May 2019 — Space Dossier 3

Electronic and Cyber Warfare **in Outer Space**

Rajeswari Pillai **Rajagopalan**

UNIDIR

Acknowledgements

Support from UNIDIR core funders provides the foundation for all of the Institute's activities. This project is supported by the Governments of People's Republic of China and the Russian Federation. The author thanks Kazuto Suzuki, Paul Meyer, John Borrie and Daniel Porras for their critical comments on drafts of this paper. Any views expressed and errors in the final paper are the author's own.

About the Author

Dr. Rajeswari Pillai RAJAGOPALAN is a Distinguished Fellow and Head of the Nuclear and Space Policy Initiative at the Observer Research Foundation (ORF) in New Delhi. She is also the Technical Advisor for a UN Group of Governmental Experts on Prevention of Arms Race in Outer Space (July 2018–July 2019). As the senior Asia defence writer for The Diplomat, she also writes a weekly column on Asian strategic issues. Rajagopalan joined ORF after a five-year stint at the National Security Council Secretariat (2003–2007), where she was an Assistant Director. Prior to joining the Secretariat, she was Research Officer at the Institute of Defence Studies and Analyses, New Delhi. She was also a Visiting Professor at the Graduate Institute of International Politics, National Chung Hsing University, Taichung, Taiwan in 2012. She is the author of four books: *Nuclear Security in India* (2015), *Clashing Titans: Military Strategy and Insecurity among Asian Great Powers* (2012), *The Dragon's Fire: Chinese Military Strategy and Its Implications for Asia* (2009), and *Uncertain Eagle: US Military Strategy in Asia* (2009). She has also co-authored and edited six other books, including *Space Policy 2.0: Commerce, Policy, Security and Governance Perspectives* (2017); *Nuclear Security in India* (2nd ed.) (2016); and *Iran Nuclear Deal: Implications of the Framework Agreement* (2015).

About UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR)—an autonomous institute within the United Nations—conducts research on disarmament and security. UNIDIR is based in Geneva, Switzerland, the centre for bilateral and multilateral disarmament and non-proliferation negotiations, and home of the Conference on Disarmament. The Institute explores current issues pertaining to a variety of existing and future armaments, as well as global diplomacy and local tensions and conflicts. Working with researchers, diplomats, government officials, NGOs and other institutions since 1980, UNIDIR acts as a bridge between the research community and Governments. UNIDIR activities are funded by contributions from Governments and donor foundations.

Note

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual authors. They do not necessary reflect the views or opinions of the United Nations, UNIDIR, its staff members or sponsors.

www.unidir.org

Contents

Acronyms

ASAT	anti-satellite
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
ITAR	International Traffic in Arms Regulations
ITU	International Telecommunication Union
OST	Outer Space Treaty
TCBMs	transparency and confidence-building measures
WMD	weapons of mass destruction

Key Findings

- The emergence of electronic and cyber counter-space capabilities is enabling a wider range of actors, including States and non-State actors to target and disrupt space objects, including both military and civilian satellites.
- These capabilities are already being used, targeting objects both in space and on the battlefield.
- The existing multilateral regulatory framework is insufficient to cope with the threat to space systems posed by electronic and cyber capabilities, requiring new measures that define norms of behaviour and rules of engagement with this technology. This paper concludes with some possible ways forward.

1 Introduction

An increasing reliance on space systems for national security and the simultaneous emergence of counter-space capabilities is making the space domain more competitive and contested than before. In particular, since anti-satellite (ASAT) demonstrations resumed in January 2007, there has been considerable competitive security pressure on States to demonstrate their own kinetic ASAT capabilities.[1] Fortunately, since then, ASAT demonstrations have not generated as much long-lived space debris. The recent Indian ASAT test, codenamed Mission Shakti, took place at an altitude sufficiently low enough that the debris will burn up in the atmosphere within weeks or months, as opposed to decades or even centuries.[2] However, there have been worrying trends in another facet of space security. States are moving away from expensive ASAT-like options (such as direct-ascent missiles) to developing more affordable and easily available electronic and cyber warfare methods that could affect space assets. Broadly, counter-space capabilities can be used to create temporary, as well as permanent, destruction of space assets. While kinetic systems create permanent and irreversible destruction of space assets, electronic and cyber means have created mostly temporary disruptions and damage to space systems thus far.

This paper outlines emerging technologies and capabilities in the electronic and cyber warfare domain as these pertain to outer space and how the international community might put in place mechanisms to prevent the potential destabilizing impact of such capabilities. Understanding existing counter-space capabilities could establish a sound basis for developing effective measures to address this challenge and prevent dangerous escalation. First, the paper briefly introduces counter-space capabilities and how they may differ from the Cold War era. The paper then describes different types of counter-space technology relating to electronic and cyber warfare in space. This includes descriptions of the technologies as well as instances of use. The third section looks at existing international measures to address counter-space capabilities. This section details the various treaties and export control regulations that apply to counter-space technologies, in addition to examining the gaps and weaknesses therein. The final section examines the requirement for more

[1] For debates within India, for instance, see R.P. Rajagopalan, "India's Changing Policy on Space Militarization: The Impact of China's ASAT Test", *India Review*, vol. 10, no. 4, 2011, pp. 354–378.
[2] R.P. Rajagopalan, "Having Tested its ASAT Capability, India Should Help Shape Global Space Norms", ORF Commentaries, 29 March 2019.

viable global mechanisms to address the growing threats from counter-space capabilities and proposes ways forward with regard to counter-space capabilities.

2 Counter-space capabilities

Counter-space capabilities “deprive an adversary of the benefits of space capabilities”.[3] Some analysts stipulate that they “involve anything that precludes an adversary from exploiting space to their advantage”.[4] However, this latter definition is far too broad and could include any possible means, including economic tools or technology transfer control regimes, to deny an adversary an advantage in space. Therefore, a modified definition is used in this paper to describe counter-space capabilities as military capabilities that seek to prevent “an adversary from exploiting space to their advantage”. These capabilities enable a space power to maintain “a desired degree of space superiority by the destruction or neutralization of enemy forces”.[5] States may conduct both offensive and defensive counter-space operations to achieve certain desired objectives.

Though counter-space capabilities have existed in the past, the conditions today are quite different, and States are demonstrating greater willingness to develop and use such capabilities. Kinetic capabilities, in which there is physical destruction of a space object, are difficult to hide from the international community, though it can be difficult to determine attribution for destruction. However, electronic and cyber attacks are much harder to detect because it is difficult to distinguish between non-intentional failure or malfunction. More important, such capabilities can be developed and deployed or even used without detection. In fact, as will be shown below, such attacks are already taking place.

It is worth examining how the current situation and threats compare to the Cold War era.[6] The biggest change from then to now is in terms of the increased number and types of actors involved in space. This is a considerable difference from Cold War space competition when the two space superpowers, the United States and the Soviet Union, dominated the space domain. The growing participation of commercial actors makes space a more innovative environment, which in turn makes access to outer space cheaper for governmental and private actors alike. At the same time, it makes space more crowded and congested.

In addition, there is a significant difference in the way States approach outer space even within the security context. During the Cold War, outer space utilization was primarily for strategic operations, such as strategic intelligence gathering, nuclear attack early warning and executing arms control agreements.[7] This scenario has changed and space today has a far more important role to play in conventional military operations. Offensive or defensive counter-space operations today would impact not just the security sector but also social and economic sectors across continents because of large-scale civilian dependency on space-based applications. The fact that space is vital to both civilian and military operations heightens the danger of inadvertent escalation and conflict if there is, for instance, a disruption or denial of service during a period of heightened tensions, even if the incident was a natural incident or due to mechanical failure.

[3] Foreword by Gen. J.P. Jumper, Chief of Staff, US Air Force, *Air Force Doctrine Document 2-2.1*, 2 August 2004.

[4] J.B. Sheldon, “Threats to Security in Space from Counter-Space Technologies”, ASEAN Regional Space Security Workshop, Hoi An, Vietnam, 6–7 December 2012, http://aseanregionalforum.asean.org/files/Archive/20th/ARF%20Workshop%20on%20Space%20Security,%20Hoi%20An,%206-7December2012/Annex%205%20-%20Space%20Security.pdf.

[5] Air Force Doctrine Document 1, *Air Force Basic Doctrine*, September 1997, p. 47.

[6] For a good account on the US and Soviet Cold War space competition, see T. Brown, “The American and Soviet Cold War Space Programs”, *Comparative Strategy*, vol. 30, no. 2, 2011, pp. 177–185.

[7] B. Weeden and V. Samson (eds), *Global Counterspace Capabilities: An Open Source Assessment*, Secure World Foundation, April 2018, https://swfound.org/media/206118/swf_global_counterspace_april2018.pdf.

However, there are some similarities to the Cold War period. First, there is renewed emphasis on hard power capabilities, including in outer space. For example, since 2007, several States have begun to test ASAT capabilities, after an unofficial moratorium that lasted for more than two decades. Another indication of the renewed competition is the setting up of dedicated space forces such as by the United States and plans for a similar force by France.

Second, balance-of-power dynamics are impacting outer space: space has become another domain where terrestrial politics and competition are playing out. For example, the military competition between India and China is finding a reflection in the space race between the two States.[8] This is important in the context of 'counter-space' discussions because many States today are approaching space from a security perspective, relying on outer space to strengthen their strategic and national security capabilities. For example, many more States today rely on outer space for military communications than during the Cold War. This is especially true as greater dependence on outer space for military operations leaves States vulnerable to a range of counter-space operations.

Third, there appears to be a greater willingness to engage in the development and possible use of new offensive counter-space capabilities than those available during the Cold War era. Competition between major space powers has led to a rise in the number of instances where electronic and cyber warfare capabilities are used (these are detailed in subsequent sections). Moreover, regional and global security competition is a likely driver for a space arms race as major spacefaring powers seek new military space capabilities. Some of the norms that have existed are being challenged because newer actors seem less bound by them. While the norm to not test ASATs is seldom breached, there are indications that other norms, such as non-interference in satellite operations, is weakening. Norms are likely to be broken when many new players enter an established field. Norms can be effective when players are committed to upholding the rules but break down when the rules are seen as a hindrance to maintaining an advantage. The erosion of norms is further aided by the changes in technology and political context, like the widespread availability of cyber warfare technologies combined with a heightened sense of competition driven by geopolitical dynamics.

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

3 Types of counter-space technology

There are four types of counter-space capabilities: kinetic physical, non-kinetic physical, electronic and cyber.[9]

Kinetic physical operations and capabilities cause permanent and irreversible destruction of a satellite or to ground support infrastructure through force of impact by an object or detonation of a warhead. These technologies include direct-ascent ASAT missiles and co-orbital systems. ASATs are essentially meant “to destroy hostile satellites through the sheer use of high speeds and kinetic energy on impact”.[10] Co-orbital systems are satellites placed on similar orbits and can be directed to intercept or interfere with other satellites through close orbital rendezvous operations.

Non-kinetic physical operations involve the use of technology to interfere with or damage space systems[11] without physical contact. Technologies in this category include electromagnetic pulses or directed energy (laser beams or microwave bombardments).

A third type is electronic warfare capabilities, using radiofrequency energy to interfere with or jam communications to or from satellites but which do not cause permanent physical damage. The last category is cyber warfare technologies which use software and network techniques to compromise, control, interfere or destroy computer systems linked to satellite operations.

As will be shown below, use of electronic and cyber means have become preferred methods of attack since their use can be plausibly denied. These counter-space capabilities can be used to deny, degrade, disrupt, or destroy space systems. What is more, the requisite technology for electronic and cyber warfare is becoming ubiquitous and diverse, accessible even to non-State actors.[12] This dossier will focus on electronic and cyber warfare capabilities in outer space.

3.1 ELECTRONIC WARFARE CAPABILITIES

Electronic warfare involves the use of electromagnetic pulses or directed energy (laser beams or microwave-bombardments) to deny, degrade or disrupt satellite systems. These capabilities cause temporary damage or disruption to a satellite or service without physically contacting the satellite.

[9] T. Harrison, K. Johnson and T.G. Roberts, *Space Threat Assessment 2018*, Center for International and Strategic Studies, April 2018, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180823_Harrison_SpaceThreat Assessment_FULL_WEB.pdf.

[10] B.S. Kuplic, “The Weaponization of Outer Space: Preventing an Extraterrestrial Arms Race”, *North Carolina Journal of International Law and Commercial Regulation*, vol. 39, no. 4, 2014, https://scholarship.law.unc.edu/cgi/viewcontent.cgi?referer=https://www.google.co.in/&httpsredir=1&article=2011&context=ncilj.

[11] It should be noted that a space system can come under attack in five different segments: launch, the control segment, the up-down link segment, the user segment and the space segment. John B. Sheldon, “Threats to Security in Space from Counter-Space Technologies,” ASEAN Regional Space Security Workshop, Hoi An, Vietnam, 6–7 December 2012, http://aseanregionalforum.asean.org/files/Archive/20th/ARF%20Workshop%20on%20Space%20Security,%20Hoi%20An,%206-7December2012/Annex%205%20-%20Space%20Security.pdf

[12] J.B. Sheldon, “Threats to Security in Space from Counter-Space Technologies”, ASEAN Regional Space Security Workshop, Hoi An, Vietnam, 6–7 December 2012, http://aseanregionalforum.asean.org/files/Archive/20th/ARF%20Workshop%20on%20Space%20Security,%20Hoi%20An,%206-7December2012/Annex%205%20-%20Space%20Security.pdf.

Electronic warfare is “military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy”.[13] Global Positioning System (GPS) satellites have proven to be particularly vulnerable to jamming as it blocks users from acquiring useful and accurate positioning, navigation and timing data from those satellites. But the jamming of navigation satellites is primarily restricted to civil GPS signals, as military signals are more robust.[14] Given large-scale global dependence on GPS data, it has emerged as an easy target to cause widespread disruption. Such actions, if they are not controlled through new rules or norms, could reduce the utility of outer space for providing services. It could also lead to a general dilution of the norms of behaviour in outer space, increasing security competition that could have longer term impact on the peaceful utilisation of space.

However, analysts believe that effective counter-systems could be developed and executed to “geolocate and characterize enemy jammers”, making enemy systems vulnerable to destruction and damage. Enemy electronic systems “could be destroyed, avoided, and negated via adaptive, real-time filtering or otherwise defeated by other electronic protection tactics like increasing transmitter power”.[15] This suggests that spacefaring powers will employ a variety of electronic tactics, which will give way to development of more counter-measures in the coming years. Such developments could make the outer space domain a lot more competitive and vulnerable.

3.1.1 Technology description

Satellites are controlled from ground stations through electronic signals and they pass their data back to ground stations, so attacking those uplink and downlink linkages electronically can render satellites ineffective.[16] Electronic attacks are usually done by targeting the signals, either through jamming or spoofing.

Jamming is a kind of electronic attack that interferes with radiofrequency communications by creating noise in the same frequency band and within the field of view of the antenna of the satellite or receiver it is targeting, thus disrupting communications. [17] Jamming causes temporary disturbance and disruption and is thus reversible. Once the jammer is turned off, the communication can return to normal. A number of different jamming options are available including proactive, function-specific or hybrid-smart jamming to produce the most effective results.[18]

Spoofing is another form of electronic attack where a fake signal is produced by the attacker’s device. In this case, if the spoofing attack targets the downlink data from a satellite to the ground, it could end up feeding false or corrupt data into the ground receiver system. Hijacking a satellite command and control and feeding it such data are well-known means of disruption. Upon a

[13] US Department of Defense, “DOD Dictionary of Military and Associated Terms”, *Defense Technical Information Center*, September 2018, http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2018-09-28-100314-687.

[14] B. Weeden: “Two points: 1) this is all about civil GPS signals (military signals are much more robust) 2) the DOD could have done more to prevent spoofing of civil GPS, but has not 3) Galileo, BeiDou & QZSS will all help, but not prevent it completely (see #2)”, 18 December 2018, https://twitter.com/brianweeden/status/1074787323357876229.

[15] L. Bonner, “Defending Our Satellites: The Need for Electronic Warfare Education and Training”, *Air & Space Power Journal*, November–December 2015, https://www.airuniversity.af.mil/Portals/10/ASPJ/journals/Volume-29_Issue-6/SEW-Bonner.pdf.

[16] Ibid.; T. Harrison, K. Johnson and T.G. Roberts, *Space Threat Assessment 2018*, Center for International and Strategic Studies, April 2018, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180823_Harrison_SpaceThreatAssessment_FULL_WEB.pdf.

[17] Ibid.

[18] K. Grover, A. Lim, and Q. Yang, “Jamming and Anti-Jamming Techniques in Wireless Networks: A Survey”, *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 17, no. 4, http://www.cs.montana.edu/yang/paper/jamming.pdf.

successful spoofing of a command and control system of a satellite, the attacker could control the satellite and use it to conduct nefarious activities. Spoofing too is quite inexpensive and thus can be developed and deployed by many actors, including non-State actors.

Lasers have also been used to blind reconnaissance satellites and have been found to be quite successful. This is called dazzling, and several States are reported to be investing in this capability.[19] But there are others who argue that the power requirements for significant effects still renders many of these systems problematic in terms of actual performance.

3.1.2 Instances of use

Open source reports indicate that all the major spacefaring nations have some form of offensive electronic warfare capabilities for outer space systems, although there may be differences in terms of technological sophistication. The following is a non-exhaustive (and non-verified) list of capabilities or instances where offensive electronic warfare means were reportedly used in the last two decades (in chronological order):

- The United States has an operational electronic warfare system, the Counter Communications System, that is deployable across the globe to undertake uplink jamming against geostationary communication satellites and was operationalized in 2004.

- According to reports, the United States may have the technical capacity to undertake jamming of Global Navigation Satellite System (GNSS) receivers, such as GLONASS or Beidou, in a small restricted area of operation to avoid those systems being used by adversaries.

- According to some reports, "several Chinese scientists claimed to have successfully blinded a satellite in a 2005 test using a '50-100 [kilowatt] capacity mounted laser gun in Xinjiang province'".[20]

- In an incident in 2006, China reportedly made efforts to blind US spy satellites flying over Chinese territory using high-powered lasers although it is not clear whether it was successful or not.[21] While these incidents have not been corroborated through publicly available information, US officials claim that China has this capability and has "exercised it".[22]

- In 2009, there were reports of the Islamic Republic of Iran engaging in electronic warfare activities. In a specific case, the Islamic Republic of Iran was accused of jamming certain news broadcasts such as that of BBC's Persian TV in order to prevent Western media from reaching

[19] B. Sutherland, "Militarising Space", in B. Sutherland (ed.), *Modern Warfare, Intelligence and Deterrence: The Technologies That Are Transforming Them*, 2014, pp. 142–143; P.C. Saunders and C.D. Lutes, "China's ASAT Test Motivations and Implications", National Defense University, Institute for National Strategic Studies, Washington DC, 2007, http://www.dtic.mil/dtic/tr/fulltext/u2/a517485.pdf; P.C. Saunders, "China's Future in Space: Implications for US Security", Space.com, 24 May 2005, http://www.space.com/1116-chinasfuture-space-implications-security.html.

[20] See R.D. Fisher Jr., "China's Progress with Directed Energy Weapons", testimony before the US–China Economic and Security Review Commission, 23 February 2017, https://www.uscc.gov/sites/default/files/Fisher_Combined.pdf.

[21] See V. Muradian, "China Tried to Blind US Sats with Laser", *Defense News*, 25 September 2006, https://www.ar15.com/forums/general/Chi-na_Tried_To_Blind_U_S__Sats_With_Laser/5-501978/.

[22] See F. Harris, "Beijing Secretly Fires Lasers to Disable US Satellites", *The Telegraph*, 26 September 2006, https://www.telegraph.co.uk/news/worldnews/1529864/Beijing-secretly-fires-lasers-to-disable-US-satellites.html.

domestic viewers. This jamming was evident during coverage of the 2009 Iranian presidential elections and the 2011 Arab Spring revolts.[23]

- According to reports, the Islamic Republic of Iran has repeatedly interfered with commercial communications satellites' ability to broadcast Persian-language programmes in the country over the last several years.

- In 2011, Tehran brought down a US RQ-170 UAV, "by jamming its satellite communications links and spoofing the GPS signals it received". These claims were not confirmed by the US government.[24]

- Between 2010 and 2012, the Democratic People's Republic of Korea was accused of jamming the Republic of Korea's GPS signals for days at a time, affecting many planes, ships and personal devices.[25]

- The Russian Federation is reported to have completed the development of a laser-based ASAT on the A-60 aircraft, designated 1LK222 Sokol Eshelon. These laser-based systems can both dazzle and blind sensors on satellites. With sufficient power, they are capable of damaging light- or heat-sensitive physical components on satellites.[26]

- According to reports, the Russian Federation has also developed two jammers, designated the R-330Zh and R-381T2. These two, along with four other jamming systems, were reported to have been used to jam GPS signals in Ukraine in 2014.[27]

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

[24] See S. Peterson and P. Faramarzi, "Exclusive: Iran Hijacked US drone, Says Iranian Engineer", *The Christian Science Monitor*, 15 December 2011, https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer. In another specific incident reported by Christian Science Monitor in 2011, according to an unnamed European intelligence source, Iran had "managed to 'blind' a US satellite by 'aiming a laser burst quite accurately'"; see T. Harrison, K. Johnson and T.G. Roberts, *Space Threat Assessment 2018*, Center for International and Strategic Studies, April 2018, p. 32, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180823_Harrison_SpaceThreatAssessment_FULL_WEB.pdf.

[25] "DPRK Jamming GPS Signals, says Seoul", *North Korea Tech*, 3 May 2012, http://www.northkoreatech.org/2012/05/ 03/dprkjamming-gps-signals-says-seoul/; "'North Korea Jamming' Hits South Korea Flights", *BBC News*, 2 May 2012, http://www.bbc.com/news/world-asia-17922021; S. Waterman, "North Korean Jamming of GPS Shows System's Weakness", *The Washington Times*, 23 August 2012, http://www.washingtontimes.com/news/2012/aug/23/ northkorean-jamming-gps-shows-systems-weakness/?page=all.

[26] See T. Harrison, K. Johnson and T.G. Roberts, *Space Threat Assessment 2018*, Center for International and Strategic Studies, April 2018, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180823_Harrison_SpaceThreat Assessment_FULL_WEB.pdf; A. Mathew, "Russia Completes Development of Airborne Anti-satellite Laser Weapon", *DefPost*, 26 February 2018, https://defpost.com/russia-completes-development-airborne-anti-satellite-laser-weapon/; D. Cenciotti, "Russia Has Completed Ground Tests of Its High-Energy Airborne Combat Laser System", *The Aviationist*, 5 October 2016, https://theaviationist.com/2016/10/05/russia-has-completed-ground-tests-of-its-high-energy-airborne-combat-laser-system/; "The Russian Plane with Laser Weapons Successfully Passed the Ground Tests", (Russian media), October 5, 2016 (only available in Russian), https://tvzvezda.ru/news/opk/content/201610051309-vplh.htm

[27] See T. Harrison, K. Johnson and T.G. Roberts, Space Threat Assessment 2018, Center for International and Strategic Studies, April 2018, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180823_Harrison_Space Threat Assessment_FULL_WEB.pdf.

- According to a Russian defence industry source reported in Sputnik, the Russian Federation is building a new electronic warfare aircraft that can disable enemy navigation and communication satellites.[28]

3.2 CYBER WARFARE CAPABILITIES

Like electronic warfare technologies, cyber warfare measures are fast emerging as a viable option for space warfare because they are cheap and easily accessible. Several States, including less advanced ones, have been able to develop cyber warfare capabilities that could interfere with outer space systems and satellite functioning, yet the number of reported incidents of use are few. Many, including the the United States, the Russian Federation, China, and the Democratic People's Republic of Korea, have demonstrated their capabilities and willingness to carry out cyber attacks against non-space targets. While satellites are attractive targets, an attack on them could have serious unintended consequences and has the potential to lead to serious conflict. Moreover, commercial space satellites may be more vulnerable compared to military assets.[29]

Cyber warfare capabilities could become a larger challenge in the coming years for a number of reasons. A basic, crude cyber capability is more easily accessible than other kinetic counter-space capabilities. It can be developed and deployed much faster than an ASAT and is much cheaper. The entry barrier for these technologies is fairly low, with many independent hackers available. The deniability factor and difficulty in attribution also makes cyber measures a perfect way to create massive disruptions and damage to space systems. In 2017, a senior US military official went on record to state that cyber attacks are the "No. 1 counter-space threat".[30] The Director of US National Intelligence, James R. Clapper, made similar observations.[31]

3.2.1 Technology description

Cyber warfare techniques directly attack data and the systems that use data. The more satellites are linked to cyber nodes, the more vulnerable these are to cyber attacks. There are several points of intrusion for an attacker, including the landlines that link ground stations to terrestrial networks, user terminals that link satellites, and antennas on satellites and ground stations.[32] Cyber attacks can be crude or sophisticated, depending on the level of disruption and destruction sought by the attacker. If the intent is more to send a message to an adversary that one has the capability and the capacity to inflict punishment, the attack need not be too disruptive. But cyber attacks are capable

[28] See "Source Reveals Tech Details of New Russian Anti-Satellite Warfare Plane", *Sputnik*, 9 July 2018, https://sputniknews.com/military/201807091066176858-russia-electronic-warfare-plane-satellites/.

[29] "Cybersecurity and the New Era of Space Activities", Council on Foreign Relations, 3 April 2018, https://www.cfr.org/report/cybersecurity-and-new-era-space-activities; G. Falco, "Job One for Space Force: Space Asset Cybersecurity", Belfer Center for Science and International Affairs, July 2018, https://www.belfercenter.org/sites/default/files/files/publication/CSP%20Falco%20Space%20Asset%20-%20FINAL.pdf/.

[30] K. Pollpeter, "Testimony Before the US-China Economic and Security Review Commission: Hearing on China's Advanced Weapons", CNA, February 2017, https://www.cna.org/CNA_files/PDF/CPP-2017-U-014906-Final.pdf; D. Coats, "Statement for the Record—Worldwide Threat Assessment of the US Intelligence Community", Office of the Director of National Intelligence, 13 February 2018, https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.

[31] J.R. Clapper, statement before the US Senate Select Committee on Intelligence, "Worldwide Threat Assessment of the US Intelligence Community, Senate Select Committee on Intelligence", 9 February 2016, https://www.dni.gov/files/documents/SSCI_Unclassified_2016_ATA_SFR%20_FINAL.pdf.

[32] T. Harrison, K. Johnson and T.G. Roberts, *Space Threat Assessment 2018*, Center for International and Strategic Studies, April 2018, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180823_Harrison_SpaceThreatAssessment_FULL_WEB.pdf.

of creating large-scale disruptions or even permanent damage to a space system. If an adversary manages to get hold of the command and control of a satellite, for instance, it could possibly "shut down all communications and permanently damage the satellite by expending its propellant supply or damaging its electronics and sensors".[33] Interference with communication satellites could affect the operational integrity of military operations in addition to creating disruptions with capabilities that are used for airline safety, security and cargo vessels in the high seas.[34]

Though cyber means are relatively new ways of interfering in satellite operations, there are older methods such as radiofrequency interference that can also create problems. Because satellites are controlled by radio waves, interfering with these connections through fake transmissions or spoofing represents another danger that broadly falls within the electronic warfare spectrum but distinct from cyber attacks.

Cyber attacks are a more direct form of attack than electronic warfare measures which target the transmitting radiofrequency signals. Cyber attacks also call for more sophisticated capabilities and expertise, but the availability of large numbers of independent hackers provides a possible source for building these.[35] States are free to subcontract operations to mercenary individuals or groups, while maintaining deniability. Currently, States can conduct a range of attacks, creating tactical and strategic impacts on the affected parties through "theft, alteration, or denial of information, as well as control or destruction of satellites, their subcomponents, or supporting infrastructure ".[36] With a greater number of space programmes using "more advanced on-board processing, all digital components, software-defined radios, packet-based protocols, and cloud-enabled high performance computing, the attack surface for cyber-attacks is likely to increase".[37]

3.2.2 Instances of use

Open-source reports indicate that many States possess cyber warfare capabilities against outer space assets but the number of openly acknowledged and verified incidents are few. The following is a list of instances where cyber warfare means were reportedly used (in chronological order):

- In 2011, a report by the US–China Economic and Security Review Commission reported that two US satellites had been compromised in 2007 and 2008 through a ground station in Norway. The attack, carried out via the internet, was traced to China. Though the US Government did not accuse anyone outright, it did say that the nature of the attack was linked to Chinese hackers and that it was consistent with policy documents published by China's military. The severity of the attack was especially alarming because, at least in the 2008 attack, the hackers were able to achieve all steps required to command the satellite,

[33] A. Gini, "Cyber Crime from Cyber Space to Outer Space", *Space Safety Magazine*, 14 February 2014, http://www.spacesafetymagazine.com/aerospace-engineering/cyber-security/cyber-crime-cyber-space-outer-space/; T. Harrison, K. Johnson and T.G. Roberts, Space Threat Assessment 2018, Center for International and Strategic Studies, April 2018, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180823_Harrison_SpaceThreat Assessment_FULL_WEB.pdf.

[34] R. Santamarta, "A Wake-up Call for SATCOM Security", *Technical White Paper*, IOActive, 2014, http://www.ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf.

[35] R. Pollock, "These Are The Hacker Groups Everyone Is Watching Right Now", *The Daily Caller*, 9 July 2015, http://dailycaller.com/2015/07/09/these-are-the-hacker-groups-everyones-watching-right-now/.

[36] B. Weeden and V. Samson (eds), Global Counterspace Capabilities: An Open Source Assessment, Secure World Foundation, April 2018, https://swfound.org/media/206118/swf_global_counterspace_april2018.pdf.

[37] A. Gini, "Cyber Crime from Cyber Space to Outer Space", Space Safety Magazine, 14 February 2014, http://www.spacesafetymagazine.com/aerospace-engineering/cyber-security/cyber-crime-cyber-space-outer-space/; and B. Weeden and V. Samson (eds), Global Counterspace Capabilities: An Open Source Assessment, Secure World Foundation, April 2018, https://swfound.org/media/206118/swf_global_counterspace_april2018.pdf.

though no harm was done. Potentially, the hackers could have stolen data, redirected the solar panel array in ways that would result in damage, or even moved the satellite.[38]

- In 2014, the US National Oceanic and Atmospheric Administration confirmed that one of its satellites had been hacked. Though none of its data was compromised, published news reports blamed China.[39]

- A group of Russian-speaking hackers, with possible links to the Russian government, has been reported to be using malware named Turla for attacks on communication satellites that use unencrypted data links.[40]

- In October 2018, the US National Aeronautics and Space Administration was hacked and personal data of current and former employees were found to be compromised. However, none of the Administration's missions seem to have been compromised.[41]

[38] J. Wolf, "China Key Suspect in U.S. Satellite Hacks: Commission", *Reuters*, 28 October 2011, https://www.reuters.com/article/us-china-usa-satellite-idUSTRE79R4O320111028.

[39] "Chinese Military Suspected in Hacker Attacks on US Satellites", *Bloomberg*, 27 October 2011, http://www.bloomberg.com/news/articles/2011-10-27/chinese-military-suspected-in-hacker-attacks-on-u-s-satellites; "China Denies It Is Behind Hacking of US Satellites", *Reuters*, 31 October 2011, http://www.reuters.com/article/ 2011/10/31/us-china-us-hacking-idUSTRE79U1YI20111031; L. Johnson, "Sky Alert: When Satellites Fail", 2013, p. 37; M.P. Flaherty, J. Samenow, and L. Rein, "Chinese Hack US Weather Systems, Satellite Network", *Washington Post*, 12 November 2014, http://www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellitenetwork/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e_story.html.

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

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

4 Current measures and their effectiveness in addressing counter-space capabilities

The renewed emphasis on space and counter-space capabilities has called into question the effectiveness of the outer space regime. As will be discussed in this section, there are several treaties and agreements that have successfully regulated outer space activities so far. However, there are gaps that need to be addressed to strengthen the effectiveness of the existing global mechanisms.

This section will examine four global mechanisms—the Outer Space Treaty, the Charter of the United Nations, International Telecommunication Union Radio Regulations, and export controls. These existing governance mechanisms do not address non-kinetic attacks.

4.1 OUTER SPACE TREATY

The Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (referred to as Outer Space Treaty, or OST) is the foundational treaty regulating outer space activities. Article IX is pertinent to the debates on non-interference in the peaceful activities of State Parties. The article says, "If a State Party to the Treaty has reason to believe that an activity or experiment planned by it or its nationals in outer space, including the moon and other celestial bodies, would cause potentially harmful interference with activities of other States Parties in the peaceful exploration and use of outer space, including the moon and other celestial bodies, it shall undertake appropriate international consultations before proceeding with any such activity or experiment". Similarly, if the State Party that is engaged in a certain activity that might cause harmful interference does not establish consultations, then the second party who will be affected by the harmful interference has a right to ask for consultation. There is a prohibition on "harmful interference" and more importantly, there is also presumption of prior consultation, however to date this has not been utilized.

Though the OST is quite comprehensive, there are gaps that need to be addressed. The Treaty has maintained the sanctity of outer space so far due to several factors, the most important of which is that it prohibits the placement of weapons of mass destruction (WMD) in outer space. But this also represents a significant gap as the OST does not explicitly ban weapons other than WMDs in outer space. This is increasingly being interpreted to suggest that "non-WMD armaments in space do not violate international law".[42] Many scholars attribute this to the somewhat indifferent attitude on the part of established spacefaring powers to the emerging trend towards weaponization of outer space.[43] Whether non-weapons of mass destruction are prohibited or not, customary international law might still forbid them and consider weaponization of outer space as illegal. Recent developments, such as kinetic ASAT tests in outer space, suggest this is not likely. Another limitation is that forbidding weapon placement in space does not necessarily forbid use of weapons in space such as ASATs.

Secondly, differences in States' interpretations of key terms such as 'peaceful use of outer space' also raise challenges for the continued effectiveness of the OST. Some States interpret 'peaceful

[42] B.S. Kuplic, "The Weaponization of Outer Space: Preventing an Extraterrestrial Arms Race", *North Carolina Journal of International Law and Commercial Regulation*, vol. 39, no. 4, 2014, https://scholarship.law.unc.edu/cgi/viewcontent.cgi?referer=https://www.google.co.in/&httpsredir=1&article=2011&context=ncilj.

[43] C. Peoples (2008) "Assuming the Inevitable? Overcoming the Inevitability of Outer Space Weaponization and Conflict", *Contemporary Security Policy*, vol. 29 no. 3, 2008.

uses of outer space' as constituting 'non-military' uses while others consider it to refer to 'non-aggressive' behaviour. Such differences constrain the effectiveness of the OST as it could limit its mandate over electronic and cyber warfare aspects in outer space.

In the context of this paper, it is important to note that broad interpretations of permissible activities in outer space allows for electronic warfare and cyber warfare technologies to be developed and used. Lack of clarity and different interpretations of key concepts like 'peaceful use', 'defensive use' and 'space weapon' represent a challenge for the OST. An additional danger is that lack of consensus on these key terms may encourage States to move towards the broader interpretation, because of fear that other States may have already done so.

4.2 CHARTER OF THE UNITED NATIONS

Article III of the Outer Space Treaty has a direct reference to the Charter of the United Nations, wherein it states that all States Parties "carry on activities in the exploration and use of outer space, including the moon and other celestial bodies, in accordance with international law, including the Charter of the United Nations, in the interest of maintaining international peace and security and promoting international cooperation and understanding".

Provisions in the UN Charter on the general use of force (art. 2.4) are relevant here because it says that "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."". This would then include all and any use force and aggression in outer space under the UN Charter mandate.

Article 51 of the UN Charter deals with the right to individual or collective self-defence in the case of an armed attack. There are on-going debates on the right to self-defense defence and defining acts of aggression, which are discussed in a subsequent section in the paper.

While the Charter remains relevant in the outer space debates, the general provisions of the Charter have had little effect in limiting terrestrial international competition, suggesting that by themselves, these provisions are unlikely to curtail competition in outer space. Definitional issues are a particular problem because the Charter does permit self-defence, implying that States can develop capabilities to that end.

Similarly, definitional problems also arise about what constitutes an act of aggression. Under the Charter, article 39 gives a role to the Security Council in determining a threat to peace or an act of aggression.[44] Given the possibly subjective nature of interpretation of threat to peace or aggression, General Assembly resolution 3314 of 1974 is also used to explain what an aggression is. The resolution reads, "Aggression is the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations, as set out in this Definition".[45] Article 3 of the resolution lists a few instances to indicate what might constitute an act of aggression, but article 4 makes it clear that it is not an exhaustive list and that the Security Council still can determine what might constitute an act of aggression.

These ambiguities become particularly acute when dealing with cyber and electronic warfare because of the difficulty of tracing the source of both cyber and electronic attacks. States can also

[44] Article 39 reads, "The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression".

[45] General Assembly, "Text of UN General Assembly Resolution 3314", 14 December 1974, http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/3314(XXIX)&Lang=E.

engage in probing electronic and cyber defences of potential adversaries but it is unclear if this would constitute an actual attack, a problem that becomes even more serious if non-State actors are employed to front such attacks. There have been several accusations of cyber attacks for which proving the source of the attacks has been difficult. Beyond strengthening cyber and electronic defences, it is unclear how States subject to such attacks can respond in a manner that would be considered legitimate under international law, what level of proof is required before a response, and what might constitute proportionality in such responses.

The presence of non-State actors further complicates these issues because it is unclear if an attack on a non-State actor, such as a private corporation, constitutes an attack by one State on another. This issue becomes even more complicated when considering attacks on satellites owned and operated by private industry which may have complex shareholding structures.

4.3 INTERNATIONAL TELECOMMUNICATION UNION RADIO REGULATIONS

The Radio Regulations of the International Telecommunication Union (ITU) are the basic documents of the ITU. The Radio Regulations along with the ITU Constitution and Convention enunciate the main principles and specific regulations for the registration of satellite network frequency assignments. The Radio Regulations, revised partially or fully in exceptional circumstances, form a binding treaty in governing the radiocommunication and orbital frequencies. They are meant to be the foundation in ensuring an "interference-free—or rather interference-controlled environment" for satellite operations.[46]

The ITU has the primary UN mandate for information and communication technologies, including outer space. It is responsible for allocating global radio spectrum and managing satellite orbital frequencies.[47] The ITU Radio Regulations are particularly important in the context of electronic warfare as they regulate the electromagnetic spectrum covering the range from 9 kHz to 275 GHz. The Radio Regulations have proven to be useful especially in defining different forms of interference such as acceptable interference, permissible interference and harmful interference. Harmful interference is defined as "interference which endangers the functioning of a radionavigation service or of other safety services or seriously degrades, obstructs, or repeatedly interrupts a radiocommunication service operating in accordance with Radio Regulations".[48]

The ITU Radio Regulations also assume importance in the context of ensuring secure, reliable and uncluttered telecommunications that are an absolute requirement for carrying out successful outer space exploration. Absence of reliable telecommunications in space would mean "no guidance, little tracking, no telemetry or command system, no contact with astronauts, no reception of scientific data from space probes, no commercial use of space communications and little radio astronomy".[49] Also, the jamming of satellites using electronic means could seriously impact a satellite's functions, possibly altering the satellite trajectories, for instance. The ITU Radio Regulations have issued several provisions to protect against any harmful interference of radio services and

[46] Y. Henri, "Long-Term Efficiency of the Space Regulatory Framework", https://www.itu.int/net/ITU-R/information/promotion/e-flash/2/article6.html.

[47] For details, see International Telecommunication Union, "Radio Regulations", http://life.itu.int/radioclub/rr/frr.htm.

[48] S. Pinnagoda, "Harmful Interference and Infringements of the Radio Regulations", Regional Radiocommunication Seminar for Asia–Pacific, The Philippines, 25–30 May 2015, https://www.itu.int/en/ITU-R/terrestrial/workshops/RRS-15-Asia/Documents/Harmful%20Interference.pdf.

[49] N. Jasentuliyana, "Regulatory Functions of I.T.U. in the Field of Space Telecommunications", *Journal of Air Law and Commerce*, vol. 34, no. 1, 1968, https://scholar.smu.edu/cgi/viewcontent.cgi?article=2576&context=jalc.

communications, which are to be abided by the member states.[50] There are also specific procedures that the Radio Regulations have laid down in case of harmful interference. However, the ITU does not make a distinction between deliberate and unintentional interference.[51]

Within the ITU, there are two bodies—the International Frequency Registration Board and the International Radio Consultative Committee that maintain the space communication data. The Board is responsible for ensuring "an orderly recording of frequency assignments made by the different countries so as to establish the date, purpose and technical characteristics of each of these assignments".[52] The Committee, on the other hand, undertakes technical studies, including the behaviour patterns of disturbances in the upper atmosphere that affect space communications. The Radio Regulations are modified from time to time through the World Radio Conferences held every four years.

While the ITU Radio Regulations have so far managed regulation of spectrum and orbit usage quite effectively, the increasing demand for radiofrequency allocation—leading to congestion not only from physical objects in orbit but also radiofrequency congestion—is a growing problem. This could lead to many interference issues, including some related to electronic warfare. Interference problems will increase dramatically with higher density in both low Earth orbit and geostationary orbit and the growth in mobile broadband usage.

Furthermore, due to poor security in commercial space systems, there is a threat to satellite communication security because malicious actors and hackers could attack satellites. There have been instances of such attacks in the past, including on GPS systems.[53] This further raises the so-called 'return address' problem, or the problem of figuring out who was responsible for the attack. This also raises questions both for States and for the international community as to how to respond to such attacks. And whether existing regulations and international norms are sufficient to address these are important questions for the global space community. Also, ITU Regulations exempt military radio installations which could limit their influence on military electronic warfare or cyber operations.

4.4 EXPORT CONTROLS

Export controls have also played a significant role in regulating the flow of space technologies and capabilities. Technology export control regimes including the Coordinating Committee on Multilateral Export Controls, later the Wassenaar Arrangement, the Nuclear Suppliers Group, the Missile Technology Control Regime, and the Australia Group were used as instruments in keeping an effective check on global trade in these dual-use technologies.

One of the most successful US domestic export control regimes with regard to outer space activities has been that of the International Traffic in Arms Regulations (ITAR).[54] ITAR covers space technology

[50] B. Ba, "Harmful Interference and Infringements of the Radio Regulations", Regional Radiocommunication Seminar for Africa 2013, Cameroon, 16–20 September 2013, https://www.itu.int/en/ITU-R/terrestrial/workshops/RRS-13-Africa/Documents/Harmful%20Interference.pdf.

[51] "Harmful Interference to Space Services", BR-SSD e-Learning Center, https://www.itu.int/en/ITU-R/space/elearning/presentations/UIT_SSD_028.pdf.

[52] N. Jasentuliyana, "Regulatory Functions of I.T.U. in the Field of Space Telecommunications", *Journal of Air Law and Commerce*, vol. 34, no. 1, 1968, https://scholar.smu.edu/cgi/viewcontent.cgi?article=2576&context=jalc.

[53] B. Weeden, "Electronic Warfare and Satellites: Challenges in Assuring Space Capabilities", Electronic Warfare GCC, Abu Dhabi, 25–26 October 2016, https://swfound.org/media/205651/bw_ew_satellitesatellites-gcc_oct2016.pdf.

[54] Even though the ITAR is a US domestic regulation, given the United States' position both in diplomacy and in trade, it has had a significant effect on high technology exchanges. For more details on the US domestic export control regulations including ITAR and EAR, see "The International Traffic in Arms Regulations",

because of its application to missile technology and possible expansion into military space programmes. Given the growing trends in space weaponization and the US decision to maintain strategic control and superiority in the space domain, ITAR will remain pertinent in US policy in the coming years. Arguably, ITAR was more effective in the past when technology was limited to a few major space powers. However, the diffusion of technology means ITAR has been less successful in recent years, particularly now that there are various alternate technologies available on the global market for space technology. While they may not be very sophisticated, their availability limits the effectiveness of technology controls.

Export controls have historically been an effective way of controlling the availability of advanced and military-related technologies. However, the dual-use nature of most space systems means that a lot of the systems and components intended for civilian uses are controlled by strategic export control regimes. Space technologies have brought significant benefits to the lives of people, be it for communications, dealing with disaster warning and management, location determination services and so on. However, the same technology has also brought immense advantages to military forces in carrying out precise military operations due to the availability of high-quality imagery, battle field information and communications, and weather data. Some of the technologies available in the civilian domain are militarily sensitive and should be controlled. Ground support equipment as well as radiation-hardened devices and certain propulsion systems are good examples. Similarly, tracking systems that are typically used for satellites can also be used for missile early-warning systems. Given this dual-use nature of space systems, the effectiveness of any export controls is going to be limited because States will be able to legitimately claim they need to buy or develop such technologies for civilian purposes. Likewise, it makes it more difficult for companies with legitimate civilian intentions to procure the technology necessary for space activities.

While still imperfect, ITAR regulations were more effective at a time when the space domain was dominated by two or three powers. Today, with the spread of technology across a vast number of players, including commercial actors, the sustained effectiveness of ITAR is questionable. Nevertheless, ITAR will remain an important pillar in US policy in the years to come.

https://www.pmddtc.state.gov/?id=ddtc_kb_article_page&sys_id=24d528fddbfc930044f9ff621f961987; Bureau of Industry and Security, Department of Commerce, US Government, “Export Licensing (ITAR & EAR)”, https://www.bis.doc.gov/index.php/forms-documents/technology-evaluation/781-export-licensing/file; Government Relations LLC, “What is ITAR?”, https://gov-relations.com/itar/.

5 The need for more viable global mechanisms

This paper suggests that, as the development of counter-space technologies accelerates, there is a growing need to develop more effective and viable global instruments that limit the potentially dangerous consequences of these new capabilities. Nevertheless, the global debate has not gone far, with broadly two perspectives. One perspective is that legally binding measures are necessary, while the other argues that such legal treaties are difficult to conclude, suggesting instead that the international community should pursue voluntary transparency and confidence-building measures (TCBMs). This dialogue played out most recently in the Group of Governmental Experts on further practical measures for the prevention of an arms race in outer space, which met in Geneva for its final session in March 2019. This Group was unable to reach consensus on a report or to make any further recommendations in part because some States do not think that adopting an effective treaty is possible at this time and that voluntary measures should be pursued. Building consensus between these two camps is critical. But several factors, including the changing balance of global and regional power dynamics, have hampered the process of building an agreement between the m. Given that this is a long-term challenge, there are those who articulate a middle path in the form of legally binding TCBMs.

Irrespective of the form and type of new efforts, the need for definitional clarity on a range of concepts is clear. Terms such as 'space weapon', 'weaponization of space' and 'peaceful uses of space' need to be defined clearly if the challenges of counter-space technologies—especially electronic and cyber warfare technologies—are to be dealt with in an effective manner. The existing legal regime has been insufficient to address these electronic and cyber warfare challenges. Given that literally any object in space can be used in a nefarious manner, to be prudent States could focus on behaviour and activities that an object in space is used for. Indeed, this was a conclusion of the 2013 Group of Governmental Experts report on *Transparency and Confidence-Building Measures in Outer Space Activities*.[55]

In the coming years, the international community will need to consider which electronic and cyber activities in outer space it will focus on to ensure outer space remains safe, secure and accessible. This requires tackling some difficult questions with a view to achieving some kind of common understanding. What, for example, should be the criteria for deciding that an electronic or cyber attack has taken place? Building a consensus among States on this question will not be easy. It is likely that most States will agree that an attack has taken place if it leads to physical destruction of space assets or causes fatalities. But it is likely more difficult to reach an agreement on this question when a State or a private corporation has used electronic or cyber measures for tampering with or stealing data or interference that does not lead to destruction of physical assets. Though unauthorized access would usually be considered a crime, whether it would amount to international aggression is not clear cut. Reaching some agreement—at the least—on what is clearly prohibited and potential casus belli should be considered a priority. There should also be discussion on where to set the bar. Should it be set so low that only the most egregious offensive act is deemed illegitimate? What would be the broader implications for the rule of law and relations between States?

Any new international measure that is developed, whether it is a legally binding treaty on the prevention of arms race in outer space or a new Code of Conduct, will need to consider whether to make a distinction between electronic and cyber technologies on the one hand and kinetic means

[55] General Assembly, Transparency and Confidence-building Measures in Outer Space Activities, UN document A/RES/65/68, 8 December 2010, http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/65/68.

on the other. It is not necessary that both of these types of capabilities be dealt with in the same instrument: they could be addressed through distinct measures. It is likely that some States will wish to retain the option to use electronic and cyber measures, for reasons explained earlier, even if they are reluctant to use kinetic means. One way forward might be to focus on the effects of an attack, irrespective of the means used. Also, given the interlinkages between these technologies, electronic and cyber warfare issues may be brought into discussions in information and communication technology forums as well. This will require more cross-cutting conversations that transcend existing policy and technical discourses, which are frequently siloed.

Another related concern is that of adjudicating complaints about electronic and cyber attacks. By their very nature, use of such means is not easy to detect or trace even after an attack has taken place. Ideally, accusations of such attacks need to be arbitrated neutrally. While mechanisms exist for such neutral arbitration in some areas, this remains the exception rather than the norm. One possibility would be an agency with a UN mandate in order to promote global participation that will have international legitimacy.

Developing consensus on some of these pragmatic aspects of addressing electronic and cyber warfare will not be easy. Yet the importance of outer space to the entire global community means that outlining the rules of the road is necessary in order to limit their negative consequences. An initial step could be to work jointly on a simple working definition of what constitutes armed attack in space. Important questions that arise in this regard include whether electronic and cyber attacks such as hacking, jamming, or spoofing a satellite can be considered as an armed attack and how and whether such actions become a threat to international peace and security. Issues such as the threshold for the use of force under such a scenario, as well as what might be a proportionate response to such attacks against space objects, could also be tackled in these discussions. Of course, these questions could become even more complicated especially when third parties such as commercial actors are involved. It would be advisable to stay aligned with the current dominant legal opinion that scale and effects of an attack should determine whether the armed attack has taken place. While this may not be entirely satisfactory, it is consistent with current legal standards.

The next step would be to assess States' responsibility—especially due to the increasing prevalence of non-State actors in outer space activities. Security Council resolution 1540 provides a potential solution because it mandates each State to control the actions of citizens and individuals within its borders.[56] With regard to cyber and electronic warfare in outer space, following the resolution 1540 example, it could be made clearer that States are responsible for ensuring attacks are prevented from within their territory.

Discussing these issues in the UN Disarmament Commission could be an appropriate way to begin this process of moving toward future regulation, and it would contribute to greater understanding and, hopefully, policy convergence. The Commission could choose from a number of tracks, from a broad approach discussing electronic and cyber warfare in outer space in a general sense, to a narrower approach in which specific issues are taken up. In view of what has been explored in this paper, some specific issues for consideration could be: defining what an armed attack against an outer space object is; the requirements for verification and monitoring mechanisms in any future mechanism; and a mapping exercise laying out the national technical means to undertake verification and monitoring. The outcomes of these discussions could subsequently be directed to the General Assembly First Committee and Security Council for further action.

[56] Security Council, UN document S/RES/1540, 28 April 2004, http://www.un.org/ga/search/view_doc.asp?symbol=S/RES/1540%20(2004)&Lang=E.

May 2019 — Space Dossier 3

Electronic and Cyber Warfare **in Outer Space**

This paper outlines emerging technologies and capabilities in the electronic and cyber warfare domain as these pertain to outer space and how the international community can address this problem through global governance. Outlining existing counter-space capabilities could establish a sound basis for developing effective measures to address this challenge and prevent dangerous escalation.

UNIDIR