is an airborne laser based on a Beriev A-60 aircraft.

The three main types of DEWs are lasers, particle beams and Radio Frequency (RF) energy of these, laser systems are the most developed and most prominent of the DEW counter-space threats. If China may choose to move towards the weaponisation of space then placing space-based ASAT DEWs in orbit has the advantage of not having to deal with atmospheric limitations but energy requirements to emit DEWs call for a heavy satellite with maximum energy generation on board. Whereas, ASAT DEWs placed on high-flying manned or unmanned platforms would also be less impaired by atmospherics, involve lower costs and be more amenable to upgrades compared to space-based DEWs. It was reported that China shall operationalise a ground-based DEW ASAT system by 2020 to target satellites in the LEO. In 2017, Chinese media celebrated the development of shipboard, a miniaturized microwave weapon that could evolve into an orbital anti-satellite system.

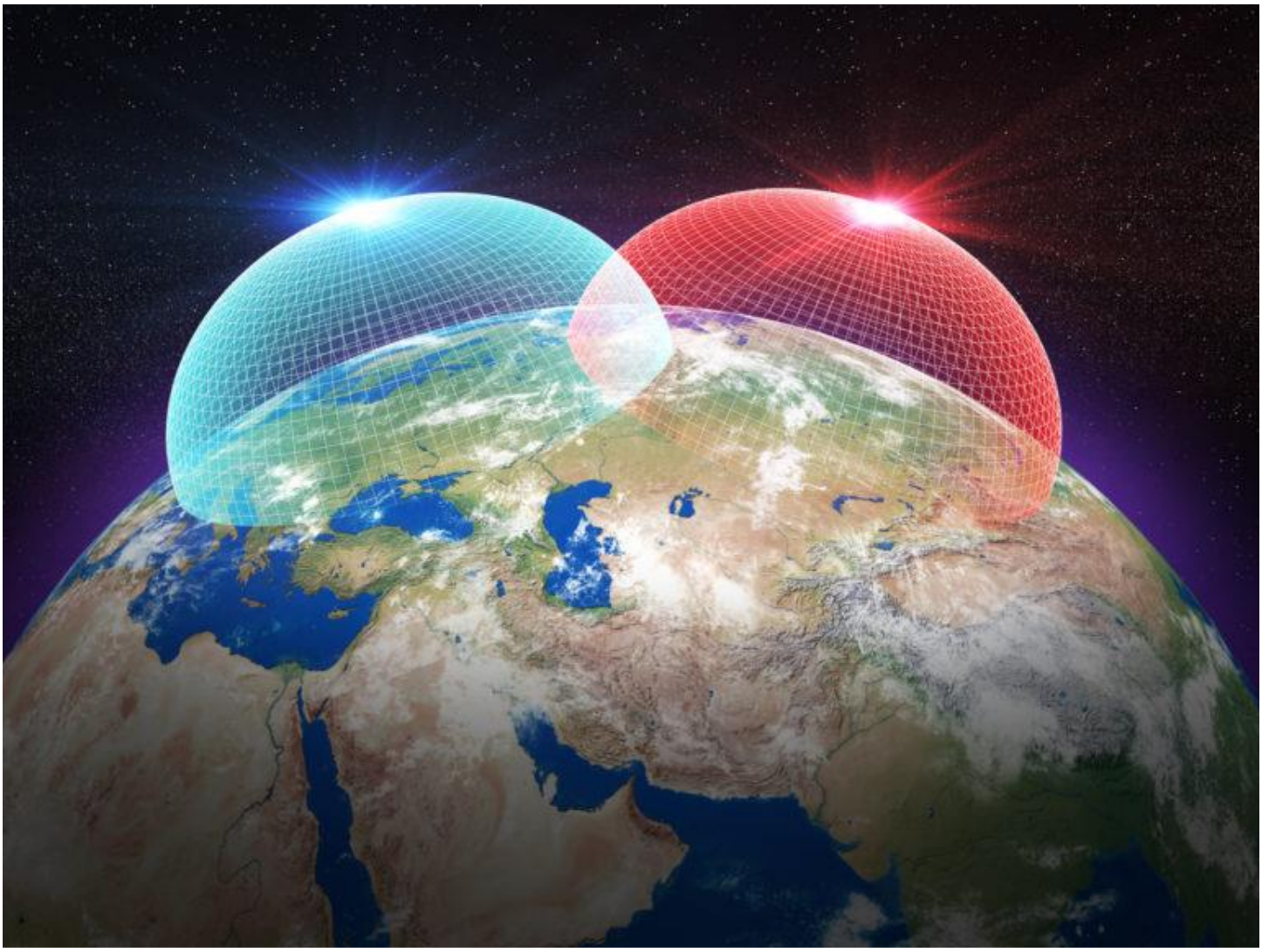


Chinese EMP experimental facility located in Xinjiang/ Col. Vinayak Bhat (Retd.)/The Print

Surveillance equipment – radio frequency or optical – fitted on military satellites can be rather jammed, blinding a satellite without a trace of emission. Take the case of an ELINT satellite - it can be overwhelmed with signals that it is painstakingly eavesdropping for SAR satellites can be similarly jammed with spurious radar returns, and optical sensors can be blinded with IR or Laser dazzling. Reportedly, an Advanced Electro-Optical System (AEOS) operated by the US Air Force (USAF) in Hawaii, has said to have satellite dazzling capability. Dazzling causes sensors to temporarily lose their imaging capability by swamping them with light that is brighter than what they are trying to image on the other hand blinding inflicts permanent damage to such systems. Shielding or shuttering the satellites against DEW is perhaps the simplest countermeasure, but this makes satellites heavier besides these reflective surfaces and non-absorbing materials have been proposed as a means of "hardening" against an attack by DEWs.

It is reported that China's EW experts have provided emphasis on developing High-Powered Microwave (HPM) Bombs deliverable through artillery shells, rockets, Ariel bombing, and missiles able to be used against terrestrial, maritime and space infrastructure. Zi Yang notes *Chinese technological maturity in the former, or an attempt to conceal advancements in the latter. Non-nuclear EMP (NNEMP) has been the subject of substantial Research and Development (R&D) that can target opponent electronics and electrical infrastructure*. It is believed that the Chung-Shan Institute of Science and Technology (CSIST) have been working on Non-nuclear EMP technology.

Dazzling *causes sensors to* ***temporarily*** *lose their imaging capability while* ***blinding*** *inflicts* ***permanent damage*** *to such systems*



CHINA'S SPACE ELECTRONIC COUNTERMEASURES (ECMS) CAPABILITIES

Under the 'Soft kill' method the threat to space assets can mostly come from jamming, spoofing, dazzling or blinding satellite sensors, communications, and command links using radio and or Surreptitious up-linking and commandeering, the ground-based space support infrastructure is equally susceptible to attack by various methods. The PLA has operationalised ground-based EW capabilities to disrupt SATCOM, navigation, SAR, missile early warning, and other satellites through the use of jamming. It is reported that PLA initially acquired ground-based satellite jammers from Ukraine in the late 1990s and has been trying to indigenously develop ground-based EW systems since then with an objective to disrupt, deny, deceive, or degrade space services. Jamming prevents users from

receiving intended signals and can be accomplished by attacking uplinks and downlinks. Following Russian advancement in EW systems, the PLA along with the industry have also been developing jammers capable of targeting satcoms over a large range of frequencies.

China is likely to have EW counter-space capabilities against US Global Navigation Satellite Space System (GNSS) and satellite communications, although the exact nature is difficult to determine through open sources. In April 2018, reports revealed satellite imagery indicating China had placed military jamming equipment on the Mischief Reef, part of the disputed Spratly Islands in the South China Sea. In January 2019, US Defence Intelligence Agency (DIA) space and the counter-space report states that *China is developing jammers dedicated to targeting SAR aboard military reconnaissance platforms, including LEO satellites, citing Chinese scientific papers describing the status of research and potential operational techniques*.

Satellite jammers with a 200-kilometre range have reportedly been available off-the-shelf for many years from the Russian company *Aviaconversiya*. A U.S. Landsat-7 earth observation satellite, built by NASA experienced 12 or more minutes of interference in October 2007 and July 2008 and another satellite Terra AM-1 earth observation satellite was similarly interfered with for two minutes or more on June 20, 2008. It is reported that China was behind these interferences. China is believed to already have much of the technology necessary to field an operational capability to dazzle or blind a satellite. It is said that it has already tested this capability on a U.S. satellite back in 2016. The US Space Force has been contending that the *US satellites are at the receiving end of the Chinese and Russian attacks through non-kinetic means, including lasers, radio-frequency jammers, and cyber-attacks, almost daily*.

***Satellite jammers** with a **200-kilometre range** have reportedly been available **off-the-shelf** for many years*

CHINA'S SPACE CYBER-ATTACK CAPABILITIES

Space assets are as vulnerable to cyber-attack as any other asset. A cyber-attack on satellites, ground centres and networks is a possibility in a potential conflict. However, targeting such a strategic sector can call for great diplomatic and international crises. Cyber-attack tools can also be used as ASAT. It is possible to seize control of a satellite by either gaining access to the network within a satellite control centres or by spoofing control signals using an independent uplink.

The SATCOM terminals typically have vulnerabilities – a backdoor, hard-coded credentials, undocumented and/or insecure protocols, and weak encryption algorithms – that allow a malicious actor to intercept, manipulate or block communications and in some cases, to remotely take control of the physical device. The transponder amplifies the carrier and transmits it back to a target area at a different frequency. A Denial-of-Service (DoS) attack on a communication satellite can be as simple as double illuminating a transponder.

Chinese electronics have further increased the chances of the presence of backdoors which can siphon the data or may lead to an attack. India imports almost 60% of its electronics from China as per some estimates. Several reports indicate that PLA cyberattack units under PLASSF can consist of an army of 50,000- 150,000 hackers besides over-the-ground cyber-attackers network.

There is a need for a resilient cyber capability to include a broad set of different tools and techniques aimed at exploiting ever-changing vulnerabilities in each layer of the infrastructure that underpins space access. Extant capabilities have demonstrated the capacity to produce a wide range of strategic and tactical effects, both kinetic and non-kinetic. These include theft, alteration, or denial of information, as well as control or destruction of satellites, their subcomponents, or supporting infrastructure. The cyber-attacks happen to the power grid, nuclear infrastructures and other strategic sectors on an almost everyday basis. **[End]**