NATO OTAN

Allied Command Transformation

Norfolk, Virginia | USA

Legal Gazette

Issue #42

December 2021

Legal Aspects of Space: NATO Perspectives

Contents

Introduction: The Woomera Manual Project and The MILAMOS Project, *by Robert Gray "Butch" Bracknell (including forewords by manual editors)*..... **3**

- **Space Domain, Autonomous Warfare and Hybrid Environments: The next challenges for NATO,** *by Borja Montes Toscano, Andrés Muñoz Mosquera* **8**
- **NATO Space Policy in the light of the Prevention of an Arms Race in Outer Space (PAROS) initiative: Legal considerations,** *by Professor George D. Kyriakopoulos* **26**
- **In pursuit of the best standards: what material and legal interoperability for NATO forces?,** *by Laetitia Cesari Zarkan* **36**
- **Nasty, brutish, and short—the Future of Space Operations in the Absence of the Rule of Law: Addressing Congestion, Contestation, and Competitiveness in the New Space Era,** *by Douglas Ligor, Bruce McClintock* **53**
- **Orbiting Legal Analysis: Armed Attacks in Space,** *by Maj Lindsay L. Rodman*... **68**
- ***Attack on Critical Space Infrastructures: A Case of Self-Defence for the NATO Alliance?,*** *by Dr Annette Froehlich* **86**
- ***Security-by-Design Approaches for Critical Infrastructure: Mapping the Landscape of Cyber and Space Law****, by Antonino Salmeri, Antonio Carlo* **97**
- ***The threat of cyber-attacks to space-based assets affecting NATO's communications and weapons systems****, by Paula Raboso Pantoja, Rodrigo Vazquez Benitez* **114**
- ***Cybersecurity Policy and Standards for Offworld Operations,*** *by Professor Roy Balleste and Gilles Doucet* **129**
- ***Intersections of International Legal Rules in Cyberspace and Outer Space,*** *by Dr Adina Ponta* **140**
- ***Legal Solutions for the Peaceful, Sustainable and Strategic Utilization of Lunar Resources,*** *by Antonino Salmeri, Antonio Carlo* **165**
- ***Strategic and Legal Implications of Emerging Dual-Use ASAT Systems****, by Linda Slapakova, Theodora Vassilika Ogden, James Black* **178**
- ***'Heavens Open' - The Need for Increased Data from Space and Creating a Duty to Share that Data,*** *by Professor Christopher J. Newman, Maj Matthew G. Zellner* **194**
- ***Debris-creating Anti-satellite Weapons and Their Indiscriminate Effects,*** *by Christopher D. Johnson* **208**

Disclaimer:

The NATO Legal Gazette is produced and published by Headquarters Supreme Allied Commander Transformation (HQ SACT). The NATO Legal Gazette is not a formal NATO document and does not represent the official opinions or positions of NATO or individual nations unless specifically stated. The NATO Legal Gazette is an information and knowledge management initiative, focused on improving the understanding of complex issues and facilitating information sharing. HQ SACT does not endorse or guarantee the accuracy of its content.

All authors are responsible for their own content. Copyright to articles published in the NATO Legal Gazette may be retained by the authors or their employer with attribution to the issue of the NATO Legal Gazette the article first appeared in. Retention of the copyright an article by the author or their employer will be identified with the copyright symbol © followed by the name of the copyright holder. Any further publication, distribution, or use of all or parts from these articles are required to remain compliant with the rights of the copyright holder.

Absent specific permission, the NATO Legal Gazette cannot be sold or reproduced for commercial purposes.

Publisher:
Monte DeBoer, ACT Legal Advisor

Editor-in-Chief:
Robert Gray "Butch" Bracknell, HQ SACT Staff Legal Advisor

Editors:
Mette Prassé Hartov, HQ SACT Deputy Legal Advisor
Galateia Gialitaki, ACT SEE Legal Assistant

Copy Editors:
Cdr Todd A. Richards (USN R)
LtCol Scott Lucchesi (USAF R)
Idil 'Muge' Karatas, HQ SACT Legal Intern
Davis M. Wright, HQ SACT Legal Extern

Source : https://ac.nato.int/

Introduction

by Robert Gray "Butch" Bracknell
Editor-in-Chief

Issue 42 of the NATO Legal Gazette explores the emergent area of legal regimes in space. In 2019, NATO Allies adopted a new Space Policy and declared outer space an operational domain, focusing NATO's policy, planning, and doctrine development efforts on yet another area for potential conflict and activities which enable NATO's terrestrial activities. Headquarters Supreme Allied Commander Transformation is fortunate to have contributions from a wide range of authors from both within and without the Alliance exploring topics germane to deterrence, disruptive technology, application of the law of armed conflict, applicable legal regimes, or the absence thereof, exploitation of space-based resources, and the overlap of cyber and space law.

Perhaps more than any other field, space law is evolving – rapidly and in new directions. Space law, like cyber law, requires a level of technical understanding of capabilities, hardware, software and astrophysics to apply legal standards and conduct legal analysis. It is governed by a more extensive treaty regime than cyber law – but like cyber law, there are capacious substantive areas which remain to be developed. Similarly, comparable to cyber law, political officials, policymakers, legal scholars, and legal practitioners rely on customary international law and "law by analogy" to derive norms and standards for state and non-state actors' behaviour in space.

Drawing on the experience and success of the two (and soon to be third) versions of the Tallinn Manual on the International Law Applicable to Cyber

Operations,[1] two sets of scholars have undertaken projects to provide similar, descriptive summaries of existing law applicable to space. These two projects are *The Woomera Manual on the International Law of Military Space Operations*,[2] organized by the University of Adelaide, the University of Exeter, the University of Nebraska, and the University of New South Wales - Canberra, and *The Manual on International Law Applicable to Military Uses of Outer Space* (MILAMOS) project, organized by Canada's McGill University. These manuals are not intended to be prescriptive, but rather *descriptive* – they attempt to capture and express the state of existing law germane to space, particularly military applications and operations in space. The textual passages which follow are introductions to each project.[3]

***

The Woomera Manual Project

Professor Dale Stephens

It has been increasingly noted in a number of official Defence publications that contemporary military reliance on space assets is both critical and very vulnerable. Similarly, it has been observed that the rules, norms and frameworks that govern military space operations are not only unclear in key parts but in danger of erosion and manipulation.

Against this background, *The Woomera Manual on the International Law of Military Space Operations* (OUP 2021), is a multinational, university led project dedicated to locating and articulating the applicable legal regime that applies to govern military operations in space. The project's goal is to especially identify the grey areas and the likely legal and policy friction points that underpin contemporary space operations with a view to providing a foundation that minimises strategic legal (and operational) miscalculation.

Central to the project is an examination of space law, the *jus ad bellum* and the Law of Armed Conflict that can and does apply to military space operations. Critically, the project focuses on State practice to discern reliable positions taken on the law and applies a methodology that seeks to reconcile the different legal regimes potentially applicable to establish the state of

[1] The Tallinn Manual, Cooperative Cyber Defence Centre of Excellence, available at https://ccdcoe.org/research/tallinn-manual/ .
[2] The Woomera Manual, University of Adelaide, available at https://law.adelaide.edu.au/woomera/
[3] The introductions are sequenced randomly, and no priority or preference should be inferred.

prevailing law across the full military operational spectrum.

The project was launched in 2018 and is spearheaded by The University of Adelaide (Australia), and The University of Exeter (U.K.), The University of Nebraska–Lincoln (U.S.) and the University of New South Wales–Canberra (Australia). It follows in the footsteps of other International Operational Law Manuals such as the *San Remo Manual on Naval Warfare*, Harvard's *Humanitarian Policy and Conflict Research (HPCR) Manual on Air and Missile Warfare* and the *Tallinn Manual 2.0 on Cyber Operations* that have all informed critical decision making by States in their respective fields.

The drafting team of the *Woomera Manual* comprises academic, government (acting in their personal capacity), and non-governmental organization (NGO) lawyers, as well as technical experts. As mentioned above, the primary methodological focus is to examine State practice in this field. While there has been much academic commentary written about military space activities, the fact remains that States make international law. The State practices examined include the negotiating history of relevant treaties, official statements and, more importantly, actions taken by States in the context of military space operations as well as military manuals and information gleaned from actual international military space exercises.

Certain questions are becoming key real-time operational issues that demand clear answers, including those related to:

- Possible safety zones between military space objects;
- What military activity is actually permitted on the Moon (and celestial bodies);
- International responsibility for the actions of companies and non-state actors;
- Where the thresholds for interference, intervention, use of force, and armed attack (and responses of retorsion, countermeasures, necessity, and self-defence) all lie; and
- On what basis, and in what manner the law of armed conflict applies to space in the event of an armed conflict occurring in this theatre of operations.

A number of countries are developing their military space programs, including their counter-space capabilities, and many of these apparently theoretical questions will become very real, very soon.

The Manual's editors are in a process of finalising the Manual and have

started an extensive international peer review process on the draft rules and commentary. In addition, there will be a dedicated State engagement process that will be undertaken with the assistance of the Dutch Government. This process will allow interested States the direct opportunity to provide their input concerning the research process and conclusions reached prior to the Manual's final submission for publication.

The central goal of the Woomera project is to provide a clear articulation on the delineation of the law applicable to military space operations. In so doing, the Manual aims to principally assist military and government decision makers (among others) by providing a reliable guide for their decision making processes.

The MILAMOS Project

Professor David Kuan-Wei Chen, McGill University
Professor Roy Balleste, Stetson University
Professor Ram Jakhu, McGill University
Professor Steven Freedland, Western Sydney University

Launched in May 2016, the McGill Manual on International Law Applicable to Military Uses of Outer Space (MILAMOS) is the first of its kind to address the legality of activities that have a bearing on strategic uses of outer space and military activities in outer space. With the involvement of over 40 world-class legal experts, technical experts and observers from various States, the European Union and civil society, the MILAMOS Project aims to define the legality and scope of responsible behaviour in situations that fall short of armed conflict in outer space.

In dissecting existing treaties and analysing State practice, the McGill Manual comprises of approximately 60 rules that provide clear restatements and objective interpretations of what the law is (*lex lata*) in relation to key subject-matters of interest and concern. In capturing nuanced discussions and consensus on such vital matters as the harmful interference of electromagnetic signals, the legality of proximity and rendezvous operations, and the threat or use of force in outer space, the McGill Manual is expected to avoid unilateral interpretations of the law. As activities in outer space and the Moon increase, it is of importance that space operators, whether military or private in nature, have a common understanding of what is permissible to reduce the risk of misinformation, misunderstanding and miscalculation arising from activities in an increasingly competitive, contested and congested arena.

Unique to the MILAMOS Project is the involvement of experts and institutions from Western as well as non-Western States, including China, India, Japan, and Russia. This will ensure the McGill Manual captures the perspectives of different States and stakeholders, and is reflective of the wide spectrum of interests and concerns relating to the military uses of outer space. The long-term sustainability, safety and security of operations in outer space require that all stakeholders in this shared global commons have a common understanding of what the law is. The McGill Manual will go a long way to inform the progressive development of international law in a domain of growing strategic, economic and geopolitical importance. The value and preliminary results of the MILAMOS Project have been underlined at several conferences and high-level forums, including at the United Nations.

Since the launch of the MILAMOS Project, consensus-forming and rule-drafting workshops and Editorial Committee meetings have been held in cities around the world, including Montreal, Adelaide, Colorado Springs, New Delhi, Beijing, Berlin and Tokyo. These meetings provide opportunities for MILAMOS Experts to discuss black-letter rules and associated commentary that aim to clarify international law as it applies to military space activities in peacetime. These events also provided valuable opportunities to engage with officials, stakeholders, and institutions around the world and contribute to ongoing discussions on transparency and confidence-building measures in outer space.

***

The "manual approach" itself is an interesting and unique development in the maturation of international law. International law is primarily the province of nations – it principally binds nations, is formed by nations, is applied by nations, and is altered by nations -- through the actions and resolutions of the United Nations, the formation of treaties, and the development of customary international law. The corpus of any body of law often has opaque edges, but the manual approach seeks to capture and define the body of law in a way that is accessible, comprehensive and objective. The manuals mark a starting point for other individuals, nations, and international bodies not involved in their development to contribute to the dialogue on obligations attendant to international law. The NATO Legal Gazette is honoured to contribute to the discourse, augmenting and adding to the body of knowledge on space law to complement the manuals.

***

Source: https://ac.nato.int/

Space Domain, Autonomous Warfare and Hybrid Environments: The next challenges for NATO[1]

by Borja Montes Toscano[2] and
Andrés Muñoz Mosquera[3]

Introduction

The space domain has recently become a new field full of new opportunities due to the advancements in technology. Nevertheless, vulnerabilities may arise as states and private companies exploit this domain to achieve strategic competitive advantage in different areas (e.g. weather monitoring, transport, environment and agriculture, science, communications, among others), and draw benefits out of them. These realities may pose challenges to the existing rule of law in the space domain leading to legal uncertainty and an apparent governance vacuum. In addition, possible

[1] **DISCLAIMER**: The views expressed in this article are solely those of the authors and may not necessarily represent the views of NATO, Allied Command Operations, or Allied Command Transformation, or of their affiliated organizations.

[2] e-LAWFAS Legal Content Manager at the NATO ACO Office of Legal Affairs (SHAPE). PhD candidate at the University of Seville. Member of the Bar Association of Lucena/Córdoba.

3 Legal Advisor, Director of the NATO ACO Office of Legal Affairs (SHAPE). Graduate of the Fletcher School of Law and Diplomacy (Tufts University) and the NATO Defense College (GFOAC), PhD candidate at the University of Leiden. Member of the Bar Association of Madrid, CCBE European Lawyer.

technological disruptions (e.g. satellites' interferences) may distort information gathered, which is essential for NATO's operations and missions, including collective defence, crisis response and counter-terrorism.

Hence, these concerns have resulted in NATO's new space policy, and in this way recognizing space as new operational domain two years ago.[4] The 1980s and 1990s bore witness that concluding new binding agreements for outer space matters beyond the existing ones would be extremely difficult. However, the fluid legal regime for the outer space does not entail that customary international law is inapplicable.[5] The crystallization of an international customary norm is a lengthy process, as is the development of treaties, and thus the introduction of a Rules-Based International Order (RBIO). Several factors within the space domain cannot be under-estimated by the Alliance such as space-based strike weapons, space support for the Alliance's operations or dual-use material/devices.

These challenges emphasize the need to complete policy and doctrine to achieve better interoperability and resilience among Allies and contribute to forge a network of reliable soft law. NATO's inclusion of space as the fifth operational domain represents a step forward in support of the principles of the Charter of the United Nations and on NATO's pathos of collective self-defence and consultation, as enshrined in articles 4 (consultation) and 5 (collective defence) of the Washington Treaty. Hence, such inclusion is an additional feature of the adaptability of these provisions to armed attacks (including non-conventional tactics).[6] Bearing in mind the Alliance's institutionalised

---

[4] NATO, 'Press Conference by NATO Secretary General Jens Stoltenberg following the meetings of NATO Defence Ministers' (27 June 2019) https://www.nato.int/cps/en/natohq/opinions_167245.htm?selectedLocale=en accessed 29 October 2021.

[5] In this sense, former ICJ Judge Manfred Lachs stated that: "[O]uter space never had been a lawless area or legal vacuum, but had been subject to international law, though the matter could never have been put to the test before." Manfred Lachs, 'The Law-Making Process' in Tanja Masson-Zwaan & Stephan Hobe (eds), *The Law of Outer Space - An Experience in Contemporary Law-Making* (Martinus Nijhoff Publishers, 2010) 125; See also Timothy G. Nelson, 'Regulating the void: In-orbit collisions and space debris' (2015-2016) 40 *Journal of Space Law* 105, 126.

[6] To name a few non-conventional tactics: disruption of order, political subversion of government or non-governmental organizations, psychological operations, abuse of legal processes, and financial corruption as part of an integrated design to achieve strategic advantage. Frank G. Hoffman, 'Examining Complex Forms of Conflict Gray Zone and Hybrid Challenges' (2018) 7(4) *PRISM* 31, 36. Such adaptability of article 5 is possible because of the Alliance's dynamic institutionalization. On the Alliance's dynamic institutionalization, see Andres B. Munoz Mosquera & Nikoleta Paraskevi Chalanouli, *North Atlantic Treaty: Travaux préparatoires reconstructed* (Wolf Legal Publishers, 2020) 46-47.

procedures and the behaviours observed over the past years in formal and informal domains, including the space domain, hybrid threats will continue proliferating at the left and the right of article 5.

In the paragraphs below, several questions will be briefly analysed NATO lawyers and policy makers must take into account when approaching the complex legal matters that entail the use of outer space. The better they understand the legal mechanisms, faults, needs and opportunities that the fluid legal framework of outer space presents, the better Allies and NATO will cope with real and tangible challenges and risks that outer space presents *vis-à-vis* their adversary in the current strategic competition governed by hybrid environments.

A Fluid Legal Framework

Public international law is a generic aspect of law that affects relations among states. International space law is a functional classification of public international law and domestic law relating to activities taking place in outer space. These activities must comply with five applicable international treaties and United Nations' general principles of which some of them (but not all) amount to customary international law,[7] and with a myriad of national laws

[7] Hard and Soft law frameworks for outer space. Treaties (binding): a) Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies; b) Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space; c) Convention on International Liability for Damage Caused by Space Objects; d) Convention on Registration of Objects Launched into Outer Space; e) Agreement Governing the Activities of States on the Moon and Other Celestial Bodies. Principles adopted by the General Assembly of the United Nations (non-binding): a) Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space; b) Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting; c) Principles Relating to Remote Sensing of the Earth From Outer Space; d) Principles Relevant to the Use of Nuclear Power Sources in Outer Space; e) Declaration on International Cooperation in the Exploration and Use of Outer Space for the Benefit and in the Interest of All States, Taking into Particular Account the Needs of Developing Countries. Related resolutions adopted by the General Assembly of the United Nations: a) Resolution 1721 A and B (XVI) of 20 December 1961: International cooperation in the peaceful uses of outer space; b) Paragraph 4 of resolution 55/122 of 8 December 2000: International cooperation in the peaceful uses of outer space; Some aspects concerning the use of the geostationary orbit; c) Resolution 59/115 of 10 December 2004: Application of the concept of the 'launching state'; d) Resolution 62/101 of 17 December 2007: Recommendations on enhancing the practice of States and international intergovernmental organizations in registering space objects.
Other documents (non-binding): a) Space Debris Mitigation Guidelines of the Committee on the Peaceful Uses of Outer Space; B. Safety Framework for Nuclear Power Source Application in Outer Space. United Nations Office for Outer Space Affairs doc. ST/SPACE/61, https://www.unoosa.org/pdf/publications/st_space_61E.pdf , accessed 29 October 2021. See

and regulations, as well as decisions taken by international organizations with space-related activities.[8] Additionally, there are "applicable" soft law instruments (recommendations, guidelines, codes of conduct…) which have been instrumental to move forward different initiatives at intergovernmental and NGO levels. In addition, these instruments have tried to fill in the existing gaps (sometimes even to provide legal advice and arguments to governments and international institutions), notwithstanding that some non-binding space instruments have a higher legal "value" than others do.[9]

This complex network of hard-law and soft-law, outer space legal framework, together with the treaty-based principle[10] that all states have the right to freely have access to outer space and therefore explore it and use it presents magnificent opportunities for the human development, but also an area or contention among the different actors capable and willing to enter into activities in outer space. This is also an open window for those capable and willing to impose practices advantageous for their own interests. Outer space legal framework does not and will not escape the strategic positioning of non-law-abiding actors.

The sustainability of space activities is subject, *inter alia*, to the type of actions that space stakeholders are ready to take up. Concerns relating to defence may make outer space the object of military activities of many kinds, i.e., not only that those activities will take place entirely in the space domain, but also that they will support kinetic and non-kinetic actions on the Earth,

---

also the 2011 UNGAR 65/68 (A/RES/65/68, 13 January 2011) and 2013 UNGAR 68/50 (A/RES/68/50, 10 December 2013) on Transparency and Confidence-Building Measures in Outer Space activities. Other initiatives that can be mentioned are the European Union Draft Code of Conduct for Space Activities, the IADC Space Debris Mitigation Guidelines or the International Code of Conduct against Ballistic Missile Proliferation (ICOC), where states parties engage to internationally regulate the area of ballistic missiles capable of carrying WMD, putting special emphasis on the need of Transparency. See HCoC - *the Hague Code of Conduct* https://www.hcoc.at/ accessed 29 October 2021.

[8] Fabio Tronchetti, *Fundamentals of Space Law and Policy* (International Space University, Springer, 2013) 85.

[9] Steven Freeland, 'Space in a Changing World: The Future Regulation of Outer Space Technology, Warfare and International Law' in Cenan Al-Ekabi, Blandina Baranes, Peter Hulsroj & Arne Lahcen (eds), *Yearbook on Space Policy 2012/2013* (Springer, 2015) 199, 208.

[10] Some have acknowledged that the right of free access to space, together with other rights, would deserve the status of *jus cogens* norms. However, *jus cogens* norms develop over time with the agreement of the majority of states. It would be difficult to acknowledge that such right has gained an elevated and protected status. See Cassandra Steer, 'Sources and law-making processes relating to space activities' in Ram S. Jakhu and Paul Stephen Dempsey (eds), *Routledge Handbook of Space Law* (Routledge, 2017)16-17.

which eventually "may make" orbital assets a military target.[11] Once again, the hard and soft law frameworks in place and how these are observed and interpreted will play a major role in the development of the use of outer space.

This complex mix of outer space "legal environment", sometimes apparently "weak" but actually "fluid" and current non-kinetic trends collectively make this domain an "obscure object of desire" for legal use and misuse, which may lead to Lawfare activities.[12] Moreover, the fact that military use of outer space sometimes is a matter of controversy, it sets substantial grounds for the use of Lawfare as a means to project influence, legitimate as well as illegitimate. On this note, it should be understood that Lawfare in hybrid environments belongs to the category of "influence operations" which mainly consists of non-kinetic, communications and information-related activities whose intent is to affect cognitive, psychological, motivational, ideational, ideological, and moral characteristics of a target audience.[13]

The path to artificial intelligence in space warfare and the question of accountability – Compliance with International Humanitarian Law

Different events have highlighted the concern of space's weaponisation. To name some of them: Unilateral missile strikes (2007) or anti-satellite (ASAT) kinetic tests reaching geostationary orbit (2014) by the People's Republic of China[14], the jamming of U.S. military drones operating in Syria by Russian Federation (2018)[15] or currently the development of programmes on intercontinental ballistic missile (ICBM) by Iran or North Korea.[16] While the use of nuclear weapons and weapons of mass destruction (WMD) in outer space is not allowed, the launch of other kinds of (autonomous) weapons (e.g. anti-satellite weapons or transit of anti-ballistic missiles) is not contrary to article IV of

[11] Fabio Tronchetti (n 6) 87.
[12] Andres B. Munoz Mosquera & Sascha Dov Bachmann, 'Lawfare in Hybrid Wars: The 21st Century Warfare' (2016) 7 *Journal of International Humanitarian Legal Studies*.
[13] Ibid, 73.
[14] Andrea Shalal, 'Analysis points to China's work on new anti-satellite weapon' (*Reuters*, 17 March 2014) https://www.reuters.com/article/us-china-space-report-idUSBREA2G1Q320140317 accessed 29 October 2021.
[15] Dan Joling, 'Russia has figured out how to jam U.S. drones in Syria, officials say' (*NBC*, 10 April 2018) https://www.nbcnews.com/news/military/russia-has-figured-out-how-jam-u-s-drones-syria-n863931 accessed 29 October 2021.
[16] David Wainer, 'Iran and North Korea Resumed Cooperation on Missiles, UN says' (*Bloomberg*, 8 February 2021) https://www.bloomberg.com/news/articles/2021-02-08/iran-and-north-korea-resumed-cooperation-on-missiles-un-says accessed 29 October 2021.

the Outer Space Treaty (OST).[17] There are currently more than 2,000 satellites operating around the Earth's orbit and performing different tasks such as meteorological forecasts, scientific research, or communications (GPS). A space object can be threatened (or attacked) in different forms; tensions (e.g. hacking of satellites or manipulation of computer systems amounting to use of force) may quickly escalate into an armed conflict.

In spite of the fact that Autonomous Weapons Systems (AWS) are at their early stage of development and not yet fielded into outer space, states may deploy certain kinetic ASAT weapons that can trigger questions if they are programmed to act autonomously; such as interceptor vehicles, global-positioning systems, pellet clouds or remote sensing[18] satellites that may stand in the way of satellites placed in orbit. States, and particularly NATO Allies, must bear in mind that the international legal framework is very weak in this field as there is no international conventional/customary norm that prohibits the testing, deployment or use of ASATs and the IADC Space Debris Mitigation Guidelines are not of much use. In case states want to deploy AWS in outer space, a threshold or balance must be sought between the activities performed by the operator (choice of target, choice of weapon system, time, place…) and, on the other side, the behaviour demonstrated by the device (performance of sensors and targeting systems, ammunition used…).[19]

The Grey Zone gap (between IHL and Human Rights scenarios)[20] remains and states (and NATO) might not feel comfortable because of the uncertainty that this situation (i.e. time/physical space in between a state of peace and a state of war) may pose and its possible effects on people and institutions placed on Earth. In addition, revisionist and rogue states are seeking to influence international law (especially in the field of the Law of the Sea) in

---

[17] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (adopted 19 December 1966, entered into force 10 October 1967) 610 UNTS 205.

[18] The fact that states may use (autonomous) remote sensing devices will hold them liable for the activities performed, especially privacy issues. Some scholars assert that sharing of satellite resource data may derogate article 2(7) of the UN Charter. See discussion in Ruwantissa Abeyratne, *Space Security Law* (Springer, 2011) 18.

[19] Tim McFarland, *Autonomous Weapons Systems and the Law of Armed Conflict – Compatibility with International Humanitarian Law* (Cambridge University Press, 2020) 94.

[20] The concept of Gray Zone must be understood as the activity that is coercive and aggressive in nature, but that is deliberately designed to remain below the threshold of conventional military conflict and open interstate war. Hal Brands, 'Paradoxes of the Gray Zone'. Available https://www.fpri.org/article/2016/02/paradoxes-gray-zone/ accessed 29 October 2021.

their favour and broadcasting this through scholar opinions, media campaigns as well as international forums. Hence, the flow of communications among NATO Allies involved must be ensured in order to effectively encounter hostile responses.

Both space law and IHL regimes are considered to be *lex specialis* within their respective fields. Thus, bearing in mind article 53 of the Vienna Convention of the Law of Treaties (VCLT),[21] possible legal conflicts may be solved bearing in mind if the conflicting norms are considered to be *jus cogens*. Otherwise, the maxim of *lex specialis*[22] would be the most suitable mechanism for solving normative divergences. However, as both regimes are considered to be *lex specialis* within each of their fields, the Sovereigns would make the final decision on the applicable regime or normative provision.[23] In this regard, Sachdeva advocates for the selection and evolution of some precepts of the OST as *Jus Cogens* of Space Law;[24] such selection should bear in mind that article 53 VCLT is not exhaustive of all *jus cogens* phenomena in international law.[25]

On the other hand, there are no general or specific international law norms that acknowledge the application of space law in case hostilities arise in outer space, as the rules related to legal regulation of the use of force (*jus ad bellum*), apply to the use of outer space, on the grounds of article III of the

---

[21] Vienna Convention on the Law of Treaties (adopted 23 May 1969, entered into force 27 January 1980) 1155 UNTS.

[22] The *lex specialis derogat lege generali* standard technique of legal reasoning depends on different considerations such as the context, concreteness or purposes of the norm. See ILC, *Fragmentation of International Law: Difficulties arising from the diversification and expansion of International Law – Report of the Study Group of the International Law Commission, finalized by Martti Koskeniemmi*, A/CN.4/L.682 13 April 2006, paras 119-120.

[23] See discussions in Dale Stephens, 'The International Legal Implications of Military Space Operations: Examining the Interplay between International Humanitarian Law and the Outer Space Legal Regime' (2018) 94 *International Law Studies* 75, 90-92 and Anja Lindroos, 'Addressing Norm Conflicts in a Fragmented Legal System: The Doctrine of Lex Specialis' (2005) 74(1) *Nordic Journal of International Law* 27, 42.

[24] G. S. Sachdeva, 'Select Tenets of Space Law as *Jus Cogen*' in R. Venkata Rao, V. Gopalakrishnan & Kumar Abhijeet (eds), *Recent Developments in Space Law: Opportunities & Challenges* (Springer, 2017) 26.

[25] Following a *jus cogens* theory as the "public order of the international community", hierarchical superior norms (within space law) could be established. However, the public order theory misunderstands the relationship *lex generalis*/lex specialis with the relationship *lex superior/lex inferior*. See discussions in Thomas Kleinlein, 'Jus Cogens *Re-examined*: Value Formalism in International Law' (2017) 28(1) *The European Journal of International Law* 295, 298-300.

OST as well as customary international law.[26] Then, states will need to determine what constitutes "armed attack" in outer space, regardless of the exercise of the inherent right to self-defence recognized by article 51 of the UN Charter. In addition, if hostilities arise (*jus in bello*) IHL principles for both kinetic and non-kinetic acts need to be observed.

States must exercise "sufficient control" over the AWS that they may deploy in outer space,[27] i.e. they must count on capabilities that may enable the reversion of actions that did not require any human intervention. Hence, (allied) commanders must have "authoritative control" over the situation, implying a legitimate basis to act (authority) and the ability to exercise powers (or at least to influence), to regulate or govern.[28] In addition, commanders shall bear responsibility as regards their weapons' testing and possible tasks to perform, how these devices may "express" their autonomy or possible constraints that they impose on it (similarly as members of armed forces).[29] A "should have known" standard is applicable for commanders; for AWS deployed in space, the commander must be aware of the use of the weapon, including its operational capabilities and limitations to ensure compliance of the activities of the device with IHL. However, in the explicit case of autonomous cyber weapons (which could be fielded in outer space in the future), powerful algorithms may constrain commander's effective control. In such cases, command responsibility would not be applicable.[30]

The notions of effective control are different when comparing state and command responsibility. In case it is not possible to attribute a conduct performed by an AWS (and therefore a breach of an international obligation) to a particular state, some alternatives must be sought in order to avoid accountability gaps, similar to article VII of the OST and article II of the 1972 UN

---

[26] Jackson Maogoto & Steven Freeland, 'The Final Frontier: The Laws of Armed Conflict and Space Warfare' (2007) 23(1) *Connecticut Journal of International Law* 165,181.
[27] See Patrick van Esch, Gavin Northey, Magdalene Striluk, Helen Wilson, 'Autonomous weapon systems: Is a space warfare manual required?' (2017) 33(3) *Computer Law & Security Review* 382, 385.
[28] John W. Bellflower, 'The influence of law on Command Space' (2010) 65 *Air Force Law Review* 107, 121
[29] Marcus Schulzke, 'Autonomous Weapons and Distributed Responsibility' (2013) 26 *Philosophy & Technology* 203, 216-217.
[30] See further in Russell Buchan & Nicholas Tsagourias, 'Autonomous Cyber Weapons and Command Responsibility' (2020) 96 *International Law Studies* 645, 657-658.

Space Liability Convention.[31] The strict liability regime[32] would be a reasonable basis to hold states accountable when failing to comply with their obligations with regard to prevention, monitoring and damage prevention in relation to autonomous weapons systems.[33]

Accountability is intrinsically related to jurisdiction,[34] as the OST imposes accountability on the states for acts or omissions for activities in outer space under their control and jurisdiction. However, problems may arise as regards control not only over spacecraft but also over people and situations. Analysing article VIII of the OST, Cheng has argued that the quasi-jurisdiction of the state of registry applies to personnel on board not only for conduct that happens within the spacecraft but also when they are outside the vehicle.[35] Finding pathways to accountability requires not denying the importance of basic space treaties such as the 1972 UN Space Liability Convention[36] and the 1974 UN Space Registration Convention.[37] Articles II and III of the former instrument recognizes absolute liability of the launching state "[t]o pay compensation for damage caused by its space object on the surface of the earth, to aircraft flight (…) or to a space object of one launching State or to persons or property on board such a space object by a space object of another launching State (…)". The 1974 UN Space Registration Convention establishes the obligation on launching states to register space objects. In case of transfer of ownership of a space object to a new state, this new state cannot be held accountable because the 1972 UN Space Liability Convention does not explicitly recognize

---

[31] Bert-Japp Koops, Mireille Hildebrandt & David-Oliver Jacquet-Chiffrelle, 'Bridging the Accountability Gap: Rights for New Entities in the Information Society?' (2010) 11(2) *Minnesota Journal of Law, Science & Technology* 497, 555.

[32] Even if the state has not violated IHL, accountability would arise because of harmful acts attributable to the state. Yves Sandoz, Christophe Swinarski and Bruno Zimmerman (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (International Committee of the Red Cross, Martinus Nijhoff Publishers, Geneva 1987) 1058, para 3661.

[33] Robin Geiss, *The International-Law Dimension of Autonomous Weapons Systems* (Friedrich-Ebert-Stiftung, October 2015) 22-23.

[34] As a matter of comparison of both the Law of the Sea and Space Law regimes, state retains jurisdiction over such objects registered within its national institutions / those ships flying its flag; consequently, acts committed by states through these objects or by state officials would be attributable to the state.

[35] Bin Cheng, *Studies in International Space Law* (Clarendon Press Oxford, 1997) 231-232.

[36] Convention on International Liability for Damage Caused by Space Objects (signed 29 March 1972, entered into force 1 September 1972) 961 UNTS 187.

[37] Convention on Registration of Objects Launched into Outer Space (opened for signature 14 January 1975, entered into force 15 September 1976) 1023 UNTS 15.

the state of registration's liability. Bearing in mind article VIII of the OST,[38] the fact that the state of registry retains jurisdiction and control over the space object "[a]nd over any personnel thereof, while in outer space or on a celestial body", this automatically qualifies the state of registry, which as a launching state is liable for damage.[39] Therefore, possible accountability gaps may be filled as a result of these normative provisions and academic opinions.

However, as per the provisions foreseen in article VI (1)[40] of the 1972 UN Space Liability Convention, states need to remain aware of possible legal vacuums that may arise as a result of reading this provision: the element of fault. This concern was pointed out when the Draft Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA) were completed in 2001. One of the questions that the International Law Commission (ILC) had to face was whether fault constitutes a necessary element of the international wrongful act. The ILC answered that: "[I]n the absence of any specific requirement of a mental element in terms of the primary obligation, it is only the act of a State that matters, independently of any intention".[41] Fielding AWS in outer space may trigger certain risks as regards the accidents that the device may cause. In addition, certain states may be less accomplished in the use of AI military applications, leading to a disadvantage in relation to their strategic position in outer space. Therefore, important questions such as attribution of internationally wrongful acts made by AI devices or the precise meaning of "peaceful uses" of outer space must be addressed to achieve greater legal certainty.

In responding to possible attacks produced by (autonomous) space devices, NATO nations need to determine whether countermeasures would be

---

[38] In addition, some scholars have asserted that the state of registry is the launching state or one or more of the launchings states. Bin Cheng, 'Space Objects and their Various Connecting Factors' in Gabriel Lafferanderie & Daphné Crowter (eds), *Outlook on Space Law Over the Next 30 Years - Essays published for the 30th Anniversary of the Outer Space Treaty* (Brill Nijhoff, 1997) 205.

[39] Marco Pedrazzi, 'Outer Space, Liability for Damage' Max Planck Encyclopaedia of Public International Law (May 2008) https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1203 accessed 29 October 2021.

[40] Article VI (1): "[S]ubject to the provisions of paragraph 2 of this Article, exoneration from absolute liability shall be granted to the extent that a launching State establishes that the damage has resulted either wholly or partially from gross negligence or from an act or omission done with intent to cause damage on the part of a claimant State or of natural or juridical persons it represents."

[41] UN ILC, *Draft Articles on State Responsibility with Commentaries*, Yearbook of the International Law Commission, 2001, vol. II, Part Two 36, para 10.

exercised in spite of the fact that territorial sovereignty is not applicable to outer space (within the meaning of article 2(4) of the UN Charter) and whether such counterattacks should involve terrestrial assets or possibly disabling the system through cyber countermeasures.[42] The incidental involvement of an international organization, such as NATO,[43] in these activities may further lead to possible questions of the organization's liability. On this aspect, the 2011 Draft Articles on the International Responsibility of International Organizations (DARIO) may provide guidance and the statement submitted by NATO that "[e]ach Member State retains full responsibility for its decisions [taken within the North Atlantic Council]".[44] Nevertheless, article VI of the OST recognizes a shared responsibility model between states and international organizations for the activities carried on (by the latter) in outer space. To solve matters in relation to the registration of space objects owned by international organizations and possible liabilities that may arise, both article XIII of the 1972 UN Space Liability Convention and article VII of the 1974 UN Space Registration Convention assert that they will be applicable to an intergovernmental organization if this institution accepts the rights and obligations provided for in both conventional instruments and if a majority of the States members of the organization are States Parties to conventional norm that is to be applied and to the OST.[45]

Some Outer Space Grey Areas: Militarization and Space Delimitation

The complexities of the legal framework of outer space tend to create grey areas or, maybe, its simple tenets can well be an object of abuse. The elusive nature of legal matters relating to military activities in outer space and

---

[42] See further discussion in Frans G. von der Dunk, 'Armed Conflicts in Outer Space: Which Law applies' (2021) 97 *International Law Studies* 188, 209-210.

[43] Bearing in mind the mission entrusted to NATO, the Alliance will be mainly focused in fostering space awareness capabilities through the coordination of data, products and services with Allies. SHAPE, 'NATO Space Centre' https://shape.nato.int/about/aco-capabilities2/nato-space-centre accessed 29 October 2021.

[44] UN ILC, 'Responsibility of international organizations Comments and observations received from international organizations' Doc. A/CN.4/637 139-140, https://legal.un.org/ilc/documentation/english/a_cn4_637.pdf , accessed 29 October 2021.

[45] As per September 2021, only three international organizations have declared their acceptance to the rights and obligations both for the 1972 UN Space Liability Convention and the 1974 UN Space Registration Convention: European Organization for the Exploitation of Meteorological Satellites (EUMETSAT), European Space Agency (ESA) and the European Telecommunications Satellite Organization (EUTELSAT-IGO). Available in United Nations Office for Outer Space Affairs, 'Treaties' https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/registration-convention.html accessed 29 October 2021.

celestial bodies, or the limits of the space domain itself are good reasons to "encourage" states willing to enter the strategic competition in these areas that are pending on further technological and common understanding regarding its use as *territorium extra commercium* and *territorium commune humanitates*.

On matters relating to the military use of outer space, first of all it is necessary to define the difference between militarisation and weaponisation.[46] The former is a legal and legitimate activity in the space domain, while the latter has limitations if not banned. Article IV of the OST is considered crucial in this regard, since it addresses questions relating to arms control and limitation *vis-à-vis* the undertaking of military activities in outer space. More particularly, article IV prohibits carrying nuclear weapons or WMDs in orbit around Earth or its installation on celestial bodies or in stations in outer space. Following the criteria of treaty interpretation set up in articles 31 to 33 of the VCLT "weapons", as referred to in article IV of the OST, have to be seen in a broad perspective. Moreover, and in comparison, the irreconcilable functional and spatial postures on how to approach the delimitation between the airspace and outer space brings out meaningful evidence for, *inter alia*, new approaches to international law. For example, China considers that "[c]ompetition among major powers today is mainly a competition of systems and rules. It is necessary to use Xi Jinping's thoughts on the rule of law to better use legal tools to protect the country's dignity and core interests in accordance with the law".[47]

In this context the 17 October 1963 UNGAR 184 (XVIII) should be recalled, which (while is it not binding) sets the tone by exhorting states to refrain from placing in the orbit around the Earth any object carrying the weapons described above, as well as from causing, encouraging or participating in activities related to the aforementioned activities.[48]

---

[46] The US has interpreted the use of Outer Space for "peaceful purposes" as "non-aggressive and beneficial" consistent with the UN Charter and similarly as UNCLOS states for the high seas "peaceful purposes". Department of Defense, *Law of War Manual* (December 2016) 944, para 14.10.4.

[47] Speech of Chen Yixin, Secretary-General of the Central Political and Legal Affairs Committee on Xi Jinping Thought on Rule of Law. Translation and analysis done by Manoj Kewalramani on 4 April 2021. https://trackingpeoplesdaily.substack.com/p/chen-yixin-on-xi-jinping-thought accessed 29 October 2021.

[48] See also the *Nuclear Tests case* at the International Court of Justice (ICJ) and the loose language with does not prohibit explicitly the carrying of nuclear test by the contracting parties of the 1963 Partial Nuclear Test Ban Treaty.

Additionally, the term "orbit" must cover all types of orbits,[49] which reduces considerably, as technology advances on low orbit satellites, attempts to water down claims of sovereign airspace beyond what is already recognized in international law. The 1966 ILA report in Helsinki and its modification adopted in 1968 in Buenos Aires reach consensus "[t]hat airspace sovereignty in no event extends as far as the lowest perigee of any satellite so far placed in orbit", to end up saying that "[t]he statement does not say that this consensus will necessarily extend to all future satellites".[50] In other words, nothing is carved in stone with respect to international space law and competing positions that may seek to shape the current legal framework.[51] The question of the "vertical sovereignty"[52] is a relevant example that has been subject of debate before the space age began. The right of absolute vertical sovereignty prevailed until the Chicago Convention 1944.[53] Before Sputnik's launch in 1957, both the USSR and the USA were in favour of absolute vertical sovereignty.[54] As counterbalance, in 1976 eight equatorial states asserted territorial claims to the geostationary orbit (36,000 kilometres), known as the Bogotá Declaration.[55] The majority of states refused this argument as it entailed the recognition of sovereignty into outer space, as both articles I and II of the OST explicitly disprove the conception of vertical sovereignty.

Outer space is not subject to national appropriation and there is no conventional binding norm that defines the upper limit of territorial airspace and outer space; hence, states acknowledge the existence of some kind of demarcation line.[56] There are divergent views between the way to delimit outer

---

[49] Low Earth and Geostationary orbits (LEO and GEO).
[50] Bin Cheng (n 33) 450 making reference to the ILA reports.
[51] Partial Test Ban Treaty, 1963; The Convention on the Prohibition of Military and Other Hostile Use of Environmental Modification Techniques (ENMOD), 1977 (with restriction on anti-satellite weapons – ASATs); International Code of Conduct against Ballistic Missile Proliferation (ICOC), (25 November 2002, The Hague) and many others on ballistic matters (ABM, SALT II, START, MTCR, The Wassenaar Arrangement, ITARs, EU Law on export control); Geneva Convention and its Protocols.
[52] There are many hurdles to define this term because of the lack of a natural boundary separating air and space.
[53] The Convention on International Civil Aviation, signed at Chicago on 7 December 1944 (15 U.N.T.S. 295)
[54] See further in Dean N. Reinhardt, 'The Vertical Limit of State Sovereignty' (2007) 72(1) *Journal of Air Law and Commerce* 65, 81-88.
[55] Declaration of the First Meeting of Equatorial States (3 December 1976) [Bogotá Declaration], ITU Doc WARC-BS (1977) 81-E. The participant states were Brazil, Colombia, Congo, Ecuador, Indonesia, Kenya, Uganda and Zaire.
[56] Baker Spring, 'An Inchoate Process for the International Regulation of Military Activities in Space' (2006) 1(1) *Space and Defence Journal* 1, 7.

space and national airspace. The dissenters are divided in two camps, the functionalist and the spatial one. For the functionalists it is the nature of the act that counts while for the "spatialists" is the locus that commands any assessment.[57] In the first approach it could be said that the functionalist approach of outer space lacks the "reality check" of how current *lex lata* works and looks forward innocently to *lex ferenda*, while the spatial one resonates in the current practice, for instance, of reconnaissance ships and aircrafts,[58] which actually would have a parallel to spacecraft's stationary or passage activities in outer space. However, the reality is that when questions are addressed to grant or exercise the right of passage in matters related to outer space the functional approach may play a more significant and practical role. Actually, nations claiming vertical sovereignty and therefore the need of consent[59] will have to deal with functional explanations on distinguishing between military and non-military space objects and eventually if the non-military objects are commercial or non-commercial or if they have a nuclear purpose or not. There is certain confusion, or 'interested' disagreement, on these matters which may amount to Lawfare. The states that appear to support this mind-set usually make claims or run a consistent practice that uses a generous interpretation of the sovereign airspace concepts in order to project them into outer space. This attitude intends to shape the current undefined legal framework for the purpose of creating a *lex ferenda* in favour of their interests and eventually turning it into *lex lata*. In other words, we will witness shaping international legal rules with the aim to obtain strategic advantage for reaching objectives which would otherwise have been impossible to achieve through for example military means.

Several states[60] are preparing themselves to take advantage of outer space and may do so due to the existing legal vacuum within the space legal regime, which enable them to project both their interests and technical

[57] See further on Andrea J. DiPaolo, 'The definition and delimitation of outer space: the present need to determine where "space activities" begin' (2014) 39 *Annals of Air & Space Law* 623, 628.
[58] Bin Cheng (n 33) 446.
[59] The practice on the right to (peaceful) passage started emerging since the beginning of the space age and has been asserted by many scholars and states (but not all of them). Existing customs can be nullified or even changed through state practice undertaken in conjunction with an assertion that such practice is consistent with international law. Orde F. Kittrie, *Lawfare – Law as a Weapon of War* (Oxford University Press, 2016) 167.
[60] In 2008, the U.S. Annual Report of China Economic and Security Review Commission already showed concern regarding China's use of "legal warfare" or "lawfare" as a pre-emptive strategy for advancing its positions in outer space. *U.S. – China Economic and Security Review Commission*, Annual Report to Congress 161 (2008) 157.

capacities. The 1979 Soviet Working Paper was an attempt to bring space powers to terms with a common understanding of the limits of the sovereign airspace that did not materialize. The Soviet Union proposed that the region above 100 (110) kilometres altitude from the sea level of the Earth should be considered as outer space, and the boundary between air space and outer space requires the agreement among states via treaty establishing an altitude not exceeding 100 (110) kilometres above sea level.[61] The paper ends by proposing that States shall retain the right of passage of the territory of other States below the 100 (110) kilometres for the purposes of reaching orbit or returning to the Earth. The Soviet Union claimed a right of passage with certain similarities to that under general public international law applicable to territorial seas and as innocent passage.[62] In comparison, the USA has acknowledged that a definite line should not be drawn until "absolutely necessary" and that geostationary orbit cannot be subjected to the sovereignty of States or that States may have preferential rights to the use of such orbits.[63] The recent 2020 USA National Space Policy also asserts that space systems of all nations have the right to pass (formerly as "right to passage" in the 2010 USA National Space Policy) through and conduct operations in space without interference.[64]

Kittrie submits that the Chinese approach to outer space with respect to its thrust on imposing vertical sovereignty, *cujus est solum*, *ejus est usque ad coelum*, is linked to its technological disadvantage in space, which is obviously catching up with the USA, Europe and Russia year by year.[65] In any case, the idea of vertical sovereignty may well be accommodated in the mind of many others since this concern is out of the scope of the current outer space legal framework. However, the concern of outer space delimitation would require

---

[61] UNGA, 'Approach to the solution of the problems of the delimitation of air space and outer space' Union of Soviet Socialist Republics: working paper. USSR, 1979 https://digitallibrary.un.org/record/1863?ln=en accessed 29 October 2021.

[62] In 1996, the Russian Federation answered to a Questionnaire proposed by the UN and followed the same approach. UN Committee on the Peaceful Uses of Outer Space, *Questionnaire on possible legal issues with regard to aerospace objects: replies from Member States*, U.N. Doc A/AC.105/635/Add.1, 6-7 (15 March 1996). Available at http://www.unoosa.org/pdf/reports/ac105/AC105_635Add1E.pdf accessed 29 October 2021.

[63] U.S. Department of State, *85. U.S. Statement, Definition and Delimitation of Outer Space And The Character And Utilization Of The Geostationary Orbit, Legal Subcommittee of the United Nations Committee on the Peaceful Uses of Outer Space at its 40th Session in Vienna from April*, available at https://2009-2017.state.gov/s/l/22718.htm accessed 29 October 2021.

[64] White House, *National Space Policy of the United States of America*, 3. Available at https://spp.fas.org/eprint/nsp-2020.pdf accessed 29 October 2021.

[65] Orde F. Kittrie, *Lawfare – Law as a Weapon of War* (Oxford University Press, 2016) 168-169.

legitimacy subsumed to the compliance with international law both conceptually and temporarily,[66] which would not be the case here since outer space is part of the commons, and thus not subject to single state sovereignty. Article 1(2) of the OST confers free exploration and use by all states, as well as free access to all areas of celestial bodies. Moreover, China's approach is obviously "astropolitik"[67] with the aim to extend supremacy in outer space. The above is confirmed by Xi Jinping thought on Rule of Law in 2021: "[F]oreign hostile forces are a big threat to our containment and suppression. They stubbornly adhere to hegemonic thinking and 'Cold War' thinking (…). This reminds us that competition among major powers today is mainly a competition of systems and rules. Jinping's thoughts on the rule of law must be analysed to use legal tools in better ways to protect the country's reputation and essential concerns in accordance with the law".[68]

Finally, the fact that there is not yet an agreement on the limits of the sovereign airspace is tantamount to say the conflict is served and somehow favours space powers. It can be easily anticipated that technology will "democratise" the access to outer space and all states will have the potential to use it; but the initial space powers, at that point, would have already taken advantage and created irreversible practices. The vagueness in outer space legal framework must not be seen as a disadvantage for law-abiding states, but an opportunity to both reaffirm the basics of the principles of public international law and refuse interest-oriented interpretations of that fluid legal framework.[69]

Conclusion

The outer space regime is challenging mainly because of the lack of a clear legal framework. Hence, transparency and information sharing necessarily will need to be strengthened specially if states (separately or jointly within the context of international organizations) decide to launch (AI) space assets in order to clarify areas such as jurisdiction and control over the space object and over any personnel on-board the object. The Alliance needs to foster deterrence[70] and resilience and be ready to act within a space domain

[66] Bellflower (n 26) 121.
[67] Bellflower (n 26) 123 referring to Everett C. Dolman, *Astropolitik: Classical Geopolitics in the Space Age* (Psychology Press, 2002) 15.
[68] Speech of Chen Yixin (n 45).
[69] I.e., to prevent the application of Hadeisian Lawfare. For Zeusian and Hadesian Lawfare see Andres B. Munoz Mosquera & Sascha Dov Bachmann (n 10)
[70] To be more specific, systems that use AI will become essential to strategic security and they may be useful to deter potential adversaries. James Kraska, 'Command Accountability for AI Weapon Systems in the Law of Armed Conflict' (2021) 97 *International Law Studies* 407, 426.

where disruption and denial is likely to be the norm. This approach would be constructive and effective as many stakeholders rely on space infrastructure for their daily activities and conflict escalation in outer space could have overwhelming effects on the parties involved. In addition, this context is a great opportunity to strengthening NATO's ties with other International Organizations such as the International Telecommunication Union (ITU), the European Union (EU) or the European Space Agency (ESA) as all of them have important regulatory roles in this field and related to international relations.

An initial key factor is to address the question of delimitation of outer space to define roles and responsibilities – and hold possible stakeholders accountable. States have jurisdiction over individuals or vehicles possessing its nationality travelling in outer space; claiming territorial sovereignty over any portion thereof is not possible. Therefore, states may not have the right to interfere in other space activities that incidentally take place within their airspace. Then, allocation of accountability (Effective Control, Overall Control or Personal Control) would be highly desirable in the space domain particularly in the context of space as a possible warfare domain. As alternative approaches to fill in the gaps that the limited reach of state responsibility entails would be, e.g., lowering the thresholds of control, attributing responsibility for omissions, recognition of shared responsibility among actors involved.[71] In addition, states need to be aware of the risks associated with the use of AI weaponry (in the medium term) and those activities that may cause further space debris, and any damage originated from them may lead to both state liability and environmental concerns.

Space might become a new theatre of operations and new rules aimed at regulating human conduct (including AI in the medium term) need to be sought and fostered. This situation presents challenges for law-abiding states, which need to confirm and reaffirm the basics of the principles of public international law, refuse interest-oriented interpretations of outer space legal framework, and reinforce the RBIO.[72] The fact that some states may opt for soft law instruments to develop and deploy some types of weapons (e.g. AI-based) may disguise their real intentions. The lack of a precise international framework

[71] Kristen E. Boon, 'Are control tests fit for the future? The slippage problem in attribution doctrines' (2014) 15(2) *Melbourne Journal of International Law* 1, 3.
[72] Chatham House, 'Ideas for modernizing the Rules-Based International Order' (Chatham House Expert Perspectives 2019) available in https://www.chathamhouse.org/sites/default/files/publications/research/2019-06-10-Expert-Perspectives.pdf accessed 29 October 2021.

may lead states not to be aware of their international obligations in this field.[73] In the meantime, this situation requires attention from States and international organizations such as NATO, also in the legal field in order to be sufficiently (legally) vigilant. This will enhance the Allies' legal resilience and bring to the table the deterrence and tools for an effective defence of NATO democracies and compliance with the Rule of Law[74] as one of the fundamental principles of NATO.

***

[73] See discussion in Jack M. Beard, 'Soft Law's failure on the horizon: The international code of conduct for outer space activities' (2017) 38(2) *University of Pennsylvania Journal of International Law* 335, 361-367.

[74] The Preamble of the Washington Treaty states: "[T]he Parties to this Treaty (…) are determined to safeguard the freedom, common heritage and civilisation of their peoples, founded on the principles of democracy, individual liberty and the rule of law." North Atlantic Treaty (Washington, D.C., signed 4 April 1949, entry into force 24 August 1949), 34 UNTS 243.

Source: www.nato.int

NATO Space Policy in the light of the Prevention of an Arms Race in Outer Space (PAROS) initiative: Legal consideration[1]

by Professor George D. Kyriakopoulos[2]

Introduction: Military space activities under international law

Military, non-aggressive, activities of states in outer space have existed since the beginning of the space adventure of humankind, mainly through the use of reconnaissance and early warning satellites. During the very early phase of space activities, the peaceful nature of space activities was put forward in an absolute manner: UN General Assembly Resolution 1148 of 1957 stated in

[1] **DISCLAIMER**: The views expressed in this article are solely those of the author and may not necessarily represent the views of NATO, Allied Command Operations, or Allied Command Transformation, or of their affiliated organizations.

[2] George D. Kyriakopoulos, Assistant Professor of International Law, School of Law, National and Kapodistrian University of Athens, Tel. +306947837333, Email: yokygr@gmail.com Member of the International Institute of Space Law (IISL); Point of contact (Greece) for the European Center of Space Law (ECSL); Member of the Space Law Committee of the International Law Association (ILA); Since 2016, Member of the Greek Delegation at ICAO and the UNCOPUOS (Legal Subcommittee and the Plenary).
1/3/2019 – 31/8/2019, Visiting Professor, Institute and Centre of Air and Space Law, Faculty of Law, McGill University, Montreal, Canada; 2014-2018, Visiting Professor in Air & Space Law, Panteion University, Athens, Greece; 2014-2015, Visiting Professor in Space Law, Université Nice Sophia Antipolis, Faculté de droit et science politique, France.

explicit terms that "the sending of objects through outer space shall be *exclusively* for peaceful purposes"[3], whereas Resolution 1348 of 1958 recognized that "it is the common aim that outer space should be used for peaceful purposes *only*"[4]. However, one year later (1959), Resolution 1472 used a more flexible language on the subject, just "recognizing the common interest of mankind as a whole in furthering the peaceful use of outer space"[5] and Resolution 1721 (1961)[6] followed in exactly the same vein. Last but not least, the famous Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space (1963)[7], although considered to encompass a preliminary version of the fundamental "space" principles, it merely refers, in its Preamble, to "the common interest of all mankind in the progress of the exploration and use of outer space *for peaceful purposes*". This language was again repeated in the Preamble of the Outer Space Treaty of 1967[8], under which the exclusive nature of the peaceful use of outer space is guaranteed only with regards to the Moon and other celestial bodies (Article IV para. 2)[9].

Considering the above, the Outer Space Treaty, while prohibiting the placement and use of weapons of mass destruction in outer space (Article IV para. 1)[10], does not contain an explicit provision prohibiting military activities in space. Consequently, military space activities that take place "elsewhere than on the Moon and other celestial bodies" can be carried out as long as international space law and general international law are respected. As

---

[3] A/RES/1148(XII), Regulation, limitation and balanced reduction of all armed forces and all armaments; conclusion of an international convention (treaty) on the reduction of armaments and the prohibition of atomic, hydrogen and other weapons of mass destruction (14 November 1957).
[4] A/RES/1348(XIII), Question of the Peaceful Use of Outer Space (13 December 1958).
[5] A/RES/1472(XIV), International Cooperation in the peaceful uses of outer space (12 December 1959).
[6] A/RES/1721(XVI), International co-operation in the peaceful uses of outer space (20 December 1961).
[7] A/RES/1962(XVIII), Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space (13 December 1963).
[8] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, adopted on 19 December 1966, opened for signature on 27 January 1967, entered into force on 10 October 1967, 610/U.N.T.S./205 (hereinafter "Outer Space Treaty" or "OST").
[9] The relevant wording of Article IV para. 2 is as follows: "*The Moon and other celestial bodies shall be used by all States Parties to the Treaty exclusively for peaceful purposes…*"
[10] …which reads as follows: "*States Parties to the Treaty undertake not to place in orbit around the Earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction, install such weapons on celestial bodies, or station such weapons in outer space in any other manner*".

already mentioned, such activities must be of a non-aggressive nature, in order for them to be in line with the prohibition of the use of force in international relations[11], enshrined in Article 2 para. 4 of the UN Charter, with the obligation of States to seek a peaceful settlement of their disputes, as reflected in Article 33 of the UN Charter, as well as with the "peaceful" nature of space operations, within the limits already exposed therein.

As already mentioned, military activities in outer space are in principle regulated by article IV of the 1967 Outer Space Treaty. Furthermore, military activities that would be permissible under space law must also be in line with Article 2 para. 4 of the UN Charter. It should, however, be further noted that, since space activities must take place "in accordance with international law, including the Charter of the United Nations"[12], the "inherent" right to self-defence, in accordance with the Charter (Article 51) and customary international law, also applies to space activities, despite the restrictions imposed by Article IV of the Outer Space Treaty.

I. Weaponisation of Outer Space

The term "weaponisation of outer space" refers to the placement of *offensive* weapons in outer space, including the development of weapons systems on Earth whose mission is to destroy targets in space. The current legal framework does not prevent states from placing conventional weapons in space and relevant scenarios have been developed in military circles. Thus, the general debate on the weaponisation of outer space is still on-going.

According to existing scenarios, space devices can be used to destroy targets on Earth (e.g. use of space for missile interception), while cyber-attacks against satellites is still a matter of discussion. The situation is made even more complex by the "dual-use" nature (civil/military) of most space systems. It is important to note that, to date, those countries that have the necessary technology to deploy and use weapons in outer space (US, Russia, China) have refrained from doing so. Hence, nowadays, the international practice is encouraging, in terms of avoiding aggressive actions in outer space.

Anti-satellite weapons (ASAT) are a good example, as they have already been used to destroy (friendly) satellites in orbit as part of military tests. The following incidents have been documented in international practice and

[11] See also, in this respect, United Nations General Assembly Resolution 3314 (XXIX), Definition of Aggression.
[12] Outer Space Treaty, Article III.

clearly show the consequences of using weapons in space, even as an exercise or test:

- On January 11, 2007, a Chinese single ballistic missile hit a (Chinese) aging, cube-shaped, weather satellite in Low Earth Orbit (LEO), at 850 km above the Earth's surface. The Chinese government acknowledged the incident only twelve days after. The satellite destruction created a large amount of space debris.

- On February 21, 2008, a malfunctioning U.S. military "spy" satellite was intentionally destroyed by a modified ballistic missile fired from a U.S. military vessel. Prior to the destruction, the U.S. Department of Defense justified the operation by the fact that the satellite would enter Earth's atmosphere carrying a fuel tank full of hydrazine that would survive re-entry.

- On March 27, 2019, India used an ASAT weapon against a satellite in LEO. According to the Indian Minister of Foreign Affairs, the test was conducted in such a (low) altitude in order to ensure that the resulting debris would fall back to Earth. However, according to NASA sources, 49 pieces of debris were still in orbit as of 15 July 2019.

- On April 15, 2020, The U.S. Space Command announced that Russia had conducted a direct ascent anti-satellite missile test.

Further, the French Space Command (CDE), created in 2019, launched its first military space exercise, called ASTERX, in March 2021, with the participation of the US Space Force and the German Space Situational Awareness Centre. The scenario of the exercise focused on a space attack against a State under French protection, with particular emphasis on the monitoring of a space object during its re-entry into the atmosphere, of an anti-satellite weapon fire, and of a satellite being approached for espionage[13].

It is thus clear that the use of weapons in the space domain can have devastating effects on the space environment, through the creation of a significant amount of space debris, so as to generate serious threats to the integrity of Earth orbits and the security of space objects (mainly satellites) in them. Considering that space debris can cause "harmful interference" to the activities of other States in their "peaceful exploration and use of outer space", Article IX of the OST provides that the State planning the use of an ASAT

[13] See the info in https://www.aerotime.aero/27437-asterx-france-starts-first-military-exercise-in-space (last visit on 5.7.2021).

weapon capable of creating space debris should initiate "international consultations" with the potentially affected outer space users, before proceeding to the relevant operation.

The issue of weaponisation of outer space has been on the agenda of the UN Conference on Disarmament (CD) since the early 1980s. In 1985, a committee was set up within the Conference in order to address the key issues related to the "prevention of an arms race in outer space" (PAROS), such as the protection of satellite systems, the use of nuclear power sources in space activities and the adoption of relevant confidence-building measures. In 2008, China and Russia jointly introduced to the CD a draft convention on the prevention of the installation of weapons systems in outer space. On 10 June 2014, Russia submitted to the CD an updated draft of this Convention ("PPWT", Draft Treaty on the Prevention of the Placement of Weapons in Space, the Threat or Use of Force Against Space Objects). However, the relevant discussions did not result in the adoption of an internationally binding text on the subject.

With the Resolution A/RES/65/68 (2011), the UN General Assembly requested from the UN Secretary General to set up a Group of Governmental Experts (GGE) to conduct a Transparency and Confidence-Building Measures (TCBMs) survey. In its report, submitted to the General Assembly in 2013[14], the GGE set up a set of TCBMs in outer space (information exchange, risk reduction, exchange of expert visits, etc.), including the proposal to establish coordination among the Office for Disarmament Affairs, the Office for Outer Space Affairs and other relevant UN entities. At the same time, the UN General Assembly has endorsed, and further encouraged (A/RES/68/50), the implementation of the TCBMs. Although it is considered that the TCBMs are non-binding, their implementation can help increasing the security, safety and sustainability of outer space. In any case, the issue of weaponisation of outer space still remains open.

In 2017, a new GGE was established, pursuant to UN General Assembly Resolution 72/250 (24.12.2017), in order to "consider and make recommendations on substantial elements of an international legally binding instrument on the prevention of an arms race in outer space, including, inter alia, on the prevention of the placement of weapons in outer space." Although the Group met in two sessions at the UN Office in Geneva, in August 2018 and

[14] A/68/189, Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities, Note by the Secretary-General, 29.7.2013.

in March 2019, its members did not reach a consensus on a substantive report.

Through recurring resolutions, the UN General Assembly, recognizing the importance of the TCBMs, has consistently urged the States members to "contribute actively to the objective of the peaceful use of outer space and of the prevention of an arms race in outer space" (A/RES/74/32, 12.12.2019). Other recent UN General Assembly resolutions deal with international cooperation on the peaceful use of outer space (A/RES/74/82, 13.12.19), on the issue of transparency and confidence-building measures in outer space activities (A/RES/74/67, 12.12.19), on the prevention of an arms race in outer space (A/RES/74/32, 12.12.19), on no first placement of weapons in outer space (A/RES/74/33, 12.12.19) and on further practical measures for the prevention of an arms race in outer space (A/RES/74/34, 12.12.19). The fact that the United Nations General Assembly adopted, only during its 2019 session, a significant number of resolutions that directly or indirectly address the problem of weaponisation of outer space demonstrates the growing interest of the international community in the prevention of a race between States to place weapons in outer space.

II. NATO Space Policy and compatibility with international law

1) The North Atlantic Treaty and the UN Charter

It is evident from a consideration of the fundamental provisions of the North Atlantic Treaty[15] that this international instrument is in line with the basic requirements of the Charter of the United Nations.

The Preamble of the Treaty mentions that:

The Parties to this Treaty reaffirm their faith in the purposes and principles of the Charter of the United Nations and their desire to live in peace with all peoples and all governments.

…whereas Article 1 builds upon fundamental obligations of international law in force (including the UN Charter) such as the peaceful settlement of international disputes and the prohibition of the use of force in international relations:

Article 1

The Parties undertake, as set forth in the Charter of the United Nations, to

[15] North Atlantic Treaty, Apr. 4, 1949, 34 U.N.T.S. 243.

settle any international dispute in which they may be involved by peaceful means in such a manner that international peace and security and justice are not endangered, and to refrain in their international relations from the threat or use of force in any manner inconsistent with the purposes of the United Nations.

Besides, Article 5, which is the cornerstone of the North Atlantic Alliance, establishes a system of collective self-defence which is within the limits set by Article 51 of the Charter (self-defence against an armed attack, which shall cease when the UN Security Council takes action):

Article 5

The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.

Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security.

Moreover, the "primary responsibility" of the UN Security Council is explicitly recognized:

Article 7

This Treaty does not affect, and shall not be interpreted as affecting in any way the rights and obligations under the Charter of the Parties which are members of the United Nations, or the primary responsibility of the Security Council for the maintenance of international peace and security.

NATO's space strategy is essentially built within these institutional frameworks.

2) NATO's Space Strategy in the context of international law and space law

NATO's Space Policy constitutes a very pertinent example of how space

security is understood at the regional level. The foundations were laid in the 2018 NATO Brussels Summit when NATO Leaders recognised that "space is a highly dynamic and rapidly evolving area, which is essential for the Alliance's security". NATO's Space Policy was adopted at the June 2019 Defence Ministers' meeting. At the December 2019 NATO Summit in London, NATO Member States declared space "a fifth operational domain, alongside air, land, sea and cyberspace, recognising its importance in keeping [NATO States members] safe and tackling security challenges, while upholding international law".

In particular:

The Organization feels that there are threats for the Alliance in connection with outer space:

"The evolution in the uses of space and rapid advances in space technology have created new opportunities, but also new risks, vulnerabilities and potential threats. While space can be used for peaceful purposes, it can also be used for aggression. Satellites can be hacked, jammed or weaponised, and anti-satellite weapons could cripple communications and affect the Alliance's ability to operate.

Some countries, including Russia and China, have developed and tested a wide range of counter-space technologies that could restrict Allies' access to, and freedom to operate in space. Various risks to space systems are increasing and can harm Allies' security and commercial interests[16]".

In this respect, it is important to stress that, in outer space, NATO intends to build on the corresponding national programmes of its member States, in accordance with international law and without seeking to place weapons in space:

"NATO is an important forum for Allies to share information, increase interoperability and coordinate actions. The Alliance is not aiming to develop space capabilities of its own and will continue to rely on national space assets. NATO's approach to space will remain fully in line with international law. NATO has no intention to put weapons in space"[17].

The question remains, however, what the Alliance's reaction will be in

[16] https://www.nato.int/cps/en/natohq/topics_175419.htm (last visited on 24.05.21).
[17] https://www.nato.int/cps/en/natohq/topics_175419.htm (last visited on 24.05.21).

the event that weapons in space are deployed by one of its members.

In particular, the Alliance's space policy highlights the following "critical areas":

"From a security and defence perspective, space is critical for the Alliance, including in the following areas:

- *positioning, navigation and timing, which enables precision strikes, tracking of forces or search and rescue missions;*
- *early warning, which helps to ensure force protection and provides vital information on missile launches;*
- *environmental monitoring, which enables meteorological forecasting and mission planning;*
- *secure satellite communications, which are essential for missions to enable consultation, command and control;*
- *intelligence, surveillance and reconnaissance, which are crucial for situational awareness, planning and decision-making"*[18].

At first glance, these "critical areas" seem to be within the scope of international law, particularly in relation to the use of force, as well as international space law. It is further noted that these areas essentially echo the "military-means-non-aggressive" concept, which is dominant in space relations and seems to be accepted by all States. Finally, the reference to "precision strikes", given its overall context, should be interpreted as referring to strikes of a defensive nature, as an implementation of the right to self-defence enshrined in the UN Charter and international customary law.

Conclusions

Space security is part of a broader security scheme in international affairs, the maintenance of which constitutes the fundamental purpose of the UN Charter. The deployment of military activities – in particular, the weaponisation of outer space - is a major challenge for the international security system.

The placement of weapons in outer space and on celestial bodies – despite its exclusively peaceful character – constitutes a threat, which has preoccupied the international community for a long time. So far, the discussions and deliberations within the framework of the UN Conference on

[18] https://www.nato.int/cps/en/natohq/topics_175419.htm (last visited on 24.05.21).

Disarmament have not been successful in adopting a binding international instrument. National security concerns are pushing some States to keep the debate on the placement of weapons in outer space open. The adoption of -voluntary- TCBMs as well as the repeated UN General Assembly resolutions on the prevention of an arms race in outer space at least demonstrate that there is a growing concern, at international level, about the need for multilateral action on this issue.

NATO's space policy, at least from the information that has been publically released so far, aims at using space applications and space assets in order to strengthen the operational infrastructure of the Alliance. At the same time, outer space is emerging as a new operational domain for NATO. However, at this stage, this policy is within the limits set by modern international law and does not seem to entail the placement of weapons in outer space.

***

Source: https://ac.nato.int/

In pursuit of the best standards: what material and legal interoperability for NATO forces? [1]

by Laetitia Cesari Zarkan[2]

Introduction

Back in 2019, space was in everybody's mouth as the North Atlantic Treaty Organization (NATO) recognised outer space as a new operational domain, and NATO Secretary General Jens Stoltenberg reminded everyone of the important role of the Alliance as a forum to "increase interoperability."[3] The distinction between space used as an operational and not as a warfighting domain offers an important backdrop to NATO when addressing the integration and interoperability of space-based assets. NATO has no plans to "weaponise" space[4] but intends to benefit from space assets belonging to

[1] **DISCLAIMER**: The views expressed in this article are solely those of the author and may not necessarily represent the views of NATO, Allied Command Operations, or Allied Command Transformation or of their affiliated organizations, or Luxembourg University.
[2] Laetitia Cesari Zarkan is a doctoral researcher in Space Law and Cyber Law at Luxembourg University.
[3] NATO – News, 'NATO Defence Ministers approve new space policy, discuss readiness and mission in Afghanistan' (*NATO*, 27 June 2019) https://www.nato.int/cps/en/natohq/news_167181.htm accessed 2 January 2021.
[4] Martin Banks, 'NATO names space as an 'operational domain,' but without plans to weaponize it' (*DefenseNews*, 20 November 2019) https://www.defensenews.com/smr/nato-2020-defined/2019/11/20/nato-names-space-as-an-operational-domain-but-without-plans-to-weaponize-it/ accessed 2 January 2021.

different NATO allies in support of its military operations.[5]

Does space matter for NATO?

Military outlays for space-related technologies have been made since the beginning of the Space Age on the national level.[6] When placed in outer space, assets have a persistent outreach over the ground at any time, providing a broader perspective due to the high altitude, and a better penetration as overflight restrictions do not hinder them.

The advantages mentioned above benefit military forces on the battlefield but also during the preparation of the missions. As of April 2021, NATO is conducting large operations for which the NATO alliance needs communication and intelligence capabilities to help them plan, program, and budget the missions. Space assets provide strategic communications between the forces, uninterrupted command and control, situational awareness, and precision strike capabilities, useful for deterrence purposes.[7] This way, space-based technology support military forces' capabilities to anticipate, communicate about, assess, and respond to emerging threats. Space systems provided by NATO member countries also underpin the alliance's general needs for collective defence, crisis response, disaster relief, and counter-terrorism.

In practice, NATO has managed to make the most of the national space assets provided by member countries to support joint military operations. Looking beyond commercial competition, the cooperative production of advanced space systems, made essentially by the United States (US) and its closest allies (France, Italy, and the United Kingdom),[8] is also a significant part of the equipment acquisition and an important cooperation step for the

---

[5] Alexandra Stickings, 'Space as an Operational Domain: What Next for NATO?' *RUSI Newsbrief,* (15 October 2020), https://rusi.org/explore-our-research/publications/rusi-newsbrief/space-operational-domain-what-next-nato accessed 2 January 2021.

[6] Kestutis Paulauskas, 'Space: NATO's latest frontier' (*NATO Review*, 13 March 2020) https://www.nato.int/docu/review/articles/2020/03/13/space-natos-latest-frontier/index.html accessed 2 January 2021.

[7] NATO Standardization Office (NSO), *Allied joint doctrine for the conduct of operations* (Allied Joint Publication 3 (AJP-03), Edn C Version 1, 2019) C-2.

[8] Kevin J. Scheid, 'What if NATO had no physical headquarters?' (2020) 3 NITECH - NATO Innovation and Technology, 12 https://issuu.com/globalmediapartners/docs/nitech_issue_03_june_2020?fr=sN2JmNzE0MTM2ODY accessed 2 January 2021; NATO – News, 'NATO provides state-of-the-art communication solutions to Allied Navies' (NATO, 27 May 2020) https://www.nato.int/cps/en/natohq/news_176046.htm accessed 2 January 2021.

alliance. A closer look, however, reveals that the US' longstanding footprint on standardisation procedures or equipment keeps influencing the design and manufacturing of new space technologies.

Balancing the space systems costs

Supporters of significant military spending on space promote the aforementioned enhanced and ubiquitous edge in joint-operations that it enables,[9] while opponents raise concerns over the existing US near-monopoly on the development and possession of advanced military space technologies.[10] Coordinating the forces' objectives require both fair burden-sharing and interoperable interfaces between states.

For NATO suppliers to collaborate in cooperative production programs, interoperability becomes a necessary development component.[11] Defined as "the ability to operate together using harmonised standards, doctrines, procedures and equipment,"[12] interoperability allows technical, procedural, and human coordination,[13] as well as the development of more affordable systems by reducing production and ownership costs.[14]

The limits of interoperability

In this Article, interoperability considerations are twofold: first involves standardisation around physical components, software and communications protocols and policy, the *material interoperability*, and second is the policy and legal challenge to define a common and consistent mind-set on rules-of-engagement, the *legal interoperability*.

On the one hand, material interoperability is an enterprise-level activity of the alliance. When developing or acquiring space technologies, NATO member countries must ensure they are interoperable, meaning the systems must be compatible with the other ones used by the other NATO allies and that

---

[9] NATO Science & Technology Organization, *Science & Technology Trends 2020-2040, Exploring the S&T Edge* (2020) 17.
[10] Le groupe de réflexions Mars, 'OTAN, inutile et indispensable' *La Tribune* (Paris, 20 April 2021).
[11] Thomas L. Koepnick, 'International Armaments Cooperation: a key to coalition interoperability' (2005) 28(1) DISAM Journal of International Security Assistance Management 21.
[12] NATO Standardization Office (NSO), *Allied joint doctrine (Allied Joint Publication 1 (AJP-01)*, (edn E version 1, 2017) LEX-5.
[13] *Ibid* 1-2.
[14] Koepnick, *supra* note 10.

logistics is interchangeable for joint operations.[15] Training makes the space systems even more interoperable for the mid- or long-term force planning. In peacetime, when national armed forces carry out exercises with standard materials and systems, they learn how to use them and, on a side note, are more likely to purchase similar assets later.[16] They also develop common risk mitigations measures for those space systems. Standardisation highly depends on national participation as NATO member countries have to ratify international standardisation agreements. Military forces are also entitled to subscribe to international standardisation to make sure they can develop and maintain defence equipment.

On the other hand, when carrying out an operation during an armed conflict, any coalition of states have to agree on collective priorities, common doctrines and thresholds.[17] The broad range of NATO activities requires coordination in the unfolding military operations, from the planning to the assessment. There is no common agreement on law application or enforcement, but a standard exists on rules of engagement training: NATO standardization agreement (STANAG) 2449.[18] This guideline provides for mutual approaches for NATO member countries when training their forces on the Law of Armed Conflict.[19] Nevertheless, the shortfall in convergent legal frameworks can cause inconsistent actions on the battlefield as a divergence in the decisions made during a joint mission is likely to raise tensions between allies.[20]

This article critically engages with the idea that interoperability poses legal problems and an unfair burden on the less developed members of the NATO alliance. This article presents a two-fold analysis of interoperability challenges in utilising space-based assets, particularly joint responsibility during hostilities. Considering the situation described above, ways to approach interoperability merit fresh reflection. To that end, this paper analyses how

---

[15] Christopher Ptachik, Edward Durell, and Robert Bamberg, 'Air Force Management of Materiel ISAs' (2014) Defense Standardization Program Journal 11-18. https://fdocuments.in/reader/full/natointernational-standardization-defense-standardization-impact-of-nato accessed 2 January 2021.

[16] Rainer L. Glatz and Martin Zapfe, 'NATO's Framework Nations Concept', 218 *CSS Analyses in Security Policy* (2017) 3.

[17] Kirby Abbott, 'A brief overview of legal interoperability challenges for NATO arising from the interrelationship between IHL and IHRL in light of the European Convention on Human Rights' (2014) International Review of the Red Cross 96 (893) 108.

[18] NATO STANAG 2449: Annual training on the law of armed conflict, June 26, 2019.

[19] Jody M. Prescott, 'Training in the Law of Armed Conflict – A NATO Perspective', (2008) 7(1) Journal of Military Ethics 68.

[20] Kirby Abbott, *supra* note 16, at 111-112.

material interoperability developed and what it means for the NATO allies. Legal interoperability is also an ambiguous point that leaves room to think about NATO member countries' responsibility. This article examines several alternative approaches and proposes suggestions for how NATO member countries can build stronger and fairer relationships.

I. From national standards to STANAG: a first-come first-served approach for material interoperability

At the 2014 Wales Summit, the NATO allies committed to dedicating 2% or more of their gross domestic product (GDP) to defence spending.[21] To meet the challenges the NATO allies could potentially face in the future and comply with the collective defence principle set out in Article 5 of the Washington Treaty, the participants to the meeting of the North Atlantic Council in Wales engaged to provide more resources, capabilities, and political will as required by the NATO Readiness Action Plan.[22] In 2020, twelve NATO member countries achieved this GNP spending goal – 3 more than in 2019.[23]

The global hegemonic position of the US

Even though the NATO allies' military spending is globally rising, the US still supports a significant share of the NATO burden and is the leading equipment supplier globally.[24] NATO allies, especially in Europe, highly depend on the US industry and US capabilities for their defence. For the NATO alliance to cooperate efficiently, they have to overcome "technological and doctrinal discrepancies", as NATO Deputy Secretary General Mircea Geoană stressed during a webinar on interoperability held on 16 July 2020.[25] NATO established STANAGs to facilitate interoperability between the US and its European NATO allies.[26] This way, the different technologies are conceived with the same standards, so the information transmitted is read and translated into formats that a system understands. Even though interoperability and common

[21] Wales Summit Declaration 2014.
[22] NATO, 'Readiness Action Plan' (NATO, 23 March 2020) https://www.nato.int/cps/en/natohq/topics_119353.htm accessed 2 January 2021.
[23] Stockholm International Peace Research Institute (SIPRI), 'World military spending rises to almost $2 trillion in 2020' (SIPRI 26 April 2021) https://sipri.org/media/press-release/2021/world-military-spending-rises-almost-2-trillion-2020 accessed 2 May 2021.
[24] SIPRI, 'Global arms industry: Sales by the top 25 companies up 8.5 per cent; Big players active in Global South' (SIPRI 7 December 2020) https://www.sipri.org/media/press-release/2020/global-arms-industry-sales-top-25-companies-85-cent-big-players-active-global-south accessed 2 January 2021.
[25] NATO – News, 'Emerging and disruptive technology webinar on interoperability' (NATO, 16 July 2020) https://www.nato.int/cps/en/natohq/news_177301.htm accessed 2 January 2021.
[26] AJP-01, *supra* note 11, 1-2.

standards allow for better detection and assessment of the operational risks, they also pose design and manufacturing constraints for small suppliers that must be compliant, even when developing new technologies, with the hegemon's rules – in this case, the US.

Most equipment purchases are made by NATO through direct commercial sales to private companies or groups of companies and often include an agreement in the form of cooperative Memorandum of Understandings (MOU). Even if NATO has the choice between competitive products provided by its pool of suppliers, the NATO Support and Procurement Agency will tend to favour the most interoperable ones, according to the standards in place.[27] In this regard, with the historically strong position of the US as a global supplier, the risk would be that US-based industry influence technical standards to further their commercial interests when developing technologies and the NATO allies must comply with longstanding US standards nonetheless.

Balancing national commercial interests and the interests of the Alliance

This leading position gives the US-based industry a competitive advantage as national and private companies keep providing the technologies and are subsequently more likely to bottom-up the best practices that the NATO Standardisation Office will adopt. In 2019, for instance, the US company Lockheed Martin announced the completion of work to enhance the NATO interoperability of uncrewed air vehicles that would be improving the potential for new sales internationally. According to the US company, this improvement was primarily due to "the sharing of knowledge and information and integration" of Lockheed Martin's software.[28]

On the competition side, this state of affairs can create disparities for those states that would like to innovate and develop new technologies. It would cost them much money not to toe the line when developing new systems. In 2013 an opposite situation illustrated how the NATO European allies sometimes could not coordinate internationally or follow NATO standards when researching and developing new technologies. In 2013, Germany had decided to withdraw its purchase interest in the Euro Hawk reconnaissance

[27] NATO STANAG 2449, *supra* note 17.
[28] Sky-Watch, 'Lockheed Martin and Sky-Watch to enhance NATO-interoperability' (11 October 2019) https://sky-watch.com/news/lockheed-martin-and-sky-watch-to-enhance-nato-interoperability/ accessed 2 January 2021.

drones as the country realised that meeting the NATO standards would have required an additional cost of 500 million to 600 million euros.[29] A French Member of the National Assembly Commented during a Commission on National Defence and Armed Forces that the US being the most powerful NATO nation, any new system they conceive would almost necessarily become the NATO standard.[30] This development would imply factory standards adjustments for the NATO allies, so they don't depend too much on the US for the conception of new systems. Given that by developing their own systems, a NATO ally would run the risk of no longer being interoperable with the other NATO allies, which could cause them to be "one war behind from a technological point of view".[31] By doing so, the smaller players have to opt to concede their intellectual property rights, so their technology is interoperable with existing systems. Back in 1996, in a communication on *The Challenges Facing the European Defence-Related Industry, A Contribution for Action at European Level*, while recognising the strategic importance of standards for the efficiency of the internal market, the European Commission noted that care should be taken in the future to ensure that "the competitiveness of the EU defence industries" is not hampered.[32]

A slender protection for intellectual property rights

Setting the foundational standards that will define next-generation technologies allows the hegemon to be the one determining how to make systems interoperable. This strong position on the market can limit interoperability to a restricted set of systems and equipment, which can subsequently cause the reduction of choices for the NATO forces. It is mainly the case for space systems that need longer-term requirements because of their long lifespan. Once established, the rules behind the design and manufacturing of the assets are difficult to uproot. To ensure the alliance purchases their products and services, NATO suppliers have to collaborate and disclose their patent and intellectual property rights to make their interfaces interoperable. The smaller players have to comply with NATO standards even with the risk they would provide information to enable competitors to develop

[29] Reuters, 'Germany will not buy Euro Hawk drones - govt source' (14 May 2013) https://www.reuters.com/article/germany-arms-eurohawk-idUSL6N0DV31220130514
[30] NATO STANAG 2449, *supra* note 17.
[31] French National Assembly, Commission de la Défense Nationale et des forces armées, Travaux de la Commission, Tome VII Défense équipement des forces – dissuasion I (Dossier législatif n°3465, 2020).
[32] The Challenges Facing the European Defence-Related Indus (Communication from the Commission, 1996) COM (96) 10.

competing technologies. Pursuant to Article 7 of the Trade-Related Aspects of Intellectual Property (TRIPS), "the protection and enforcement of intellectual property rights should contribute to the promotion of technological innovation and to the transfer and dissemination of technology, to the mutual advantage of producers and users of technological knowledge and in a manner conducive to social and economic welfare, and to a balance of rights and obligations."[33] Article 7 of the TRIPS illustrates the need to balance proprietary rights and the larger interests of social welfare. Without this balance, the development of a technology or an innovative product is at stake as entities investing in inventions expect a return on investment.

However, in the space sector, the US' dominant position creates a quasi-monopolistic situation favouring the US-based industry, which benefits from the hegemon's standing.

Material interoperability of space systems: "historical standards" through the ages

In the 2000's, under the NATO SATCOM Post-2000 (NSP2K) program, satellite communications (SATCOM) capabilities have been used for expeditionary missions by NATO forces. France, Italy and the United Kingdom formed a consortium for 15 years (2005-2019) to provide NATO with access to SYRACUSE 3, SICRAL 1 and 1 bis and Skynet 4 and 5 geostationary satellites.[34] The three countries signed a MOU with the NATO alliance in 2004.

On this basis, France, Italy and the United Kingdom controlled the satellites through the Joint Program Management Office and the NATO Mission Access Centre.[35] The Joint Program Management Office was in charge of the overall management, including dialogue about NATO requirements. The NATO Mission Access Centre carried out daily operations and execution of the capacity on behalf of the countries, while the NATO Communications and Information Agency (NCI) managed the MOU and provided service allocation and network monitoring on behalf of NATO.[36] Under this cooperation,

---

[33] Annex 1C to the Marrakesh Agreement (General Agreement on Trade-Related Aspects of Intellectual Property, TRIPS) (15 April 1994) 1869 U.N.T.S. 299.
[34] NATO, 'SATCOM Post-2000 (Archived)' (NATO 23 April 2021)
[35] *Ibid.*
https://www.nato.int/cps/en/natolive/topics_50092.htm accessed on 2 May 2021; Space Daily, 'France And NATO Sign Satellite Communications Agreement' (3 December 2004) https://www.spacedaily.com/news/milspace-comms-04zzx.html accessed on 2 January 2021.
[36] Ibid; NATO, 'Satellite communications' (23 April 2021)

European countries have proved their capacity to work together efficiently, providing MILSATCOM capabilities that offered NATO access to the military Ultra High Frequency band and Super High Frequency (SHF) band. With this access, NATO forces could transmit significant amounts of data for tactical communications and transmissions with military hardening features based on common standards.[37] Hence, the NP2K program was designed to accommodate the 5 Kilohertz (KHz) and 25 KHz channels of legacy UHF systems, first employed in US Navy satellites and US Air Force satellites.[38] Remotely piloted aircraft such as the Northrop Grumman Block 40 Global Hawk,[39] the Boeing P-8A Poseidon,[40] and the Boeing E-3 Sentry[41] all rely on SATCOM for data transfer and, to a lesser extent, control.[42] Operated by the NATO's Alliance Ground Surveillance (AGS) system, based at Sigonella, Italy, Global Hawk is capable of collecting imagery over large areas and using the SATCOM architecture designed by the NCI. Since April 2016, the Luxembourgish government started providing NATO SHF band and commercial Ku band.[43] SATCOM supports the deployment of surveillance and mobility operations through the Alliance Ground Surveillance system as part of the Luxembourgish contribution in kind to NATO.

Under the contract concluded between the Luxembourg Authorities and NATO, Luxembourg acquires and the NCI Agency manages the services

https://www.nato.int/cps/en/natohq/topics_183281.htm accessed on 2 May 2021.

[37] Gordon Adams, Guy Ben-Ari, John Logsdon and Ray Williamson, 'Bridging the Gap – European C4ISR Capabilities and Transatlantic Interoperability' (The George Washington University, 2004) 20.

[38] Madhavendra Richharia and Leslie David Westbrook, 'Satellite Systems for Personal Applications Concepts and Technology' (2010) Wiley, 332.

[39] NATO, 'Alliance Ground Surveillance (AGS)' (NATO 23 February 2021) https://www.nato.int/cps/en/natohq/topics_48892.htm accessed on 2 May 2021.

[40] John Keller, 'Boeing looks into installing MUOS SATCOM system to improve communications aboard P-8A reconnaissance plane' (Military & Aerospace Electronics, 28 May 2020) https://www.militaryaerospace.com/communications/article/14176773/p8a-satcom-communications accessed on 2 January 2021.

[41] John Keller, 'Boeing to equip E-3 AWACS avionics with high-speed internet SATCOM capability in $50 million contract' (Military & Aerospace Electronics, 12 August 2020) https://www.militaryaerospace.com/communications/article/14181448/internet-satcom-awacs accessed on 2 January 2021; Boeing, 'E-3 Airborne Warning And Control System', Historical Snapshot https://www.boeing.com/history/products/e-3-airborne-warning-and-control-system.page accessed on 2 January 2021.

[42] Jim Winchester, The Phoenix has risen, interview with Laryssa Pattern and Ramon Segura' (2020) 3 NITECH - NATO Innovation and Technology, 78. https://issuu.com/globalmediapartners/docs/nitech_issue_03_june_2020?fr=sN2JmNzE0MTM2ODY accessed on 2 January 2021.

[43] GovSat, NATO AGS Contract awarded to GovSat (Press Release, 8 November 2016)

provided by GovSat, a public-private partnership between the Luxembourg Government and the private satellite operator SES, to create a link between the NATO Global Hawk unmanned aerial vehicles (UAV) and ground segment over the AGS operational area.[44] More recently, a new SATCOM program has replaced the NSP2K program from 1 January 2020. France, Italy, the United Kingdom and the US concluded a MOU to provide SATCOM services that would enable intelligence gathering and navigation, tracking forces worldwide and detecting missile launches.[45] For this NATO SATCOM Services 6th Generation program, the NCI Agency operates the satellite communications capability delivering services to NATO as a part of the deterrence and defence capacities of the Alliance until 2036.[46]

The International Telecommunication Union (ITU), leading United Nations agency for information and communication technologies, adopted instruments used for frequency allocations on a global scale, including specific provisions for the military use of frequency spectrum. However, in exceptional cases, extended to NATO forces, Article 48 of the ITU Constitution and paragraph 4.4 of the Radio Regulation provide exceptions to achieve flexibility of the radiofrequency spectrum.[47]

Nevertheless, with a fleet exclusively composed of US aircraft, there is a high probability SATCOM architecture complies with the US-industry originated standards that the other NATO allies will have to fit with in the long run, and that will serve as a reference for ITU purposes. As stated in an article published by the French company Thales about an anti-jam modem protecting satellite communications, "to meet the specific requirements of each customer, each country and each branch of the military, [the system] has had to adapt."[48] In other words, when inventing a new waveform protocol, Thales' engineers had

---

[44] *Ibid.*
https://govsat.lu/news/press-release-nato-ags-contract-awarded-to-govsat/ accessed 2 January 2021.
[45] NATO, 'NATO begins using enhanced satellite services' (12 February 2020) https://www.nato.int/cps/en/natohq/news_173310.htm accessed on 2 January 2021; NATO, 'Satellite communications' (23 April 2021) https://www.nato.int/cps/en/natohq/topics_183281.htm accessed on 2 May 2021.
[46] *Ibid.*
[47] NATO Joint Civil/Military Frequency Agreement (2002) https://halberdbastion.com/sites/default/files/2018-04/NATO-Joint-CivilMilitary-Frequency-Agreement_%282002-Dec%29.pdf accessed on 2 January 2021.
[48] Thales, 'Modem 21: A Dynamic of Innovation for Milsatcom Security' (News, 4 December 2018) https://www.thalesgroup.com/en/worldwide/defence/news/modem-21-dynamic-innovation-milsatcom-security accessed on 2 January 2021.

to comply with NATO standards so it could be integrated on board UAVs and fast jets to link them to satellites.[49]

When building the network architecture, NATO forces are likely to base the standards on the US remote aircraft that were used for decades by the AGS system.[50]

The current state-of-the-art described above has an interesting story to tell about innovation. Standards generally change much more slowly than new technologies conception. NATO forces will have to adjust equipment and systems with more diverse technologies if they want a military power that is able to adapt to all types of hostile operations and interference. This comes in handy for satellite operators and space beneficiaries, which will gladly benefit from increased competition that continues to drive down the cost of the materials. However, buying technologies developed outside of the NATO allies industry is not without risk. Any corrupted equipment or software can facilitate access to a system and subsequently wide swaths of sensitive data and control functions through the equipment architecture. These are strong factors that lead states to consider other commercial partnerships for the financial set-up of their national industry while being cautious when purchasing technologies from foreign countries.

II. Shaping minds for the legal course of action: building interoperability at the strategic, operational and tactical levels

For the past ten years, some NATO allies have taken on an increasing share of joint activities supported by space assets. Their level of investment in the space industry keeps growing without, for the moment, appearing to level off. Despite this increase, the US continues to assume the brunt of NATO operations.

The variety of mind-sets within NATO

During joint operations, the views of the NATO allies can differ on various points. No matter how much intelligence is provided or how good communications are between the NATO allies, NATO member countries' mind-sets are very diverse. Whether complete equality in burden-sharing or the involvement of national troops can or should be achieved in these realms is an open question. It is a question, however, that masks a much more serious issue

[49] *Ibid*
[50] Winchester, *supra* note 41, 80; Gordon Adams et al., *supra* note 36, 61.

for the NATO allies, particularly for those less developed countries and their capabilities and operational concepts becoming outdated or are incompatible with those of the US.[51]

At the operational level, the NATO commander is in charge of leading tactical activities to achieve the NATO alliance's strategic objectives. The Supreme Headquarters Allied Powers Europe (SHAPE) is in charge of preparing, planning, conducting and executing joint military operations, missions and tasks.[52] In this process, the expectation that all the NATO allies apply the same standards at the strategic, operational, and tactical levels is widely held by NATO which plans, budgets, and operates with its own objectives.

The importance of training and coordinating forces

NATO allies benefit from the training of their capabilities. Testing to which extent they are interoperable, knowing their skills and equipment and understanding their responsibilities improves their overall performance in more complex situations. Yet, even if NATO forces are trained with the same standards, it is only over time, when individuals and small groups interact, that they accommodate the workarounds and follow the same rules of engagement.[53]

Nevertheless, one of the rationales for the latter is not what the applicable law is or what the standards are but that getting forces into joint exercises helps to disrupt deeply rooted patterns and mind-sets of how to perform a mission.[54]

NATO plans a considerable number of exercises each year, including national and multinational exercises organised by the NATO allies. In 2020, the NATO allies had the opportunity to participate in 88 NATO military exercises and held 176 national and multinational exercises altogether.[55] For the year 2021, NATO plans to carry out 95 exercises, and the NATO allies intend to conduct

---

[51] Myron Hura, Gary McLeod, Eric V. Larson, James Schneider, Daniel Gonzales, Daniel M. Norton, Jody Jacobs, Kevin M. O'Connell, William Little, Richard Mesic, et al., *Interoperability A Continuing Challenge in Coalition Air Operations* (RAND Corporation 2000) 30.
[52] NATO, 'The NATO Command Structure' (Factsheet, 2018) 1 https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_02/1802-Factsheet-NATO-Command-Structure_en.pdf accessed on 2 January 2021.
[53] Myron Hura et al, *supra* note 50, 10 and 46.
[54] *Ibid.*
[55] NATO, ' Key NATO and Allied exercises in 2021' (Factsheet, 2021) 1 https://www.nato.int/nato_static_fl2014/assets/pdf/2021/3/pdf/2103-factsheet_exercises.pdf accessed on 2 May 2021.

220 national and multinational exercises.[56] The exercises are organised either in multi-domain, on the land domain, in the air domain, or are conducted as maritime operations. The troops can train specific skills such as "cyber defence, crisis response decision-making, Chemical, Biological, Radiological Nuclear defence, logistics, communications and medical activities".[57] As mentioned above, STANAG 2449 allows NATO member countries to adopt a common understanding of the Law of Armed Conflict when training their forces.[58]

Law of Armed Conflicts as a paradigm for legal interoperability

Change does not happen quickly, but without interactions and exchange of best practices, which are part of peacetime operations, a common doctrine is unlikely to be shaped, as even the strongest rules and standards are subject to interpretation. As a military alliance, NATO member countries have to spend more means coordinating their operations and policy decisions since a tremendous public interest exists in these issues. STANAG 2449 is a voluntary standard established by NATO to help ensure compliance with the Geneva Conventions and the Additional Protocols.[59] It provides common ground for training and implementation methodology of the Law of Armed Conflicts (LOAC) through the NATO forces. The military training dispensed to the troops at the national level provides an understanding of the minimum standards within subjects such as methods of warfare, protection of cultural property, the use of force in peacekeeping operations, or the commander's responsibilities.

According to STANAG 2449, the LOAC is applicable to a variety of situations. It is the case of armed conflict between states, when a state occupies another's state territory, during disputes related to the right of self-determination, and of internal armed conflicts in which dissident armed forces "under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement."[60] Conversely, it also applies to peace support operations not constituting armed conflict. A good understanding of LOAC allows the NATO allies to understand not only the individual phases but rather the overall effects of their missions, and to assess the impact made by their operations.

---

[56] *Ibid.*
[57] *Ibid.*
[58] Jody M. Prescott, *supra* note 18, 68.
[59] Ibid.
[60] NATO STANAG 2449, *supra* note 17.

What's in a Law? Or how to make space activities interoperable

Greater involvement of NATO forces in operations requiring the use of force, lethal or not, against opposing troops has led to a greater need for minimum standards regarding rules of engagement.[61] This need stems from two complementary questions: does LOAC bind NATO if all of its member countries have ratified the 1949 Geneva Conventions, and all but two have ratified Additional Protocols I and II to the Geneva Conventions? If so, do NATO member countries have to enforce the rules when carrying out joint operations? Today on the battlefield, a wide diversity of forces from different cultures and backgrounds composes NATO forces. During joint missions, some individuals or groups can fall short of the rules, especially if they haven't been trained to follow the standards applicable to armed forces and develop another mind-set off the beaten tracks.

Coalition operations supported by space-based assets may seem more complicated than it is in practice. As addressed in the introduction, space has been recognised as an operational domain, meaning that there is a greater reliance on the space domain and therefore, a growing need for safety measures 'precluding inherent malfunction and mitigating the risks of accidental damage that would be caused by or undergone by a space object, including its component parts.'[62] It is not to be confused with warfighting domain, even though the normalisation of space operations increase vulnerabilities of space-based assets and subsequent need for space security, understood as 'the protection of a space object, including its component parts, against the risk of intentional actions undertaken by external or unauthorized actors.'[63] The need for safety measures for all types of space assets will benefit all countries, but not all of them will have the willingness and money to invest in this matter. The political will is important, so, as for material interoperability, the US influence is significant, especially in space.[64] For instance, the Space Policy Directive 7 on Space-Based Positioning, Navigation, and Timing Policy adopted in January 2021 states the need to "maintain lead responsibility for negotiating with foreign defence organizations for any

[61] David Cloud, 'NATO Plans to Command 12,000 G.I.'s in Afghanistan' (The New York Times 29 September 2006).
[62] Laetitia Zarkan Cesari, 'What's in a word? Notions of "security" and "safety" in the space context' (United Nations Institute for Disarmament Research – UNIDIR, 2020) https://www.unidir.org/commentary/whats-word-notions-security-and-safety-space-context accessed on 2 January 2021.
[63] Ibid.
[64] Myron Hura et al, *supra* note 50, 52.

cooperation regarding access to or information about GPS military services."[65]

Whether they are space actors or space beneficiaries, many among the NATO allies will follow the same US practices and procedures they have followed for years, even though the non-US powerful NATO allies can provide good leverage on a case-by-case basis.[66] If the aim is to build a solid and coherent framework for the emerging space activities, nobody has succeeded yet. But if the aim is to support lagging NATO member countries in applying LOAC when using space-based assets for joint operations, there is a greater chance that legal interoperability works.

To get comprehensive space cooperation off the ground, awareness of the sector, transparency of the activities and rules of behaviour must spread. Intent to follow common standards must be followed up by action. Finally, even though US-European space collaboration is not without precedent, NATO commanders must find ways to consider all the various NATO member mind-sets when making decisions. This view on international cooperation can be seen in part in last year's US National Space Policy. The document emphasises the importance of strengthening "United States leadership in space".[67] This influence is twofold.

First, the US National Space Policy highlights the need for a framework that would include "the pursuit and effective implementation of best practices, standards, and norms of behaviour."[68] The NATO allies would set up this common framework by adopting "United States space regulatory approaches and commercial space sector practices".[69] In a very transparent way, the US National Space Policy draws out the US' strategy of carrying out diplomatic and public diplomacy efforts with its NATO allies, "to strengthen the understanding of, and support for, United States national space policies and programs and to promote the international use of United States space capabilities, systems, and services."[70]

Second, the National Space Policy clearly states the US intention to

---

[65] Memorandum on Space Policy Directive 7: The United States Space-Based Positioning, Navigation, and Timing Policy, 15 January 2021.
[66] Myron Hura et al, *supra* note 50, 41-42.
[67] National Space Policy of the United States of America, 9 December 2020, 3 https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/12/National-Space-Policy.pdf accessed on 2 January 2021
[68] US National Space Policy, 12.
[69] *Ibid*.
[70] *Ibid*, 13.

"facilitate new market opportunities for United States commercial space capabilities and services".[71]

In short: the NATO allies have to comply with their international obligations, they have to follow US standards even more, out of necessity. The classified policy adopted by NATO in 2019 is not a space strategy as it is the case for the US National Space Policy mentioned above. NATO Secretary General Jens Stoltenberg presented it as an overarching space policy approved by the NATO ministers. The fact that NATO allies manage to agree on a common space policy is encouraging not only for the protection of space systems[72] but also for international cooperation in this field, as internationally accepted behavioural norms on existing and potential threats and security risks to space systems still have to be developed.[73] The NCI Agency is increasingly using satellite communications delivered by commercial and national capabilities in support of military operations. To ensure coordination among the NATO allies, NATO needs to set up a comprehensive policy on providing and using space data, information and effects[74] and in this context, not focusing on the US and its closest NATO allies only but on all of the space beneficiaries.

One way to do it would be to carry out an open consultation within the NATO alliance, as is done in the General Assembly of the United Nations (UNGA). The UNGA recently adopted resolution 75/36, encouraging UN Member States "to study existing and potential threats and security risks to space systems."[75] This resolution calls for states to share their considerations about what "could be considered responsible, irresponsible or threatening and their potential impact on international security, […] to share their ideas on the further development and implementation of norms, rules and principles of responsible behaviours and on the reduction of the risks of misunderstanding

---

[71] Ibid.
[72] NATO, 'NATO Defence Ministers approve new space policy, discuss readiness and mission in Afghanistan' (27 June 2019) https://www.nato.int/cps/en/natohq/news_167181.htm accessed on 2 January 2021.
[73] Benjamin Silverstein, 'NATO's return to space', Commentary (War on the rocks, 3 August 2020) https://warontherocks.com/2020/08/natos-return-to-space/ accessed on 2 January 2021; Alexandra Stickings, *supra* note 4.
[74] Laryssa Patten, 'NCI Agency provides critical support to development of new NATO space policy' (NCI Agency Newsroom, 23 July 2019) https://www.ncia.nato.int/about-us/newsroom/nci-agency-provides-critical-support-to-development-of-new-nato-space-policy.html accessed on 2 January 2021.
[75] UNGA Resolution 75/36 on 'Reducing space threats through norms, rules and principles of responsible behaviours' (23 October 2020).

and miscalculations with respect to outer space."[76]

Space-based assets enable and support military operations – and other areas of civilian life. For this reason, space assets can become targets for attack or disruption. Thus, the dynamics between States on Earth and in space differs, and a multilateral dialogue could be a way to reduce the vulnerabilities, misunderstandings and tensions that drive the greater involvement of space assets in military operations.

Conclusion: going off the beaten track

Interoperability was thought to minimise the misunderstandings between the NATO allies and to reduce military costs. All the NATO member countries are addressing these issues to some degree, but great disparity remains. Indeed, despite the emergence of new space actors all over the world, the influence balance is in favour of the US and its closest NATO allies.

There is a growing trend among NATO members countries in which the troops will tend to follow their national standards or, conversely, the one standards put in place by the US over the years even without realising it.[77] But nobody knows how to apply or enforce the law to outer space. There is no global understanding of these questions, even in case of incidents caused by counter-space capabilities, dual-use systems, or harmful interference.

The quest for greater consideration of collective priorities requires multiple strategies that not only involve the US, but also its NATO allies, individually.[78] All NATO country members are becoming more dependent on space services. For this reason, the challenges that the NATO allies face, both as space powers or are space beneficiaries, should be considered collectively without excluding any stakeholder.

***

[76] *Ibid.*
[77] Kirby Abbott, *supra* note 16, 110-111.
[78] Alexandra Stickings, *supra* note 4.

Source: https://ac.nato.int/

Nasty, brutish, and short—the Future of Space Operations in the Absence of the Rule of Law: Addressing Congestion, Contestation, and Competitiveness in the New Space Era[1]

by Douglas Ligor, Esq. and
Bruce McClintock[2]

Introduction

In 2013, U.S. Ambassador Jeffery Eberhardt stated that space is increasingly "congested, contested, and competitive ('three C's')."[3] This was a prescient statement. Space, in many substantive ways, continues to be mostly ungoverned. This leaves nations, and their social, economic, and security interests, at significant risk. In this paper, we seek to first highlight factors that underlie the three C's. Second, we describe the inadequacies of the current system of space governance. Third, we offer some potential recommendations to address the governance dilemma by applying social contract theory, which may allow the international community to move with more alacrity toward ensuring a safe, secure, and prosperous space

[1] **DISCLAIMER**: The views expressed in this article are solely those of the authors and may not necessarily represent the views of NATO, Allied Command Operations, or Allied Command Transformation, or of their affiliated organizations.

[2] Douglas Ligor is a senior behavioural/social scientist at the non-partisan, non-profit RAND Corporation. Prior to RAND, Ligor served as a government attorney in various capacities for the U.S. Departments of Commerce, Justice, and Homeland Security. A former U.S. Army officer, Ligor received his J.D. from the University of Connecticut School of Law, and his B.S. in economics from the U.S. Military Academy, West Point. Bruce McClintock is the lead of the RAND Space Enterprise Initiative, a virtual centre that provides a focal point for all RAND space-related research, for the U.S. government and U.S. allies. McClintock joined RAND in 2016 after retiring from the Air Force as a Brigadier General. McClintock received his M.S. in aerospace engineering from the University of Florida and his B.S. in Astronautical Engineering from the U.S. Air Force Academy.

[3] Jeffrey L. Eberhardt, 'Outer Space Increasingly 'Congested, Contested, and Competitive' (*United Nations*, 25 October 2019) https://www.un.org/press/en/2013/gadis3487.doc.htm

environment for all nations.

Because of the three C's, space is in jeopardy of becoming an unusable graveyard. Without quick and meaningful actions, humanity could lose access to critical low earth orbits (LEO) and geostationary orbits (GEO). As a result, the global community at all levels could suffer significant social and economic instability, as well as national and international turmoil and insecurity. To be sure, this is a worst-case scenario. However, notwithstanding the undetermined probability of such a scenario, experts agree that the potential for catastrophic consequences is very real.[4]

Yet rather than take deliberate steps to develop solutions to stem this danger, nations and other powerful stakeholders have either ignored the problem, or debated—rather than implemented—mitigation measures, for decades. Worse still, some nations are affirmatively engaged in detrimental behaviours, such as debris-generating anti-satellite (ASAT) testing (as part of the "contested" aspect of space). These are short-sighted, self-serving, and outrightly dangerous behaviours that could hasten the demise of space as a critical global asset.

Many of these harmful behaviours are deeply rooted in our shared human dispositions toward fear, competitiveness, greed, and the spirited desire to achieve and be recognized—a concept the ancient Greeks referred to as *thumos*.[5] Spacefaring nations and stakeholders succumb to these dispositions as they compete and jockey for superiority over, or at least a secure presence in, the domain of space. This can drive nations and stakeholders into what resembles a state of nature, which the political philosopher Thomas Hobbes described as an environment without civil governance, and where infinitely appetitive and competitive individuals are subject only to their own private, unchecked judgements. This environment is plagued by perpetual distrust and conflict as individuals attempt to acquire [naturally limited] resources and maintain their own security and self-preservation.[6] We argue that Hobbes's

---

[4] See Donald J. Kessler, et. al., 'The Kessler Syndrome: Implications to Future Space Operations,' (2010) AAS 137(8) p 8-11; Paul B. Larsen, 'Solving the Space Debris Crisis' (2018) 83 J.Air L. &Comm p 475, 478-495; and 'The Cost of Space Debris' (European Space Agency, 5 July 2020) https://www.esa.int/Safety_Security/Space_Debris/The_cost_of_space_debris accessed 21 April 2021

[5] Harvey Mansfield, 'How to Understand Politics: What the Humanities Can Say to Science' (*2007 Jefferson Lecture in the Humanities*, 10 May 2007) p 15 https://neh.dspacedirect.org/bitstream/handle/11215/3769/LIB40_008-public.pdf?sequence=1 accessed 21 April 2021

[6] See generally Partel Piirimae, 'The Explanation of Conflict in Hobbes's *Leviathan*' (2006)

hypothetical, pre-political world accurately describes the current state of space with respect to three key elements.[7]

First, as continually more nations and non-government entities compete in space, they tend to do so almost entirely on a self-interested basis.[8] Second, these interests are essentially unchecked by any defined governance or rule of law system capable of arbitrating and resolving conflict, or of ensuring the fair and equitable distribution of resources among the nations of the world. Third, there is no "Leviathan" to which autonomous nations relinquish a certain measure of their sovereign decision-making authority in exchange for the assurance of security for the entire international community.[9]

These three elements are, however, not insurmountable. Social contract theory offers a means to check negative behaviours. Applying the theory will require nations to better manage, constrain, and mediate their rights and liberties in space through multi-national mechanisms, procedures, and processes. Any limitations set on current rights and liberties, however, will be overwhelmingly offset by an increase in other rights and liberties, which will be made secure because of inherent safeguards offered by a more defined rule of law system that resolves conflict and risk.

For instance, members of NATO (both spacefaring and otherwise) might agree to create a social contract vehicle, such as a new treaty or the addition of a protocol to the existing NATO treaty,[10] to develop rules of behaviour in

10(1) TRAMES p 3-20 https://www.kirj.ee/public/trames/trames-2006-1-1.pdf accessed 7 April 2021

[7] Because space does have some level of international governance in the form of a treaty regime, discussed further on in this paper, it is not a true state of nature. There are, however, gaps in the current treaty regime that have allowed elements of the state of nature to emerge since the signing of the five treaties.

[8] We note, however, that there are also entities and coalitions promoting the use of space resources safely. These entities are actively supporting the development and adoption of governance measures, and the tools that would support them. To further international cooperation and scientific advancement in the field of space systems safety, see, for example, 'Welcome to IAASS' (*International Association for the Advancement of Space Safety*, undated) http://iaass.space-safety.org/ accessed 22 April 2021. For the development of safety metrics for launches and objects, see "Project Space Sustainability Ratings", 'MIT Media Lab' (*MIT Media Lab*, undated) https://www.media.mit.edu/ accessed 22 April 2021.

[9] We apply the term "Leviathan" as a general term of governance to mean: any system, of any size, where entities agree to surrender certain decisions to a central authority to better achieve civil order and safety, but maintain their liberty in all other areas where those particular decisions are not relevant or material.

[10] We acknowledge that the development of a new treaty or protocol to the NATO treaty (aka the Washington Treaty of 1949) would be no small endeavor for NATO members. Additionally, notwithstanding the difficulty in developing consensus to particular conditions of

space. To be achievable, the initial goal of these rules could be specific and circumscribed: to limit the production of space debris and incentivize its targeted removal. Members would agree to a series of binding norms, rules, and joint debris removal operations. If successful, the regime could attract additional spacefaring nations and yet-to-be spacefaring nations to the social contract, providing a safer, more secure space environment for the entire international community.

Problems in Space

The current situation in space is complicated by "more spacefaring nations and companies seeking to use space and space resources (competition), more risk of collisions (congestion), and a growing risk of conflict (contestation)."[11] More recently, the number of spacefaring actors (both nations and private companies) has skyrocketed. As of 2020, more than 80 countries have registered satellites into orbit, at least 11 countries have full or partial launch capability, and dozens of companies provide private launch options, operate their own constellations, or provide space-oriented services.[12] Complicating this is the fact that many countries have formed indemnity agreements with commercial space companies to limit their liability in the event of a catastrophic space accident.[13] This situation, and varying licensing requirements in different countries, encourages commercial space companies to forum shop to limit their liability in the event of a catastrophic space

---

such new agreement, it would also need to be consistent with currently binding international law in the same manner as the Outer Space Treaty, Article III (see *infra*, Table 1) and the Washington Treaty, Article 7, see "The North Atlantic Treaty," 4 April 1949, 34 U.N.T.S 243, art. 7. This effort could be done in parallel to existing efforts to enhance space governance through the United Nations Committee on the Peaceful Uses of Outer Space (COPUOS), see generally COPUOS materials at https://www.unoosa.org/oosa/en/ourwork/copuos/index.html accessed 13 September 2021.

[11] Bruce McClintock, et. al., 'Responsible Space Behaviour for the New Space Era: Preserving the Province of Humanity' (*RAND Corporation*, April 2021) p 3 https://www.rand.org/content/dam/rand/pubs/perspectives/PEA800/PEA887-2/RAND_PEA887-2.pdf accessed 5 September 2021

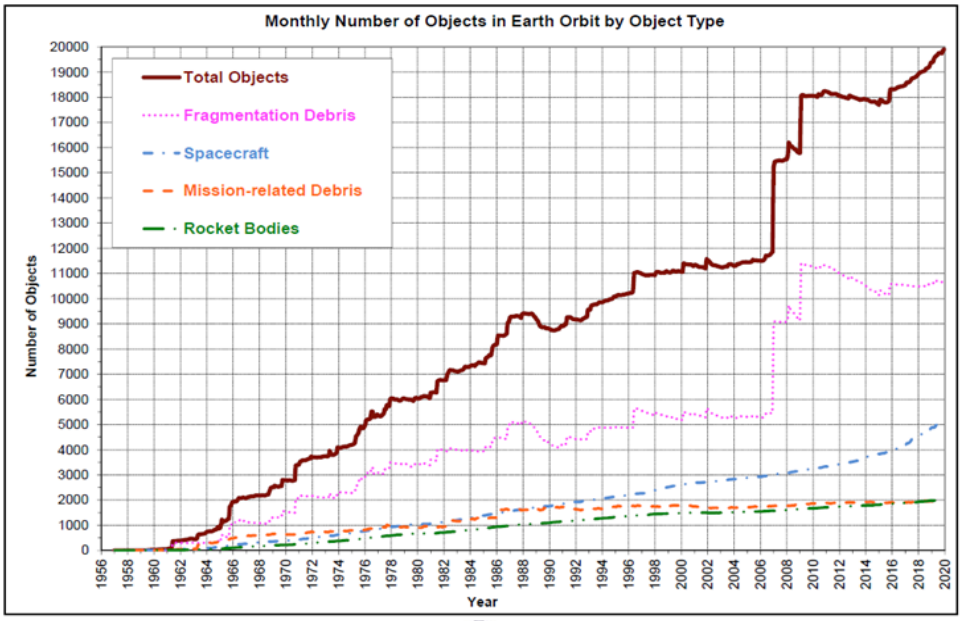
[12] Organisation for Economic Co-operation and Development's Space Forum, 'Measuring the Economic Impact of the Space Sector' (7 October 2020) https://www.oecd.org/sti/inno/space-forum/measuring-economic-impact-space-sector.pdf accessed 21 March 2021

[13] James A. Vedda, '*Study of the Liability Risk-Sharing Regime in the United States for Commercial Space Transportation*' (Aerospace Corporation, 2006)

incident,[14] or to avoid more strict licensing rules in places like the United States.[15]

With this expansion, the number of objects in space has been steadily growing (see Figure 1). This includes not only active satellites but inactive and uncontrolled space debris. As of 2019, there was an estimated more than 170 million pieces of debris in space--most of them untracked because of their small size.[16] According to NASA's Orbital Debris Program Office, "More than 21,000 orbital debris larger than 10 cm are known to exist."[17]

Figure 1. Monthly Number of Objects in Earth Orbit by Object Type



SOURCE: Adapted from NASA, *Orbital Debris Quarterly News*, Vol. 25, No. 1, February 2021.

Space debris forces satellites to manoeuvre to avoid collision, which can

[14] Albert Caley, 'Liability in International Law and the Ramifications on Commercial Space Launches and Space Tourism' (2014) 36(233) Loy. L.A. Int'l & Comp. L. Review p 235 https://digitalcommons.lmu.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1708&context=ilr accessed 21 March 2021. We note that, under the Liability Convention, absolute liability exists for launching nations with respect to a launch that causes damage on Earth or in the atmosphere. However, liability in space depends on a determination of fault, which is a function of determining both a duty of care and negligence. The current treaty regime does not have a defined process for this to occur besides the possibility for the institution of a claims commission under Article XIV of the Liability Convention. Such a commission has never been created.

[15] David Shepardson, 'FCC fines Swarm $900,000 for unauthorized satellite launch' (*Reuters*, 20 December 2018) https://www.reuters.com/article/us-usa-satellite-fine/fcc-fines-swarm-900000-for-unauthorized-satellite-launch-idUSKCN1OJ2WT accessed 13 April 2021

[16] Michael Byers, 'Cold, Dark, and Dangerous: International Cooperation in the Arctic and Space' (2019) 55 Polar Record

[17] As quoted in 'Responsible Space Behavior for the New Space Era: Preserving the Province of Humanity' p 15 (n 10)

increase the probability of collisions between objects. The risk of unintentional space collisions is on the rise.[18] More concerning, in 1978, Donald Kessler conducted research focusing on the potentially dangerous ramifications of the steadily increasing amount of space debris in orbit. Kessler hypothesized that collisions between debris generates new debris at a rate faster than it can decay into Earth's atmosphere. This creates a positive feedback loop where more debris leads to more collisions, resulting in a significantly more risky and dangerous environment for space operations. Today, this scenario is known as the "Kessler Syndrome."[19]

Finally, there is a rapidly growing focus on space as a domain for conflict in a way not seen since the height of the Cold War. The intent to use space for national security is not, in fact, new.[20] The United States and the Soviet Union began developing and testing ASAT weapons in the 1950s and 1960s.[21] In the last decade both China and Russia have accelerated their ASAT activities.[22] The United States has also recently declared space a warfighting domain, created the U.S. Space Force to protect U.S interests in space, and re-established the U.S. Space Combatant Command.[23] France has also formed its own military space command, while other nations such as the United Kingdom and Australia are considering similar steps. NATO, in declaring space an operational domain, has also acknowledged both the importance of space to maintaining international security, and the growing risk of combat in space.[24]

"The various organizational changes are a symptom of the growing dependence on space and the increasing number of space actors that can

---

[18] Kaitlyn Johnson, 'Key Governance Issues in Space' (*CSIS*, September 2020) https://aerospace.csis.org/key-governance-issues-in-space/ accessed 22 April 2021

[19] Donald J. Kessler and Burton G. Cour-Palais, 'Collision Frequency of Artificial Satellites: The Creation of a Debris Belt' (1978) 83(A6) Journal of Geophysical Space Physics Research

[20] Both the United States and the Soviet Union initially prioritized freedom of operations in space to allow for unimpeded overflight of each other's territories for surveillance and reconnaissance. However, both also designed and tested space weapons.

[21] Brian Weeden, 'Through a Glass, Darkly: Chinese, American, and Russian Anti-satellite Testing in Space' (2014) Secure World Foundation Issue Brief p 20-21

[22] Defense Intelligence Agency, 'Challenges to Security in Space' (January 2019) https://apps.dtic.mil/sti/pdfs/AD1082341.pdf accessed 22 April 2021

[23] United States Space Force, 'United States Space Force History' (*United States Space Force*, undated) https://www.spaceforce.mil/About-Us/About-Space-Force/History/ accessed 20 December 2020

[24] Aaron Bateman, 'America Needs a Coalition to Win a Space War' (*War on the Rocks*, 29 April 2020) https://warontherocks.com/2020/04/america-needs-a-coalition-to-win-a-space-war/ accessed 22 April 2021

contest space. The possibility of a terrestrial conflict extending into space or a conflict beginning in space is becoming increasingly real."[25] These three interrelated trends--more spacefaring nations and companies, more risk of collisions, and growing risk of conflict—are exacerbated by the lack of a mature governance system for space.

Space Governance

The concept of the state of nature is not new in international law or relations.[26] Although international legal regimes may constrain the behaviour of individual nations, there is no sole authority and power to enforce compliance, mete out punishment, or strip nations of their jurisdictional powers. Notwithstanding this fact, nations have been able to manage and resolve conflicts over certain terrestrial, global-common, domains (e.g., the high seas, the atmosphere, and the Antarctic) through the negotiation of treaties and other agreements, the use of diplomacy, the imposition of sanctions regimes, and/or the application of theories such as deterrence.[27]

However, the domain of space is unique, making the application of these standard tools less efficacious. In particular, although there is general agreement that outer space is a global-commons similar to the archetypical terrestrial commons,[28] the physical characteristics of space are radically different.[29] In space, geocentric orbits drive conceptions of time, movement, and boundaries that are inapplicable on Earth. A wrench dropped by a sailor

---

[25] As quoted in 'Responsible Space Behavior for the New Space Era: Preserving the Province of Humanity' p 20 (n 10)

[26] Heath Pikering, 'Why Do States Mostly Obey International Law' (*E-International Relations*, 4 February 2014) https://www.e-ir.info/2014/02/04/why-do-states-mostly-obey-international-law/ accessed 7 April 2021

[27] We define "governance" as a system [government] that is able to make and enforce rules; direct, control, or regulate actions or conduct; and deliver services. Adapted from Francis Fukuyama, 'What Is Governance?' (2013) 26 Governance p 350-351; and Henry Campbell Black, et al., 'Black's Law Dictionary: Definitions of the Terms and Phrases of American and English Jurisprudence, Ancient and Modern' (1990) West Publishing Co. p 695.

[28] See Ram Jakhu and Joseph Pelton, eds., 'Global Space Governance: An International Study' (2017) Springer International Publishing; and Cassandra Steer, 'Global Commons, Cosmic Commons: Implications of Military and Security Uses of Outer Space' (2017) 18 Georgetown Journal of International Affairs. See also the United Nations, *UN System Task Team on the Post-2015 UN Development Agenda*, January 2013 https://www.un.org/en/development/desa/policy/untaskteam_undf/thinkpieces/24_thinkpiece_global_governance.pdf accessed 22 April 2021

[29] See generally, Space Capstone Publication, 'Spacepower: Doctrine for Space Forces' (2020) p 3-10 https://www.spaceforce.mil/Portals/1/Space%20Capstone%20Publication_10%20Aug%202020.pdf accessed 22 April 2021

sinks to the seabed and does not threaten maritime navigation. A wrench dropped by an astronaut becomes an uncontrollable 7000 m/s projectile capable of damaging or destroying any satellite(s) in its path.

The current international governance regime for space is treaty-based (see Table 1). These treaties represent the extent to which "hard law"[30] imposes requirements, conditions, responsibilities, and obligations on party nations. However, for the most part, these treaties suffer from three primary weaknesses that make them inadequate as instruments to address the problems described above.

Table 1. Major United Nations Space Treaties[31]

Treaty (short name)	Date	Total Parties	Total Signatories
Outer Space Treaty	1967	110	23
Rescue Agreement	1968	96	23
Liability Convention	1972	95	19
Registration Convention	1975	67	3
Moon Agreement	1979	18	4

SOURCES: United Nations, "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies' 19 December 1966, 610 U.N.T.S. 205; United Nations, 'Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space' 22 April 1968, 672 U.N.T.S. 119; United Nations, 'Convention on International Liability for Damage Caused by Space Objects' 29 March 1972, 961 U.N.T.S. 187; United Nations, 'Convention on Registration of Objects Launched into Outer Space' 14 January 1975, 1023 U.N.T.S. 15; United Nations, 'Agreement Governing the Activities of States on the Moon and Other Celestial Bodies' 19 December 1979, 1363 U.N.T.S. 3; United Nations Office for Outer Space Affairs, 'Status of International Agreements Relating to Activities in Outer Space as at 1 January 2020' 1 January 2020; and Jessica West, 'Not a Frontier: The Outer

[30] We define "hard law" as any instrument that has a binding legal effect (e.g., treaty, protocol, statute, regulation, etc.). A hard law instrument is typically self-executing or requires domestic legislation; creates mechanisms for interpretation, monitoring, enforcement, and dispute resolution; and increases the damage or cost to state or other actor in the form of sanctions or credibility loss for reneging or violating the law's requirements. See Gregory C. Shaffer and Mark A. Pollack, 'Hard vs. Soft Law: Alternatives, Compliments and Antagonists in International Governance' (2010) 94 Minnesota Law Review p 706-799, as referenced in 'Responsible Space Behavior for the New Space Era: Preserving the Province of Humanity' p 11 (n 10)

[31] Re-printed from 'Responsible Space Behavior for the New Space Era: Preserving the Province of Humanity' p 7 *(n 10)*

Space Governance Framework' (*UNIDIR*, 30 January 2019) < https://www.unidir.org/sites/default/files/conferences/pdfs/presentation-jessica-west-eng-0-793.pdf > accessed 22 April 2021

First, they articulate general principles that are broad in scope and ambiguous. While it may be true that these characteristics have benefits, i.e., allowing for nations to negotiate and find agreement, they can also be detrimental to governance. Ambiguity can lead to, *inter alia*, misperceptions (e.g., perceiving a use of force as offensive when it is intended to be anodyne or defensive), miscalculations (e.g., the inability to determine a safe distance during a proximity operation), and the intentional avoidance of responsibility (e.g., the purposeful contamination of an orbit or celestial body due to the adoption of a "contamination" standard that incentivizes pollution).

Second, no treaty contains a verification or enforcement mechanism that allow for the punishment of malicious, nefarious, or negligent actors. For example, Articles VI of the OST provides that member nations "bear…responsibility for [their] national activities," including that of "non-government" entities within their jurisdiction. Article VII provides that launching nations "shall retain jurisdiction and control over" a space object (or parts thereof) on its registry.[32] This includes space objects owned and operated by other entities.[33] However, there is no articulation in the OST as to how to a nation or entity that denies responsibility for an object, or that engages in an activity that is dangerous or objectionable, would be held accountable.[34]

Third, the treaties (including the 1972 Liability Convention) do not define

[32] See United Nations, "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies' 19 December 1966, 610 U.N.T.S. 205, Articles VI and VII

[33] Phillippe Achilleas and Stephen Hobe, eds., *Fifty Years of Space Law* (The Hague Academy of International Law 2020) p 233-236

[34] In contrast to the lack of defined and operable enforcement and dispute resolution articulations in the OST and the 1972 Liability Convention, see the United Nations Convention on the Law of the Sea (adopted 10 December 1982, entered into form 16 November 1994) 1833 UNTS 3 arts 100-107 (criminalizing piracy), as analyzed by Tamsin Phillipa Paige, 'The Impact and Effectiveness of UNLCOS on Counter-piracy Operations,' (2016) Journal of Conflict & Security Law, p 100-109 ; see also analysis of third-party conflict settlements by Stephen C. Nemeth, Sara McLaughlin Mitchell, Elizabeth A. Nyman, and Paul R. Hansel, 'Ruling the Sea: Managing Maritime Conflicts through UNCLOS and Exclusive Economic Zones,' (2014) International Interactions, 40:5, p 711-736. Although the maritime domain presents significant and substantive differences in terms of enforcement and dispute resolution, UNCLOS does offer nations an example of how these two concepts can be developed from general principle-based language to specific codes of conduct administered by institutionalized mechanisms and processes.

key terms such as "outer space", "space object", or "contamination" such that legal concepts like duty, negligence, and *mens rea* (i.e., intent) can appropriately be applied to aberrant conduct.[35] This impedes the codification of rules that would mitigate against debris creation, allow for an adjudication of fault (e.g., for a collision or inappropriate use of force), or avoid dangerous proximity operations. As a result, nations and their commercial entities are free to determine, for example, whether they should manoeuvre to avoid a collision with another object, or to accept responsibility if a collision occurs.

Nations may apply the current rules as they see fit, or may even apply the rules arbitrarily if pursuing interests in an ad hoc manner stemming from a lack of a defined body of domestic space law and regulation. This can make conflict resolution difficult if not impossible, as was recently the case when Russian satellites came within 100 miles of a U.S. satellite, a manoeuvre that U.S. officials stated, "has the potential to create a dangerous situation in space."[36] Without any established proximity rules, the Russian government can justifiably claim the activity as an "experiment" that was not in violation of any treaties or standards of conduct.[37]

As a legal matter, these weaknesses in the treaties are structural impediments to efforts not only to update the current space governance regime, but also to develop simple norms, rules, codes of conduct, and other soft law instruments.[38] This is not to say that the U.N. and certain member

---

[35] Because concepts of duty, negligence, and intent are normally defined within nation's domestic legal regime, and because these definitions may vary, it may be necessary to develop a common set of definitions and standards for these concepts. Existing mechanisms may offer a basis for this development, see for example, International Law Commission, "Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries" November 2001, Supplement No. 10 (A/56/10), article 39, p 109 to 110 (discussing "injury by willful or negligent action or omission" by a State).

[36] W.J. Hennigan, 'Exclusive: Strange Russian Spacecraft Shadowing U.S. Spy Satellite, General Says' (Time, 10 February 2020) https://time.com/5779315/russian-spacecraft-spy-satellite-space-force/ accessed 22 April 2021

[37] Similarly, the U.S. has conducted its own proximity operations, opening itself up to equal criticism on this point from the Russians and other nations. See Kaila Pfrang and Brian Weeden, 'U.S. Military and Intelligence Rendezvous and Proximity Operations in Space' (2020) Secure World Foundation

[38] We define "soft law" as instruments that are nonbinding that facilitate state cooperation without the threat of enforcement. They typically "are easier and less costly to negotiate"; impose lesser "sovereignty costs"; are flexible and adaptable (to cope with uncertainty); and are "available to non-state actors." See Gregory C. Shaffer and Mark A. Pollack, 'Hard vs. Soft Law: Alternatives, Compliments and Antagonists in International Governance' (2010) 94 Minnesota Law Review p 719, as referenced in 'Responsible Space Behavior for the New Space Era: Preserving the Province of Humanity' p 11 (n 10)

nations are not seeking to develop soft law. Initiatives on Transparency and Confidence-building Measures (TCBMs) and the creation of Long-term Sustainability (LTS) guidelines are evidence of these efforts.[39] However, nations have not agreed to adopt these voluntary measures. Or, if adopted, they have not agreed how issues of detection, attribution, and enforcement should be resolved.

The failure of soft law to advance to adoption is concerning. In the absence of new or amended treaties, soft law instruments are a potential means to maintain a safe and secure space environment while nations work more deliberately to develop customary or hard law instruments.[40] Additionally, an argument may be made that powerful governments (and powerful non-government entities) have become diplomatically, strategically, commercially, and operationally addicted to the weaknesses inherent in the current five-treaty regime.[41] A prime example of this is the persistent launch of thousands of space objects[42] into increasingly cluttered and dangerous LEO and GEO orbits despite the rising prevalence and risk associated with collisions and the required manoeuvres to avoid them.

The accelerating growth in satellite launches has not been offset by a

---

[39] See 2018 United Nations Disarmament Commission, 'Non Paper by the Secretariat' https://www.un.org/disarmament/wp-content/uploads/2018/03/WG2-secretariat-non-paper-outer-space-TCBMs-FINAL.pdf accessed 22 April 2021

[40] See Jack M. Bear, 'Soft Law's Failure on the Horizon: The International Code of Conduct for Outer Space Activities' (2017) 38 University of Pennsylvania Journal of International Law p 345-353 https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1936&context=jil accessed 22 April 2021

[41] Jon E. Grant, et. al., 'Introduction to Behavioral Addictions' (2010) 36 American Journal of Drug and Alcohol Abuse p 9, 233-241 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3164585/ accessed 22 April 2021. Of course, we do not mean to apply the term "addicted" in the clinical sense. Instead, we apply the term generally to describe "persistent behavior despite the knowledge of adverse consequences." Although some may object to this characterization, we believe this definition is accurate nonetheless with respect to the underlying behaviours of spacefaring entities as they relate to the problems identified in this paper.

[42] As of March April 7, 2021, SpaceX alone has launched 1443 Starlink satellites since May of 2019. See Adam Mann, 'Starlink: SpaceX's satellite internet project' (*Space.com*, 17 January 2020) https://www.space.com/spacex-starlink-satellites.html accessed 22 April 2021; and see Darrell Etherington, 'SpaceX launches 60 more Starlink satellites, now at 300 launcher in just over one month' (*TechCrunch.com*, 7 April 2021) https://guce.advertising.com/collectIdentifiers?sessionId=3_cc-session_dc25e1e5-e64e-4d9d-8e38-50c89e80631f accessed 22 April 2021. Additionally, China is taking steps to launch a 13,000 satellite mega-constellation, with launches to start in 2022. See Andrew Jones, 'China is developing plans for a 13,000-satellite mega constellation' (*SpaceNews*, 21 April 2021) https://spacenews.com/china-is-developing-plans-for-a-13000-satellite-communications-megaconstellation/ accessed 22 April 2021

more holistic approach to managing their impact on the environment. Additionally, nations have made no substantive effort to allow for the lawful removal of unidentifiable debris. Although there have been efforts by the U.S. and others to develop debris mitigation guidelines,[43] they also remain voluntary and without enforcement mechanisms.[44] Nations have also been slow to develop the capability to actively remove debris,[45] and cannot agree on mitigation guidelines that provide for the end of life of space objects such that debris is not continually created.[46] Perhaps most startlingly, nations cannot agree on binding or voluntary measures that would check, or even limit, the impulse to engage in debris creating ASAT testing.

An addiction to a weak or laissez-faire governance regime can lead to unpredictable acts, conflict, and a destabilization of the civil order over which that regime applies. Both China and Russia exemplify this type of behaviour in terms of their recent ASAT activities.[47] In these instances, a weak space regime invites these addictive-like negative behaviours that exacerbate an already unstable space environment.

---

[43] See National Aeronautics and Space Administration, 'U.S. Government Orbital Debris Mitigation Standard Practices' (2019) https://orbitaldebris.jsc.nasa.gov/library/usg_orbital_debris_mitigation_standard_practices_november_2019.pdf accessed 22 April 2021

[44] See Brian Weeden, 'The United States is losing its leadership role in the fight against orbital debris' (*The Space Review*, 24 February 2020) https://www.thespacereview.com/article/3889/1 accessed 22 April 2021

[45] See Mandy Mayfield, 'Industry Offering On-Orbit Satellite Servicing' (2021) National Defense https://www.nationaldefensemagazine.org/articles/2021/1/29/industry-offering-on-orbit-satellite-servicing accessed 22 April 2021

[46] This is not to say that nations and commercial entities are not developing technologies that could mitigate debris in the future if mitigation rules could be agreed upon. For servicing technologies that could extend the life of satellites and, therefore, prevent an increase in derelict objects, See 'Northrop Grumman and Intelsat Make History with Docking of Second Mission Extension Vehicle to Extend Life of Satellite' (*Northrup Grumman*, 12 April 2021) https://news.northropgrumman.com/news/releases/northrop-grumman-and-intelsat-make-history-with-docking-of-second-mission-extension-vehicle-to-extend-life-of-satellite accessed 22 April 2021

[47] See generally, Brian Weeden, '2007 Chinese Anti-Satellite Test Fact Sheet' (2010) Secure World Foundation https://swfound.org/media/9550/chinese_asat_fact_sheet_updated_2012.pdf accessed 22 April 2021; and Hanneke Weitering, 'Russia has launched an anti-satellite missile test, US Space Command says' (*Space.com*, 16 December 2020) https://www.space.com/russia-launches-anti-satellite-missile-test-2020 accessed 22 April 2021. We would also note, however, that the U.S. has resisted any efforts to create any hard law mechanisms to restrict or inhibit ASAT testing, which can invite indifference by other nations.

Solutions

Long term security cannot be guaranteed in an environment subject to the state of nature. Even powerful entities are not safe because, "even the weakest has the strength to kill the strongest, either by secret machination, or confederacy with others…"[48] As applied to space, even unsophisticated actors may be able to destroy critical national or commercial space assets.[49] Or, a dangerous debris field may do the same if an asset fails to manoeuvre or does not detect an object in its path.[50] To avoid this, some type of internationally recognized rule of law system should be developed. This need not be a panoptic, Hobbesian "Leviathan"—a more limited, internationally palatable, and bridled Leviathan may suffice.

Organizations like NATO are exemplars of the successful application of social contract theory. They bring together like-minded entities for the purposes of alleviating the state of nature in favour of collective and deliberative decision-making regimes. Entities agree to be bound by decisions of the regime, which in turn, increases trust, predictability, and security for all members—the opposite of a state of nature in which life may be "nasty, brutish, and short."[51] Such exemplars can be developed and/or built upon to be the focal points for establishing a more effectual rule of law in space.

NATO members are in a prime position to develop a robust rule of law system for space. NATO spacefaring members currently account for approximately 50% of all active satellites.[52] The formation of such a group into a treaty-like agreement, perhaps by first agreeing to bind themselves to existing soft law instruments like the TCBMs and/or LTS, could become a centre of gravity for the maturation of norms, rules, and standards of space behaviour. Eventually, even adversaries or less constrained actors may feel compelled to abide the rules for fear of being shut out of the benefits of such a system, e.g., information and data sharing, enhanced collision avoidance networks, debris

---

[48] Thomas Hobbes, Leviathan (first published 1651, Penguin 1985) Ch XIII

[49] See generally, Rachel A. Gabriel, et. al., 'Malicious Non-state Actors and Contested Space Operations' (2018) https://nsiteam.com/social/wp-content/uploads/2018/07/START_Malicious-Non-state-Actors-and-Contested-Space-Operations-Final.pdf accessed 22 April 2021

[50] See *supra* note 44. The threat of an unknown or undetected debris object is akin to Hobbes's formulation that even the mightiest have to lock their doors to avoid being killed in their sleep.

[51] Thomas Hobbes, Leviathan (first published 1651, Penguin 1985) Ch XIII

[52] Dr Kestutis Paulauskas, 'Space: NATO's latest frontier' (*NATO Review*, 13 March 2020) https://www.nato.int/docu/review/articles/2020/03/13/space-natos-latest-frontier/index.html accessed 22 April 2021

removal efforts, etc.

Additionally, the formation of such a compact could hasten other significant benefits that may be achievable in the short term, such as:

- Member nations and commercial entities could increase communication and engagement. They could develop a global information campaign that would build awareness and facilitate the alignment of nations toward goals that bring the benefits of space to all. The U.N. Committee on the Peaceful Uses of Outer Space (COPUOS) already has some initiatives in this area.[53] Additionally, and owing to a wider international audience, the UN General Assembly adopted a UK proposal in December 2020 to facilitate the adoption of norms of behaviour.[54] As many members as possible should join or support these efforts at the upcoming UN General Assembly's 76th Session in late 2021.

- Members could initiate efforts to cooperate on increased transparency regarding on-orbit operations. Just as the world experienced an evolution in maritime domain awareness, members could develop space situational awareness (SSA) that is widely available and better integrated. Most space operators already pool their satellite data, which allows them to more effectively manage and mitigate the risk of collision.[55] Members should support more detailed technical analysis to better develop SSA.

- Finally, members could work to disentangle safety issues from security issues and focus on near-term gains. This is a difficult step, but it has been done in other domains.[56] It will likely require "further research to study the

[53] United Nations General Assembly, 'Report of the Committee on the Peaceful Uses of Outer Space' 12–21 June 2019, A/74/20 p 4; and UNOOSA, 'The Promoting Space Sustainability Project' (*United Nations Office for Outer Space*, January 2021) https://www.unoosa.org/oosa/en/ourwork/topics/promoting-space-sustainability.html accessed 22 April 2021

[54] United Nations, 'Reducing Space Threats Through Norms, Rules and Principles of Responsible Behaviours' 23 October 2020, A/C.1/75/L.45/Rev.1 p 3. On December 7, 2020, the UN General Assembly voted on the proposal, and it passed with 164 in favour, 12 against, and six abstentions. Noteworthy votes against included China, Iran, North Korea, Russia, and Venezuela. Notable abstentions included India and Israel.

[55] Daniel L. Oltrogge and Salvatore Alfano, 'The Technical Challenges of Better Space Situational Awareness and Space Traffic Management' (2019) 6 Journal of Space Safety Engineering

[56] For one perspective on the problems separating safety form security, see Christopher Ford, 'Arms Control in Outer Space: History and Prospects' (2020) 1 Arms Control and International Security Papers https://2017-2021.state.gov/wp-content/uploads/2020/07/T-Paper-Series-

evolution and structure of governance frameworks for other domains and to consider best practices and approaches for the space domain."[57] Although there are distinct and fundamental differences between space and domains (e.g., airspace, maritime, etc.), it would be informative to conduct and in-depth assessment as to how other domains "have encouraged more-efficient use and stewardship of common-pool resources."[58]

Conclusion

Developing a rule of law for space is challenging given the sheer number of actors, each with different interests. Hobbes would recognize this dilemma and likely offer social contract theory as a solution. Resolving issues related to the congested, contested, and competitive space environment requires entities to align together and agree on rules to preserve each entities' security and ability to thrive. While humanity's future is inextricably linked to space, it is increasingly uncertain, particularly given the recent activities, posturing, and rhetoric of many spacefaring nations, whether there is sufficient political will to set aside short-term self-interests and focus on the collective international solutions offered above to help ensure long-term space sustainability.[59]

***

Space-Norms-Formatted-T-w-Raymond-quote-2543.pdf accessed 22 April 2021

[57] As quoted in 'Responsible Space Behavior for the New Space Era: Preserving the Province of Humanity' p 33 (n 10). Other domains to research would be, for example, airspace (and the development of the Chicago Convention and resulting International Civil Aviation Organization (ICAO)), maritime (and the development of the Law of the Sea Convention and resulting International Maritime Organization (IMO)), and telecommunications (and the development of the International Telecommunications Union (ITU)).

[58] As quoted in 'Responsible Space Behavior for the New Space Era: Preserving the Province of Humanity' p 33 (n 10).

[59] See 'Responsible Space Behavior for the New Space Era: Preserving the Province of Humanity' p 33 (n 10).

Source: www.ncia.nato.int

Orbiting Legal Analysis: Armed Attacks in Space[1]

by Maj Lindsay L. Rodman, USMCR

So far, outer space remains a zone of peace. In space, astronauts from a diverse range of states collaborate and states themselves cooperate despite volatile politics on earth. While a combination of luck and under-developed technology have prevented armed attacks in space thus far, one cannot presume that such attacks are impossible, especially in the medium-to-long term. As technology improves and the global geopolitical environment changes over time, our luck will be tested.

NATO is already preparing for this eventuality. In late 2019, NATO officially named space as an operational domain.[2] NATO's Allied Joint Doctrine for Air and Space Operations (AJP 3.3(A)) states: "Commanders must anticipate

[1] **DISCLAIMER**: The views expressed in this article are solely those of the author and may not necessarily represent the views of NATO, Allied Command Operations, or Allied Command Transformation, or of their affiliated organizations.

[2] Martin Banks, 'NATO names space as an "operational domain," but without plans to weaponise it,' *DefenseNews* (Washington, DC 20 November 2019).

hostile actions that attempt to deny friendly forces access to or use of space capabilities."[3]

In anticipation of such hostile actions, this article addresses the *jus ad bellum* question of what constitutes an armed attack in space. There is no precedent or history of state practice to inform this question.[4] Therefore, the question must be addressed through evaluating existing law with only hypothetical fact patterns and analogies to other domains to inform the analysis. This article concludes that jus ad bellum analysis as it is evolving today, especially in the other new domain – cyberspace – suggests that states will engage in circular logic (or, in this case, orbital logic) to derive a *jus ad bellum* justification after they deem a self-defence response is warranted.[5] This article notes the importance of distinguishing between *ex ante* (intent or instrument-based) versus *ex post* (consequence-based) legal analysis and between treaty law-based versus customary international law-based analysis in determinations of whether an armed attack has occurred to avoid excessive weakening of the law. In the space domain, the Liability Convention and the Outer Space Treaty will further complicate the legal analysis by imputing absolute liability to states for the actions of non-state actors. In the absence of further treaty law, there is a danger of quick escalation in outer space of which NATO member states in particular should be mindful.

This article is drafted with the practitioner in mind and will proceed as

---

[3] North Atlantic Treaty Organisation (NATO), *Allied Joint Doctrine for Air and Space Operations* (AJP 3.3(A)), November 2009, paragraph 0603. Paragraph 0617 of AJP 3.3(A) notes the importance of thinking through legal considerations as applied to space: "**Legal Considerations**. Numerous national and international laws and treaties exist that must be considered in the planning stages of any mission anticipating space support, and Legal Advisers must be immediately available during all stages of planning and execution of space operations in order to ensure compliance. Although some acts are prohibited. Many of the restrictions may be applicable during space negation operations. International laws, including contracts and consortium agreements, prohibit certain space assets from being used for military purposes. For example, certain corporation agreements prohibit using satellite communications for military operations. International law, as it pertains to the use of force, regulation of the means and methods of warfighting, and protection of non-combatants, must be considered when conducting space control, space force enhancement and space support operations."

[4] Dale Stephens, 'The International Legal Implications of Military Space Operations: Examining the Interplay between International Humanitarian Law and the Outer Space Legal Regime' (2018) 94 Int'l L. Stud. 75, 88.

[5] Other possible justifications for the use of force in response to an action would be a United Nations Security Council Resolution or host nation consent. This article will focus on the narrow question of "armed attacks" and the resultant justification for a self-defence response.

follows. In Section I, the article will summarize the relevant approaches legal practitioners take to what constitutes an armed attack outside of the space domain. Section II applies the analysis to space operations, attempting to address the predictable ways in which an armed attack might manifest. The analysis in Section I and Section II presumes state-on-state actions. Section III highlights the ways in which the international liability regime in space might complicate jus ad bellum analysis with respect to non-state actors. Section IV is the conclusion.

I. What constitutes an armed attack?

Article 2, paragraph 4 of the UN Charter prohibits 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."[6] The term "force" in Article 2(4) denotes violence.[7] Article 51 of the UN Charter provides: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations."[8]

The incongruity between the language in Article 2(4) ("threat or use of force") and in Article 51 ("armed attack") presents the question of which uses of force would justify a self-defence response. According to the U.S. Department of Defense (DOD) Law of War Manual, "[t]he United States has long taken the position that the inherent right of self-defence potentially applies against any illegal use of force."[9] The International Court of Justice, however, makes a distinction: "As regards certain particular aspects of the principle in question, it will be necessary to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms."[10] A deeper contextual reading of the drafting of the UN Charter suggests that the term "armed attack" in Article 51 was intended to signal a

---

[6] Charter of the United Nations (24 October 1945) 1 UNTS 16 (UN Charter), Article 2(4).
[7] Michael N. Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 Colum. J. Transnat'l L. 885, 904-05 (noting that Article 2(4) was intended to achieve its preambular goal of preventing use of "armed force").
[8] U.N. Charter, Article 51.
[9] Office of the General Counsel Department of Defense, *U.S. Department of Defense Law of War Manual* (December 2016) [hereinafter "DOD Law of War Manual"], ¶ 1.11.5.2. The DOD Law of War Manual is cited in this article not as a source of law, but as evidence of the American approach to the applied legal analysis.
[10] *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States)* [1986] Merits, Judgment, ICJ 14, 101 (¶191).

higher standard; whereas the term "force" was chosen instead of "armed force" to lower the standard on which actions might be considered violative of Article 2.[11]

The prohibition on the use of force against another state is *jus cogens* in international law.[12] The term "use of force" in the land and sea domains has historically been fairly straightforward, with the term "use of force" being primarily associated with kinetic uses of force.

Scholars of jus ad bellum have debated the precise scope of the term "force" since the Charter's enactment in 1945. Nonetheless, the predominant position among scholars is that the term "force" should be narrowly construed to mean "armed force," and that Article 2(4)'s prohibition therefore does not preclude a state from imposing economic pressure on another state.[13]

Article 49 of the Additional Protocol I to the Geneva Conventions further defines "attacks" as "acts of violence against the adversary, whether in offence or in defence."[14] "Violence has, for these purposes, been interpreted as involving violent consequences, namely injury or damage."[15] This provision of Additional Protocol I is accepted as customary international law, including by the United States.[16]

The advents of electronic warfare and then cyber warfare have required legal practitioners to address non-kinetic actions that have the potential to result in significant harms, including harms that produce injury or damage and harms that affect "the territorial integrity or political independence of any state or in any other manner inconsistent" with the UN Charter. In the absence of additional applicable treaty law, customary international law is developing related to these questions. In practice, the analysis typically devolves into a consequence-based analysis. For example, Michael Schmitt asserts that

---

[11] Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' 904-05 (noting that the negotiations contemplated economic and other forms of coercion, but opted instead for the term "force," which was meant to connote armed force) (n 6).
[12] Vienna Convention on the Law of Treaties (23 May 1969) 1155 UNTS 331, Article 53.
[13] Manny Halberstam, 'Hacking Back: Reevaluating the Legality of Retaliatory Cyberattacks' (2013) 46 Geo. Wash. Int'l L. Rev. 199, 210.
[14] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (8 June 1977) 1125 UNTS 3 (Additional Protocol I), Article 49.
[15] Bill Boothby, 'Space Weapons and the Law' (2017) 93 Int'l L. Stud. 179, 210 n. 112.
[16] Theodore Richard, *Unofficial United States guide to the First Additional Protocol to the Geneva Conventions of 12 August 1949* (Air University Press 2019), p. 84.

"attacks" can include "non-kinetic operations that cause damage or destruction to civilian objects or injury to, or death of, civilians. Operations directed against civilians or civilian objects which result in consequences short of this standard, such as inconvenience or non-injurious hardship, would not constitute an attack."[17] This *ex post* analysis would analogize to or distinguish from kinetic land-based uses of force and their consequences, using the degree of injury to persons or damage to property as a way to determine whether an action is akin to kinetic uses of force.

Consequence-based analysis is somewhat inconsistent with the UN Charter approach as described above,[18] which relies upon the nature of the action as an "armed attack" or "use of force," and is not defined in terms of results. Taking the ICJ approach – that "armed attack" and "use of force" mean different things – the term "armed attack" ascribes a sense of intention and military association; one does not typically attack by mistake or through civilian government bodies. Even if one agrees with the American approach that "armed attack" and "use of force" are synonymous, "the concept of the use of force is generally understood to mean armed force."[19] Therefore actions that are not "violent" in the sense of Additional Protocol I or that do not appear to be "armed force" are not obviously included in the treaty law approaches to jus ad bellum.

The UN Charter regime instead suggests an instrument-based or intention-based approach, i.e. an analysis of the action *ex ante*, not *ex post*. Uses of armed force have the greater potential for harm and escalation, regardless of consequence. However as new means of warfare and of coercion have resulted from new technologies, some might argue that the term "use of force" has become more ambiguous. These assertions push the treaty law into new territory that belies the textual foundation.

The cyberspace domain is the next-newest warfighting domain and many actions with effects in space might also be categorized as cyber-attacks. In 2019, NATO Secretary General Jens Stoltenberg stated that a cyber-attack

---

[17] Michael Schmitt, 'International Law and Military Operations in Space' (2006) 10 Max Planck UNYB 89, 117; *see also* M. Schmitt, 'Wired Warfare: Computer Network Attack and International Law' (2002) 94 Int'l Rev. of the Red Cross 365, 375-378.

[18] For a fuller analysis of UN Charter drafting and support for this statement, see Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 909-910 (n 6).

[19] Ibid at 908. *Cf.* Hans Kelsen, 'Collective Security Under International Law' (1954) 49 Naval War College International Law Studies 57 n.5.

could trigger an Article 5 collective self-defence reaction, implicitly suggesting that a finding that an armed attack under the UN Charter would have taken place.[20] The best example of a cyber-attack that manifested in "use of armed force"-like consequences was the Stuxnet attack. In that case, a cyber-attack resulted in significant harm to military and government property in Iran associated with the nuclear program.[21] The lack of a self-defence response from Iran does not mean that the cyber-attack could not have justified such a response, but the matter was never addressed as such. Preceding cyber warfare was electronic warfare (EW), but EW has not produced many relevant fact patterns because it is mostly regarded as a defensive measure.[22] There is no significant state practice, customary international law, or even academic analysis suggesting whether EW could (or could not) be a use of force rising to the level of an "armed attack."

Certain obvious analogies to traditional kinetic warfare, such as a cyber-attack that produces significant loss of life, are presumed to be treatable as uses of force amounting to an "armed attack" under customary international law.[23] However, those cases are a rarity. There are many examples of cyber-attacks that do not result in harms directly comparable to uses of armed force. One such example would be the coordinated cyber-attacks on Estonia in 2007. Despite suspicions that such attacks were coordinated by Russia, they did not result in loss of life or significant damage to property, as a kinetic assault would have. Despite a reasonable argument that the attacks undermined the political independence and sovereignty in Estonia, cooler heads prevailed and Estonia "retaliated" instead by sponsoring the drafting of the Tallinn Manual.[24]

The problem with the consequence-based approach is its susceptibility to the slippery-slope. If the UN Charter regime was intended to justify self-defence responses only in narrow circumstances, opening the door to justification through analogy would not meet that intent. Legal practitioners

---

[20] Jens Stoltenberg, 'NATO will defend itself' (*NATO Newsroom*, August 27, 2019) https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en accessed 22 April 2021 (originally published in Prospect's new cyber resilience supplement).

[21] Kim Zetter, 'An Unprecedented Look at Stuxnet, the World's First Digital Weapon' *Wired* (New York, 3 November 2014) https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ accessed 22 April 2021.

[22] *Cf*. Gerard O'Dwyer, 'Finland, Norway press Russia on suspected GPS jamming during NATO drill' *DefenseNews* (Washington DC, 16 November 2018).

[23] *See* Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework,' 913 (n 6).

[24] Michael Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013).

who wanted to "get to yes"[25] for their political or military leaders might have been able to stretch the law in the Iran or Estonia examples cited above, but a self-defence response could have produced dangerous escalation. The downside of not allowing for analogy, however, is the impracticality of insisting that treaty law excludes application to new technologies. While a narrow interpretation is prudent, to determine whether a consequence-based approach would justify a self-defence response, one must revisit the question of whether the term "armed attack" is different than the term "use of force."

The American approach (equating "use of force" and "armed attack") and the ICJ approach (using a higher standard for "armed attack") lead to substantially different outcomes, including potentially in the space domain. The American approach lends itself inherently to tautological analysis in practice. Because the United States finds equivalence in the terms "armed attack" and "use of force," the analysis instead focuses on whether self-defence would be justified in a given scenario as a proportional response to the use of force, rather than whether a use of force is sufficient to constitute an armed attack. The ICJ approach requires a different analysis: one must consider whether a use of force constitutes an armed attack, and only an armed attack would potentially justify self-defence.

The principle of non-intervention is also relevant to this inquiry, especially for the American approach. The ICJ noted in the Nicaragua case: "[t]he principle of non-intervention right of every sovereign State to conduct its affairs without outside interference… is part and parcel of customary international law."[26] The principle of non-intervention makes uses of force against another state illegal according to customary international law as well as the UN Charter. Because the American approach equates uses of force with armed attacks,

---

[25] Legal practitioners are often taught that they should try to enable the intent of the commander or political leadership. Lawyers who "get to yes" are lauded for doing the right thing. This often requires pushing the law to its boundaries. This article suggests that such a culture of "getting to yes" will have the long term effect of pushing more actions into the "armed attack" category. *See, e.g.,* Matt Montazzoli, 'Lessons for Legal Advisors from the Brereton Report' (*Articles of War (Lieber Institute)*, 19 January 2021) https://lieber.westpoint.edu/lessons-legal-advisors-brereton-report/ accessed 22 April 2021.

[26] Nicaragua v. United States ¶202 (n 9); *see also* Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty, G.A. Res. 2131, U.N. GAOR, 20th Sess., Supp. No. 14, at 12, U.N. Doc. A/6220 (1965); Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the United Nations, G.A. Res. 2625 (XXV), U.N. GAOR, 25th Sess., Supp. No. 28, at 121, U.N. Doc. A/8082 (1970).

any such use of force could therefore justify a self-defence response. Nevertheless, there are cases where an action by one state against another might be wrongful or even illegal but would not constitute a use of force or an armed attack, even under the US approach.

The US position on self-defence is meant to hedge against escalation. By responding early and proportionately at lower-levels of force, the United States seeks to avoid escalation into large armed attacks that lead into fully realized wars.[27] The US position enables tit-for-tat responses in the cyberspace domain[28] as well as so-called "retaliatory" strikes.[29] Public justifications for tit-for-tat responses and "retaliatory" strikes typically do not engage in *ex ante* analysis of whether the initial use of force constituted an armed attack or justified self-defence. In the American approach, the political question of whether a self-defence response is favoured drives the analysis regarding the initial action from the opposing state. Other states are beginning to employ this circular (or, in the case of outer space, orbit-shaped) analysis as well.[30]

II. What is an armed attack in space?

Article II of the Outer Space Treaty provides: "outer space, including the Moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means." Most states agree on the definition of outer space. Outer space and airspace do not overlap; outer space is everything above airspace. "This question is crucial, for airspace is sovereign territory of the sub adjacent state."[31] According to the United Kingdom Ministry of Defence, for example: "For practical purposes, it can be said that the upper limit to a state's rights in airspace is above the highest altitude at which an aircraft can fly and below the lowest possible perigee of an earth satellite in orbit."[32]

Space is the newest warfighting domain, but other new domains have

---

[27] *See* Ryan Goodman, 'Cyber Operations and the U.S. Definition of "Armed Attack"' (*Just Security*, 18 March 2018 https://www.justsecurity.org/53495/cyber-operations-u-s-definition-armed-attack/ accessed 22 April 2021.
[28] *See* ibid.
[29] *See, e.g.*, Eric Schmitt & Thomas Gibbons-Neff, 'U.S. Carries Out Retaliatory Strikes on Iranian-Backed Militia in Iraq' *New York Times* (New York, 12 March 2020) https://www.nytimes.com/2020/03/12/world/middleeast/military-iran-iraq.html accessed 22 April 2021.
[30] Goodman, 'Cyber Operations and the U.S. Definition of "Armed Attack"' (n 29).
[31] Schmitt, *International Law and Military Operations in Space*, 99 (n 16).
[32] UK Ministry of Defence, *The Manual of the Law of Armed Conflict* (2004) ¶ 12.13.

come before it. The Hague Conventions initially addressed only "War on Land" and "Naval War."[33] As the use of force moved into the air domain and then the cyberspace domain, legal experts joined together to draft manuals to address applicability of the law of armed conflict to new domains in the absence of robust state practice.[34] A similar effort to draft a manual relevant to military operations in space is taking shape in Woomera, South Australia.[35] Until such a manual exists, this article seeks to illuminate the analysis related to the jus ad bellum question of armed attacks in space.

Before addressing the analysis, however, it is important to address the applicability of the law of armed conflict to outer space and distinguish legal analysis related to choice of law between the outer space treaty regime and the law of armed conflict.[36] This article aims to inform the legal practitioner who faces a novel fact pattern in outer space and seeks to determine whether it constitutes an armed attack. Whether such an attack is wrongful because it also violates the Outer Space Treaty, other treaties, other customary international law or certain norms, is not particularly relevant to this specific inquiry.[37] Those determinations may be relevant to the analysis regarding appropriate response more broadly; for example, claims,[38] sanctions or international diplomatic condemnation might be appropriate responses under certain circumstances. Those determinations may also be relevant to legal

---

[33] *See* Convention No. V Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, Oct. 18, 1907, 36 Stat. 2310, T.S. No. 540 (Hague Convention V); Convention No. XIII Concerning the Rights and Duties of Neutral Powers in Naval War, Oct. 18, 1907, 36 Stat. 2415, T.S. No. 545; 36 Stat. 2415 (Hague Convention XIII); *see also* Frans von der Dunk, 'Armed Conflicts in Outer Space: Which Law Applies' (2021) 97 Int'l L. Stud. 188, 206.

[34] *See* Program on Humanitarian Policy and Conflict Research at Harvard University, *Manual on International Law Applicable to Air and Missile Warfare* (2009); Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (n 24).

[35] The Woomera Manual on the International Law of Military Space Operations https://law.adelaide.edu.au/woomera/system/files/docs/Woomera%20Manual.pdf accessed 16 April 2021.

[36] *See, e.g.*, Frans von der Dunk, 'Armed Conflicts in Outer Space: Which Law Applies' (n 35); Ryan Esparza, 'Event Horizon: Examining Military and Weaponisation Issues in Space by Utilizing the Outer Space Treaty and the Law of Armed Conflict' (2018) 83 J. Air L. & Com. 333; Caitlyn Georgeson & Matthew Stubbs, 'Targeting in Outer Space: An Exploration of Regime Interactions in the Final Frontier' (2020) 85 J. Air L. & Com. 609.

[37] See note 22 and accompanying text. *See also* John Yoo, 'Rules for the Heavens: The Coming Revolution in Space and the Laws of War' (2020) 2020 U. Ill. L. Rev. 123, 144 ("Regardless of whether states may use force narrowly or broadly under conventional international law, the OST itself does not alter the jus ad bellum rules of when nations may decide to initiate war. Instead, the OST places jus in bello limits on how nations can use space once a war has already begun.").

[38] Convention on International Liability for Damage Caused by Space Objects, Mar. 29, 1972, 24 U.S.T. 2389, T.I.A.S. 7762, 961 U.N.T.S. 187 (Liability Convention).

analysis related to *jus in bello*. However, the inquiry into whether a certain fact pattern constitutes an armed attack, and therefore justifies a self-defence response according to *jus ad bellum*, does not rely upon a competing legal regime analysis in this domain (and it does not rely upon such analysis in any other domain).

Nevertheless, the Outer Space Treaty (OST) is important to this analysis because it is the vehicle through which the law of armed conflict become applicable in space. Article III of the Outer Space Treaty states:

States Parties to the Treaty shall 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.[39]

There are two important aspects of Article III for the purposes of this analysis: first, the imputation of international law including the Charter of the United Nations to outer space and second, the emphasis on peaceful purposes. A small number of scholars argue that the focus on peaceful purposes might keep the law of armed conflict away from space.[40] The majority of scholars accept the notion that the law of armed conflict applies in space through the application of Article III. Helpfully, the high seas are also preserved for peaceful purposes, but there is no serious argument that the law of armed conflict would not apply to naval warfare on the high seas.[41] "Why the OST would be interpreted differently is unclear at best."[42]

Through the Outer Space Treaty both the U.N. Charter's baseline prohibition on the use of force (at least in interstate conflicts) that threaten 'the territorial integrity or political independence of any state' and the two fundamental categories of exceptions to it--the right of self-defence in U.N.-

[39] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies (27 January 1967) 610 UNTS 205 (Outer Space Treaty).
[40] Jackson Nyamuya Maogoto & Steven Freeland, 'Space Weaponisation and the United Nations Charter Regime on Force: A Thick Legal Fog or a Receding Mist?' (2007) 41 Int'l Law. 1091, 1098; Sudhakar Chandrasekharan, 'The Space Treaty' (1967) 7 Indian J. Int'l L. 61, 63; Kubo Macak, 'Silent War: Applicability of the Jus in Bello to Military Space Operations' (2018) 94 Int'l L. Stud. 1, 5.
[41] United Nations Convention on the Law of the Sea, (10 December 1983) 1833 UNTS. 397 (UNCLOS), Article 88, Note 37.
[42] Schmitt, 'International Law and Military Operations in Space' (n 16).

ordered or U.N.-mandated military sanctions--have become applicable to outer space as well.[43]

Having acknowledged outer space as the newest warfighting domain, NATO doctrine helps illuminate the types of capabilities and actions that could require *jus ad bellum* legal analysis.[44] NATO AJP 3.3(A) provides the doctrine for Joint Military Space Operations. Included among the mission areas in space are space control offensive operations and space control defensive operations. An adversary's space capabilities can be presumed to approximate NATO's. AJP 3.3(A) describes these as follows:

Offensive Operations. Offensive space control operations deny, degrade, disrupt, destroy or deceive an adversary's space capability or the service provided by a third-party's space asset(s) to the adversary at a time and place of own choosing through attacks on the space nodes, terrestrial nodes, or the links that comprise a space system. These operations range from dropping ordnance on terrestrial nodes of space systems to jamming enemy satellite uplink or downlink frequencies. Offensive space control operations initiated early in a contingency can result in an immediate advantage in space capabilities and control of the space medium.

Defensive Operations Defensive space control operations preserve space capabilities, withstand enemy attack, restore/recover space capabilities after an attack, and reconstitute space forces. Defensive space control operations should be proactive in nature to protect friendly capabilities and prevent the adversary from disrupting overall friendly operations. Suppression of threats to friendly space capabilities is a key of defensive space control operations.[45]

For operations that affect the space domain but manifest in the land domain, traditional jus ad bellum rules would apply. For example, an action that involved "dropping ordnance on terrestrial nodes of space systems" would fairly be called an armed attack if the same action against terrestrial nodes of a land-based system would be called an armed attack. It is the activities with effects in space that may require additional analysis.

While there is no state practice directly on point, the experience within

[43] Von der Dunk, 'Armed Conflicts in Outer Space: Which Law Applies' 199 (n 38).
[44] For a fuller discussion of military space operations and the definition of the space warfighting domain, *see* Macak, 'Silent War: Applicability of the Jus in Bello to Military Space Operations' 6-8 (n 42).
[45] AJP 3.3(A) at ¶ 0610 (n 3).

the last 15 years related to anti-satellite weapons (ASAT) tests from China and Russia is potentially illuminating. Article IX of the Outer Space Treaty states: "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… would cause potentially harmful interference with activities of other States Parties… it shall undertake appropriate international consultations before proceeding with any such activity or experiment." In 2007, China conducted an ASAT test by firing a ballistic missile at a defunct Chinese weather satellite.[46] Legal scholars have expressed concern that the Chinese never engaged in consultation and no negative consequences resulted.[47] No consultation has ever been conducted by the United States or the Soviet Union/Russia for their ASAT tests either. The United States stopped its program in the 1980s, but in 2008 destroyed an "out of control" satellite with a missile in an urgent mission without consultation.[48] Russia has continued its ASAT tests, including most recently in 2017 and 2020.[49] The presumption now is that state practice by both the United States and the Soviet Union with regard to ASAT tests during the Cold War, and now by both China and Russia, without invoking the Article IX consultation requirement created customary international law that excludes ASAT tests from the consultation requirement.[50]

The significance of the ASAT question is that state practice has not aligned with the treaty law and yet may be producing customary international law. In space there will be fewer sources of law to inform states' interpretation of what might constitute an armed attack. Once states begin behaving in a

---

[46] Carin Zissis, 'China's Anti-Satellite Test' (*Council on Foreign Relations Backgrounder*, 22 February 2007) https://www.cfr.org/backgrounder/chinas-anti-satellite-test accessed 22 April 2021.

[47] *See* David Koplow, 'ASAT-isfaction: Customary International Law and the Regulation of Anti-Satellite Weapons' (2009) 30 Mich. J. Int'l L. 1187.

[48] 'U.S. Missile Hits "Toxic Satellite"' (*BBC NEWS*, 21 February 2008) http://news.bbc.co.uk/2/hi/7254540.stm last accessed 23 April 2021. The U.S. test was done at low-earth orbit, where any debris would likely fall toward earth. India conducted a similar low-earthy orbit test in 2019. Vasudevan Mukunth, 'Mission Shakti: India Likely Destroyed Microsat R Satellite in First ASAT Test' (*WIRE*, 27 March 2019) https://science.thewire.in/spaceflight/mission-shakti-india-likely-destroyed-microsat-r-satellite-in-first-asat-test/ last accessed 23 April 2021.

[49] Hitoshi Nasu and Michael Schmitt, 'A Threat or A Warning: Russia's Weapons Testing in Space' (*Just Security*, 31 July 2020) https://www.justsecurity.org/71783/a-threat-or-a-warning-russias-weapons-testing-in-space/ accessed 22 April 2021.

[50] This presumption was debated during a number of sessions at the USSPACECOM Legal Conference on April 7-9 2021. Recordings of those sessions are available at https://www.youtube.com/channel/UC8aV-RW0AH3mYZmB0opKtLA?app=desktop last accessed 23 April 2021; *see also* Stephens, 'International Law in Space' 87-88 (n 2).

certain way, the absence of accountability mechanisms will create presumptions that certain behaviour is permissible, even if it sparked international outrage, as recent Chinese and Russian ASAT tests have.

Jus ad bellum therefore appears particularly impotent in the space domain, especially when considered in the context of tautological armed attack interpretations discussed in Section I, where desired outcomes tend to drive the legal analysis. Use of state practice to define customary international law will continue to degrade the existence of a legal regime. In the absence of more treaty law or the establishment of accountability mechanisms, the only hedge against expansion of the law[51] is for practitioners to adhere more faithfully to the existing treaty structure. The rest of this section favours this approach, turning to potentially predictable scenarios in space and determining what might constitute an armed attack that would justify a self-defence response.

Satellites are the predominant targets in space.[52] Satellites can be military, civilian or dual-use in nature. Satellites can be targeted with a range of existing and emerging technologies, including: jamming, dazzling, lasers, and kinetic weapons.[53] Although not all satellites are critical infrastructure, some legal scholars suggest that a demarcation of certain targets as "critical infrastructure" would facilitate a legal conclusion that the disabling of that target was an "armed attack" or "use of force."[54]

---

[51] *See* Ross Brown, 'Deficiencies in the Law of Space Conflict below Armed Attack' (2019) 51 Geo. J. Int'l L. 11, 56-57 (discussing the pressure on legal advisors to state to classify actions as "armed attacks").

[52] Frans von der Dunk addresses the question of the treaty law versus customary international law approaches to attacks on satellites. Von der Dunk, 'Armed Conflicts in Outer Space: Which Law Applies' 209 (n 38). "However, by virtue of the structural principles of the Outer Space Treaty, territorial sovereignty does not apply to outer space, and since there is no territory in the legal sense, "territory" cannot be attacked. The Charter cannot be simply applied in outer space on an "as if" basis, given the profound and consciously drafted structural provisions of space law, notably Article II of the Outer Space Treaty. Thus, unless an armed attack against a space object would in itself threaten the political independence of a State, it would not violate Article 2(4) of the U.N. Charter. Does this mean that armed attacks on satellites are not fundamentally prohibited by the U.N. Charter, but merely limited under non-Charter-based law of armed conflict rules?"

[53] *See* Ryan Esparza, 'Event Horizon: Examining Military and Weaponisation Issues in Space by Utilizing the Outer Space Treaty and the Law of Armed Conflict' 349-355 (n 38).

[54] Halberstam, 'Hacking Back: Reevaluating the Legality of Retaliatory Cyberattacks,' 204 n 34 (n 12); Sean M. Condron, 'Getting It Right: Protecting American Critical Infrastructure in Cyberspace' (2007) 20 Harv. J. L. & Tech. 404, 410; Eric Talbot Jensen, 'Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense' (2002) 38 Stan. J. Int'l L. 207, 231.

"Jamming is the overloading of enemy receivers with strong signals sent via another satellite or an uplink station."[55] Sufficient defensive encryption can protect military targets from jamming; civilian targets are more susceptible to such attacks.[56] Common targets of jamming attempts include communications or navigation satellites. A jamming attack on a satellite with broad civilian use for communications or navigation could be the proximate cause of widespread harms, including loss of life. Therefore, such an attack could plausibly be deemed a use of force, but it would be difficult to articulate jamming as "violence," unless violence is purely being defined by its consequences, e.g. loss of life. As discussed above, relying solely on such consequence-based analysis moves the analysis out of the treaty law regime and potentially into stretching customary international law with novel state practice.

Spoofing is where a "third party broadcasts a fake signal to make GPS devices think they're somewhere else other than where they actually are."[57] The results of spoofing are similar to jamming. The nature of the attack, however, is not kinetic. Spoofing is potentially analogous to deception or sabotage. For the *jus ad bellum* inquiry, the question of whether violence is intended or whether the instrument predictably would result in violence, will likely affect the legal analysis. The question of *mens rea* of the state action is relevant to the *ex ante* inquiry, especially for non-kinetic actions that are being analysed as potential uses of force. Whether a state intended *ex ante* to attack another state and impact their political independence or sovereignty will be highly influential in the legal analysis. Consequence-based analysis would be more straightforward: if the results seem analogous to kinetic uses of force, then the action may be deemed an armed attack or use of force.

Dazzling is "the temporary blinding of a sensor by overloading it with an intense signal of electromagnetic radiation, e.g., from a laser."[58] Dazzling often involves ""using a low-powered, ground-based laser to spread just enough radiation over the satellite's electro-optical sensors to blind it,"[59] though more

---

[55] Ibid at 351.
[56] Bill Boothby, 'Space Weapons and the Law' (2017) 93 Int'l L. Stud. 179, 210.
[57] Kyle Mizokami, 'Russia is Disrupting GPS Signals and It's Spilling into Israel' (*Popular Mechanics*, 1 July 2019) HTTPS://WWW.POPULARMECHANICS.COM/MILITARY/WEAPONS/A28250133/RUSSIA-GPS-SIGNALS-ISRAEL/ accessed 22 April 2021.
[58] U.S. Congress, *Office of Tech. Assessment, Anti-Satellite Weapons, Countermeasures, and Arms Control* (1985) vii https://aerospace.csis.org/wp-content/uploads/2018/09/OTA-Report-on-ASAT-Weapons-and-Countermeasures-1985.pdf accessed 22 April 2021.
[59] Jameson W. Crockett, 'Space Warfare in the Here and Now: The Rules of Engagement for

powerful lasers could be used to disable, damage, or destroy the satellite. The analysis for dazzling would be similar to the analysis for electronic weapons and jamming. Errant uses of more powerful dazzling lasers could also result in damage to satellites nearby. Lasers can also be used as kinetic weapons,[60] and the same precautions and risk of error would apply. In all of these cases, the *mens rea* is relevant, as it would be hard to imagine "armed attacks" that are inadvertent.

Kinetic weapons, such as the ballistic missile that China used in its ASAT test in 2007, would likely be analysed similarly as on earth. Kinetic weapons are inherently violent and satisfy "use of force" or "armed attack" inquiries by definition. Their use in space is therefore a fairly straightforward legal inquiry. An attack on an object using a kinetic weapon could fairly be called an armed attack and thus justify a self-defence response.

A more complicated inquiry would apply to kinetic effects from non-weapons. These could include damage from space debris, satellite collision, or uses of other space objects as projectiles in space. These actions could be advertent or inadvertent, and they could be acts of commission or omission. The analysis would likely be situation dependent, but it would have the general character of the analysis discussed above. Practitioners must decide whether to use *ex ante* (intention or instrument-based) or *ex post* (consequence-based) analysis and whether the American or ICJ approach is favoured. The political circumstances and the desired outcomes of political leaders may be outcome determinative, as discussed above.

Aside from satellites, spacecraft (including space shuttles and the International Space Station), equipment on the moon, mars or an asteroid, or personnel in space are the other potential targets in outer space that would produce a *jus ad bellum* inquiry. Attacks on space shuttles, equipment or personnel in space could be deemed an armed attack. Using an intent or instrument-based approach, once again the question would be about whether the political independence of a state were threatened. If the attack were deliberate and high-status individuals such as astronauts or a space shuttle (significant government property) were targeted, the event could

U.S. Weaponized Satellites in the Current Legal Space Regime' (2012) 77 J. Air L. & Com. 671, 675.

[60] Use of lasers would also be subject to legal analysis as a potentially prohibited weapon, but such analysis would not necessarily inform whether their use constitutes an "armed attack." *See* The Protocol on Blinding Laser Weapons, Protocol IV of the 1980 Convention on Certain Conventional Weapons (13 October 1995) 1380 UNTS 370.

amount to an armed attack. In practice, the analysis would likely focus on the outcome of the attack and whether it seems to justify a self-defence response in the tautological approach described above. In space, the lack of state practice creates a relative clean slate where an event would likely be taken as an issue of first impression and responses would be driven by factors outside of the legal analysis (e.g. geopolitics, domestic reactions, etc.).

In the absence of any effort to create additional treaty law in this area, future state practice will "begin to highlight the contours of these fundamental principles and thresholds, and will be essential in elucidating the content of international law in this domain."[61] The United States has been relatively transparent, as compared with other states, about its positions on the law of armed conflict's applicability in space.[62] Other states have not been as forthcoming, leading to some uncertainty about potential future state practice. The American and international positions will be illuminated when put to the test.

III. Absolute Liability for Harms in Space and Armed Attacks by Non-state Actors

The foregoing analysis assumed state-on-state actions for the sake of clarity. An important consideration in space, however, is the extent to which space activities are being undertaken by non-state actors, and the potentially wide-reaching effects such activities may have. Article IV of the Outer Space Treaty states:

States Parties to the Treaty shall bear international responsibility for national activities in outer space, including the Moon and other celestial bodies, whether such activities are carried on by governmental agencies or by non-governmental entities, and for assuring that national activities are carried out in conformity with the provisions set forth in the present Treaty. The activities of non-governmental entities in outer space, including the Moon and other celestial bodies, shall require authorization and continuing supervision by the appropriate State Party to the Treaty.[63]

Article IV thus imputes state responsibility for the actions of non-state actors. Nothing in the text of the Outer Space Treaty would distinguish criminals,

[61] Matthew T. King & Laurie R. Blank, 'International Law and Security in Outer Space: Now and Tomorrow' (2019) 113 AJIL Unbound 125, 129.
[62] Ibid.
[63] Outer Space Treaty, Article IV (n 42).

ordinary citizens, or corporations from each other; states bear responsibility for the actions emanating from that state. This liability regime is unique to outer space.[64]

The Liability Convention establishes absolute liability for states with respect to damages in space resulting from actions emanating from the territory of that state or from space objects launched from the territory of that state.[65] The Liability Convention creates a claims process and regime for damages in space and does not speak directly to questions of *jus ad bellum*.[66] Nevertheless, the combined obligations from the Outer Space Treaty and the Liability Convention regarding state liability for the actions of non-state actors suggests states will be held to a higher level of responsibility for aggressive actions of non-state actors emanating from their territory.

The most straight-forward scenario of an armed attack in space would be the launching of a ballistic missile at an important satellite of another state. If that missile emanates from the territory of a specific state, an immediate presumption would be that the specific state is responsible. If a terrorist group within that state were instead responsible, effects on earth might not justify a self-defence response against the sovereign state;[67] in space they could.

In the cyber domain, attribution creates serious problems and legal analysis of jus ad bellum questions is often hampered by the ability to trace harms back to a state actor. Absolute liability in space significantly alters the legal inquiry. If damage results from a space object that can be traced to the territory of a State, then that state is arguably liable. If such damage can be categorized as an armed attack, then a self-defence response might be justified. This creates the potential for dangerous escalation in the face of uncertainty and is an area worthy of further legal analysis and political attention.

IV. Conclusion

This article seeks to illuminate the treaty and customary international law

---

[64] Von der Dunk, 'Armed Conflicts in Outer Space: Which Law Applies' 196 (n 38).
[65] Liability Convention (n 40).
[66] Only one case has invoked the Liability Convention thus far. In 1978, the Cosmos 954 Soviet maritime surveillance satellite fell from orbit onto uninhabited Canadian territory. Rather than adjudicate the case through the Liability Convention claims process, Canada and the USSR negotiated a settlement. Canada-Union of Soviet Socialist Republics: Protocol on Settlement of Canada's Claim for Damages Caused by 'Cosmos 954,' (1981) ILM 20 (1981). In the course of the negotiations, the USSR argued that the Liability Convention did not apply.
[67] *Cf.* The NATO missions in Afghanistan.

approaches to determining whether an armed attack has occurred in space. Legal practitioners should distinguish whether they are using *ex ante* or *ex post* analysis, and understand the consequences of either choice. Whether an action is akin to a kinetic use of force, whether it meets colloquial definitions or notions of "violence" or can fairly be called "armed" are all relevant factors in the legal analysis. *Mens rea* is also important in the *ex ante* analysis. Ultimately, political interests and a legal culture of "getting to yes" may push legal practitioners toward outcomes-based analysis. In space, there is not a lot to constrain the analysis, so each of these decisions must be taken carefully and with an understanding of the significance of state practice in building customary international law.

While any action that constitutes an armed attack in space justifies a self-defence response, a self-defence response is never required. The concern or apprehension that an act authorizes a self-defence response should therefore not cloud the analysis. There are ample options for responses, including diplomacy, communications, sanctions, and non-lethal military responses. This point is particularly important because, while there are few actions that would necessarily constitute an armed attack in space according to treaty law, a customary international law approach that is state practice-focused might be more permissive. There are many actors who, through the state responsibility and liability framework in outer space, would trigger a right of self-defence from state-to-state. If self-defence is authorized, there are many reasons one still need not act.

***

Source: www.nato.int @SpaceX Starlink Mission

Attack on Critical Space Infrastructures: A Case of Self-Defence for the NATO Alliance? [1]

by Dr Annette Froehlich[2]

Satellites are very vulnerable since they orbit the Earth in allocated and therefore predictable trajectories that can be tracked even on various Internet platforms. An attack on critical space infrastructure may take various forms, meaning the terrestrial based ground stations but also and foremost the satellites in orbit. They may be affected in a physical way (destruction of the satellite as already demonstrated by several national ASAT tests) or by non-kinetic means (interfering with space-based services by blinding, jamming or spoofing). Those hostile interferences may lead to a non-functioning of the essential capabilities of a state, in particular when related to communication

[1] **DISCLAIMER**: The views expressed in this article are solely those of the author and may not necessarily represent the views of NATO, Allied Command Operations, or Allied Command Transformation, or of their affiliated organizations.

[2] Dr Annette Froehlich is a scientific senior expert seconded from the German Aerospace Centre (DLR) to the European Space Policy Institute (ESPI) in Vienna, and an honorary adjunct senior lecturer at the University of Cape Town (SA) at SpaceLab. Moreover, she lectures space defence related topics at the Austrian National Defence Academy (Vienna) and the Bundeswehr Command and Staff College (Hamburg). Email: Annette.Froehlich@espi.or.at; Annette.Froehlich@southernspacestudies.com.

and navigation space-based services. This applies to civil and commercial domains, but also for military space applications, especially as those services are strongly interrelated. Moreover, as part of the North Atlantic Treaty Organization's (NATO) defence and crisis management, the functioning of NATO member states' satellite-based services is vital for its complex defence equipment and missile detection systems. However, the international United Nations (UN) space treaties are mute in regard to attacks on space infrastructure - no provisions explicitly cover these aspects. Nevertheless, this does not lead to the conclusion that defending one's own space assets (satellites) is not allowed. Indeed, the international space treaties were mostly elaborated and adopted during the first satellite launches to ensure a minimum standard and the non-militarization of outer space, in a domain qualified as the global commons. This is characterized by the absence of any sovereignty and thus common to all states (*res communis omnium*) because it is considered as the province of humankind.

Since technical developments could not be foreseen in detail, various space related aspects were not covered by those UN space treaties in the second half of the last century. Moreover, during the Cold War, certain provisions were formulated deliberately vaguely to reach consensus among the Western/capitalist and Eastern/communist bloc. Therefore, essential terms for defining the scope of the UN space treaties like "(outer) space" or "space object" were kept undefined. However, consensus was achieved on various principles and adopted in the form of the "Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space"[3] in 1963. Its main principles were later echoed in the Outer Space Treaty (OST) of 1967[4], considered as the Magna Carta of international space law. In the following years, various stipulations of the OST were refined by further UN treaties such as the Rescue and Return Agreement (ARRA) in 1968[5] in regard to co-operation and assistance for personnel of a spacecraft in the event of accidents, distress, or emergency landing, and the return of space objects; in

[3] Legal Principles Declaration – LPD, UNGA Res 1962 (XVIII) (13 December 1963)
[4] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies (adopted 5 December 1979, entered into force 10 October 1967) 610 UNTS 205 (OST) (Status of ratification as of 1 January 2020: 110 states)
[5] Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space (entered into force 3 December 1968) 672 UNTS 119 (Status of ratification as of 1 January 2020: 98 states)

1972 by the Liability Convention (LIAB)[6] to clarify the liability provisions in view of adequate and prompt compensation for damage caused by space objects; and in 1975 by the Registration Convention (REG)[7] to facilitate the identification of human-made space objects. Finally, ten years after the first Moon landing by the U.S., the Moon Agreement (MOON)[8] was adopted in 1979 by the international community and includes a controversial regime for the use of natural resources of the Moon. Although those rules were elaborated and adopted at a common international level, only a few states have signed or ratified this Moon Agreement, which highlights the difficulties of achieving consensus on an international level.

1. International Space Regulations to Ensure the Peaceful Use of Outer Space

The OST was widely signed and ratified by the members of the international state community and its fundamental provisions are considered as having the status of international customary law. Moreover, Art. I-1 OST stipulates clearly that "The exploration and use of outer space (…) shall be carried out for the benefit and in the interests of all countries"[9]. Already those first provisions may be invoked in case of an attack against a space object (satellites) since any interference may certainly not be considered as "for the benefit and in the interests of all countries"[10]. Moreover, in the general context of the peaceful use of outer space, reference is also made to Art. IV OST, which proclaims that states commit themselves not to place in orbit nuclear weapons or weapons of mass destruction. However, this article only refers to those explicitly mentioned weapons and no placement in orbit is needed to damage or interfere with the well-functioning of a satellite. In addition, paragraph 2 of Art. I OST relates only to activities around the Moon, which must be exclusively for peaceful purposes. Therefore, those stipulations do not specifically cover the question of attacking a space infrastructure or the case of self-defence in

[6] Convention on International Liability for Damage Caused by Space Objects, UNGA Res 2777 (XXVI) (29 March 1972) (Status of ratification as of 1 January 2020: 98 states)
[7] Convention on Registration of Objects Launched into Outer Space, UNGA Res 3235 (XXIX) (12 November 1974) (REG) (Status of ratification as of 1 January 2020: 69 states)
[8] Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, UNGA Res 34/68 (5 December 1979) (Status of ratification as of 1 January 2020: 18 states, i.e., Armenia, Australia, Austria, Belgium, Chile, Kazakhstan, Kuwait, Lebanon, Mexico, Morocco, Netherlands, Pakistan, Peru, Philippines, Saudi-Arabia, Turkey, Uruguay and Venezuela. Four further states have signed, but not yet ratified: France, Guatemala, India, and Romania).
[9] OST (n 2) art. I-1
[10] OST (n 2) art. I-1

this regard. However, further provisions may shed more light, such as Art. I-3 OST which declares: "Outer space (…) shall be free for exploration and use by all States (…) in accordance with international law, including the Charter of the United Nations, in the interest of maintaining international peace and security."[11]

2. The Right to Self-Defence in Outer Space

Art. I-3 OST explicitly mentions the UN Charter, however it does not contain any further space related regulations. Art. 2.4 UN Charter requires only in a broad sense 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."[12] This means that the use of force is prohibited unless it falls within the enumerated permitted exceptions, i.e., either an authorization provided by the UN Security Council or in case of self-defence. Therefore, the question that arises is whether self-defence can be invoked in case of hostile interference with a satellite.

Art. 51 UN Charter clearly states that "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security"[13]. Moreover, this article explicitly recognizes not only an individual but also a collective right for self-defence in case "an armed attack occurs against a Member of the United Nations". Even if this collective right is explicitly enumerated, which would be for example the case of NATO, essential aspects of this article were not further defined. Therefore, jurisprudentially, the International Court of Justice (ICJ) has developed criteria over the last decades such as the "occurrence"[14] of an armed attack, its imputation to a state[15], and a certain "necessity and proportionality"[16] as the countermeasures

---

[11] OST (n 2) art. I-3
[12] UN Charter art. 2.4
[13] Ibid art. 51
[14] *Nicaragua Case, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)* (Merits) [1986] ICJ Rep. 392 para. 195 and 211; *Oil Platforms (Islamic Republic of Iran v. United States of America)* (Judgment) [2003] ICJ Rep. 161 para. 51
[15] *Oil Platforms (Islamic Republic of Iran v. United States of America)* para. 51; see further: Froehlich/Tăiatu, *Space in Support of Human Rights* (Studies in Space Policy Vol. 23, Springer 2020) 63 ff; *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)* (Judgment) [2005] ICJ Rep. 168 para. 146
[16] *Nicaragua Case, Military and Paramilitary Activities in und against Nicaragua (Nicaragua v.*

that are meant to keep or restore peace should have no punitive character. Moreover, since self-defence should also prevent an attack[17], the aspect of a pre-emptive right of self-defence has been elaborated. Otherwise, after a hostile raid the attacked state may no longer exist or be able to exercise its right of self-defence.

These well-established jurisprudential criteria may however nowadays be challenged by high technology. Therefore, it is debatable if those criteria are still suitable for space-based activities. Indeed, already even the notion of "occurrence of an armed attack" or "imminence" can no longer be evaluated as it used to be for terrestrial manoeuvres due to the high speed and mostly invisibility of those attacks. In parallel to cyberspace those attacks may consist of non-physical or non-visible threats. Consequently, war or conflict situations may increasingly take on the character of non-physical or non-visible attacks and will become a constant part of our daily life. Therefore, any assessment of intention may turn out to have an uncertain character. Moreover, it may be very difficult or quite impossible to demonstrate that those hostile interferences were emanating from another state (entities) and consequently imputable to this state. In addition, the criteria of "proportionality" may also be very difficult to assess since in case of the physical destruction of a satellite, the much greater damage lies in its dysfunction and loss of the correct transmission of satellite signals and data. Misleading data can have tremendous, unpredictable and devastating consequences if not discovered forthwith. This may lead to impairment or failure of communication or navigation-based applications affecting tremendously the functionality, even the survival, of a state and its society.

3. An Attack on a Satellite in Outer Space - A Case for the NATO Defence Alliance?

Since around half of the 2,000 functional satellites in orbit belong to NATO member states (with an upward tendency) and all NATO member states are members of the UN, it is of utmost importance to analyse if any kind of hostile attack against a satellite of a NATO member state may trigger the Alliance case according to Art. 51 of the UN Charter as it is "against a Member of the

United States of America) (n 13) para. 194 and 237; *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep. 226 para. 41

[17] Annette Froehlich, *The Right to (Anticipatory) Self-Defence in Outer Space to Reduce Space Debris*, in: Annette Froehlich (eds), *Space Security and Legal Aspects of Active Debris Removal* (Studies in Space Policy Vol. 16, Springer 2019) 71-92

United Nations"[18].

3.1. NATO as a Defence Alliance with Geographic Boundaries

With respect to collective defence, Art. 5 of the North Atlantic Treaty stipulates: "The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations will assist"[19]. However, this armed attack has to occur within NATO's geographic boundaries according to Art. 6 North Atlantic Treaty which defines the scope of the aforementioned Art. 5. Therefore, according to the first sub-paragraph of Art. 6, the armed attack has to occur either on allied territories meaning "on the territory of any of the Parties in Europe or North America, on the Algerian Departments of France[20], on the territory of Turkey or on the Islands under the jurisdiction of any of the Parties in the North Atlantic area north of the Tropic of Cancer"[21] or, according to the second sub-paragraph of Art. 6, "on the forces, vessels, or aircraft of any of the Parties, when in or over these territories or any other area in Europe in which occupation forces of any of the Parties were stationed on the date when the Treaty entered into force or the Mediterranean Sea or the North Atlantic area north of the Tropic of Cancer."[22] Despite this extensive list, outer space is however not mentioned *expressis verbis*. Therefore, whether the mutual assistance clause of Art. 5 of the North Atlantic Treaty, which constitutes the core and purpose, the *raison d'être* of NATO, is also applicable in case of an attack in outer space, must be analysed.

3.2. Outer Space - NATO's New Operational Domain

As mentioned at the beginning, outer space is considered as global commons meaning free access to outer space is granted to all countries. NATO recently reconfirmed these global commons character of outer space in its report on "Assured Access to the Global Commons, Maritime, Air, Space,

---

[18] UN Charter art. 51
[19] The North Atlantic Treaty (Washington D.C., 4 April 1949) art. 5
[20] Note footnote 2 of the North Atlantic Treaty "On January 16, 1963, the North Atlantic Council noted that insofar as the former Algerian Departments of France were concerned, the relevant clauses of this Treaty had become inapplicable as from July 3, 1962", https://www.nato.int/cps/en/natohq/official_texts_17120.htm
[21] The North Atlantic Treaty (n 18) art. 6, sub-para. 1
[22] Ibid art. 6, sub-para. 2

Cyber"[23] and underlined its importance. "The Alliance relies and increasingly depends on assured access to all four domains – often simultaneously. Assured access is vital for the indivisibility of NATO's security and a prerequisite for the Alliance to fulfil its essential core tasks: collective defence, crisis management, and cooperative security".[24] Moreover, NATO clearly stated that those four domains are interwoven. "The loss of access to one of these domains would affect detrimentally NATO's ability to operate effectively in any of the others. Perhaps the most compelling example would be NATO's integrated air and missile defence system that depends on concurrent access to all four domains. A missile targeting NATO territory would be detected and tracked by a combination of cyber- and space-enabled systems and finally intercepted by a ground or sea based missile."[25] Therefore, within those recommendations for the Alliance, it is highlighted that NATO should "establish the Alliance's state of preparedness and (...) determine implications for the ability of the Alliance to conduct its core tasks if access to the commons were denied."[26] This is of utmost importance since "NATO's membership comprises several of the most advanced space-faring nations in the world"[27] and outer space has been becoming more and more a recognised domain of warfare in NATO's member states concretized by the creation of special space entities within its armed national forces (as the United States Space Force – USSF) or by the elaboration of a dedicated Defence Space Strategy as in France, leading to a reorganization of its Air Force into Air and Space Forces for "better protecting our satellites"[28].

Furthermore, on 20 November 2019, the representatives of NATO member states "agreed to recognize space as a new operational domain for NATO, alongside air, land, sea and cyber."[29] This constitutes an important decision to adapt the Alliance to the changed position of outer space due to

---

[23] NATO, 'Assured Access To The Global Commons: Maritime, Air, Space, Cyber' (3 April 2011) https://www.act.nato.int/images/stories/events/2010/gc/aagc_finalreport.pdf accessed 4 May 2021

[24] Ibid. p. 3

[25] Ibid. p. 5

[26] Ibid. p. 8

[27] Ibid. p. 4

[28] Nicholas Wu, 'French President Emmanuel Macron Announces Creation Of French Space Force' (*USA TODAY*, 13 July 2019) <https://eu.usatoday.com/story/news/world/2019/07/13/french-space-force-macron-announces-creation-space-force-command/1723998001/> accessed 4 May 2021

[29] NATO, 'Foreign Ministers take decisions to adapt NATO, recognize space as an operational domain' (20 November 2019) https://www.nato.int/cps/en/natohq/news_171028.htm accessed 4 May 2021

the increased variety of actors and privatisation or commercialisation of outer space.[30] Whether the space faculties of NATO's member states are sufficient to cover this wide domain of outer space, may be questioned. However, it is not the facility to cover a wide geographic area that is required but the capacity to intervene for concrete space related actions. In this regard, NATO member states have already demonstrated a high competence in tracking space objects thanks to their sophisticated surveillance systems.

In former times, it was doubted if outer space was part of NATO's operational domain and several scenarios were drafted especially regarding the geostationary satellites. They orbit the Earth in an assigned equatorial slot geosynchronous with a part of a surface on Earth in a "fixed" position over its assigned territories. Therefore, they could be considered as "over" the territory of a NATO ally, especially in the case of communication and navigation satellites, which provide essential data services and applications for the survival of NATO member states.

However, on the international level, the status of geostationary orbits has already been widely discussed. Several Equatorial states, in particular, have advocated that these orbiting positions belong to the state geographically below (in analogy to air space where the air corridor over a country is considered as belonging to the state below). Those Equatorial countries (hoping for fees for the use of those geostationary slots above their territories) issued the Bogotá Declaration[31], stipulating their sovereignty on the part being "over" their territory. This declaration was widely rejected by the spacefaring nations fearing for their free use of outer space as guaranteed by Art. 1-2 OST ("shall be free for exploration and use by all States without discrimination of any kind, on a basis of equality and in accordance with international law, and there shall be free access to all areas of celestial bodies."[32]) Moreover, reference was made to Art. II OST and its non-appropriation clause stipulating that "outer

[30] However, NATO Secretary General Jens Stoltenberg clarified that "NATO will not become an autonomous space actor. (…) NATO has no intention to put weapons in space. We are a defensive Alliance" and will therefore continue to rely on national space capabilities for its missions and operations; Dr. Kestutis Paulauskas, 'Space: NATO's latest frontier' (*NATO Review*, 13 March 2020) https://www.nato.int/docu/review/articles/2020/03/13/space-natos-latest-frontier/index.html accessed 4 May 2021

[31] The Bogotá Declaration (signed in Bogotá 3 December 1976 by Brazil, Ecuador, Indonesia, Kenya, Columbia, Republic of Congo, Uganda, and Zaire) https://bogotadeclaration.wordpress.com/declaration-of-1976/ accessed 4 May 2021

[32] OST (n 2) art. I-para. 2

space, including the moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means"[33]. Furthermore, other satellites are not orbiting the Earth synchronously and therefore are not matching its rotation. In consequence, a declaration that a portion of an orbit belongs to the territory of a state, would anyway not be very effective.

4. Exercise of Power Based on Non-Territorial Criteria

Since harmful interferences on satellites are not necessarily of a physical nature (destruction of the satellite), but more likely to occur by non-kinetic means, the right of self-defence based on sovereignty should find its legal foundation in the exercise of power rather than on territory criteria. Although international space law does not foresee state flags for space objects (in contrast to the Law of the Sea and its system of state flags for ships), other legal requirements can provide similar connection links between a state and its space object. Indeed, even if satellites are situated in an international area of global commons according to Art. I OST, this does not exclude an exercise of sovereignty rights over own space objects since the space related UN treaties set up the concepts of launching state(s) and registry state.

4.1.1. Concept of Launching State(s)

According to the OST, several states can be qualified as launching state. The OST defines launching states in Art. VII OST as the state that "launches or procures the launching of an object into outer space"[34], and/or any State "from whose territory or facility an object is launched"[35]. This definition was confirmed by the LIAB in its Art. I. Therefore, due to this broad definition, a multitude of states may be considered as launching state for one and the same space object, which differs from the status of registry state.

4.1.2. Registry State and Deriving Rights and Obligations

In addition, international UN space regulation system includes the system of registration of space objects with the UN. Indeed, in its Art. II para. 1 the REG requires that "the launching State shall register the space object"[36]. Even if it seems just to be a kind of administrative formality, this registration is of high importance as it entails several rights and obligations for the registry state on

[33] Ibid. art. II
[34] Ibid. art. VII
[35] Ibid.
[36] REG (n 6) art. II para. 1

the international level. Indeed, Art. VIII OST determines that the state of registry has the right to exercise jurisdiction and control over the space object registered under its name. The state of registry follows the idea of flag state so that the satellite keeps being under the jurisdiction as does a ship, regardless of its geographic position. Indeed, this registration is the constituent element, i.e., the link between the space object (satellite) and its state. Since attacks on space assets may occur more and more in an invisible manner, this may impact the traditional three-element-doctrine[37] of Georg Jellinek, in view of the constitutive criteria of statehood. Art. VIII OST confers a clear right to the state to exercise jurisdiction and control over its space objects, regardless of their presence in space.[38] Those rights are confirmed by the LIAB under Art. VIII which reveals the counterpart of this right of exercising control by stipulating that in case of damage caused by this space object compensation may be sought from this state.

Thanks to this registration with the UN, which establishes this important link between the state of registry and the satellite, the satellite is considered as belonging to the state as this registration entitles the state of registry to exercise jurisdiction and control, a form of expression of its sovereignty. Therefore, from an international law perspective, the state of registry may be considered as entitled to exercise the right of self-defence in case of harmful interference against this satellite. However, it is essential to clarify in advance which state has the right to register. Therefore, Art. II para. 2 REG defines the particular state in the event of a multitude of states being involved in the satellite launch (which nevertheless all may be qualified as launching states). "Where there are two or more launching States in respect of any such space object, they shall jointly determine which one of them shall register the object". This is an important decision as a change of state of registry at a later stage is not possible, so far.[39]

Furthermore, in the context of the International Space Station (ISS) and the right to exercise jurisdiction in outer space, reference may also be made to its Intergovernmental Agreement (IGA) signed by the involved countries. Art. 5.2 IGA stipulates that "each Partner shall retain jurisdiction and control over the elements it registers (…) and over personnel in or on the Space Station who are its nationals"[40]. Moreover, it is settled that each partner owns the respective

[37] A state territory, a state people and state power.
[38] OST (n 2) art. VIII
[39] This context is meanwhile questioned and debated due to the development of technology and the upcoming practice of change of ownership of satellite in orbits.
[40] Agreement Concerning Cooperation on the International Space Station (signed 29

elements provided to the ISS.

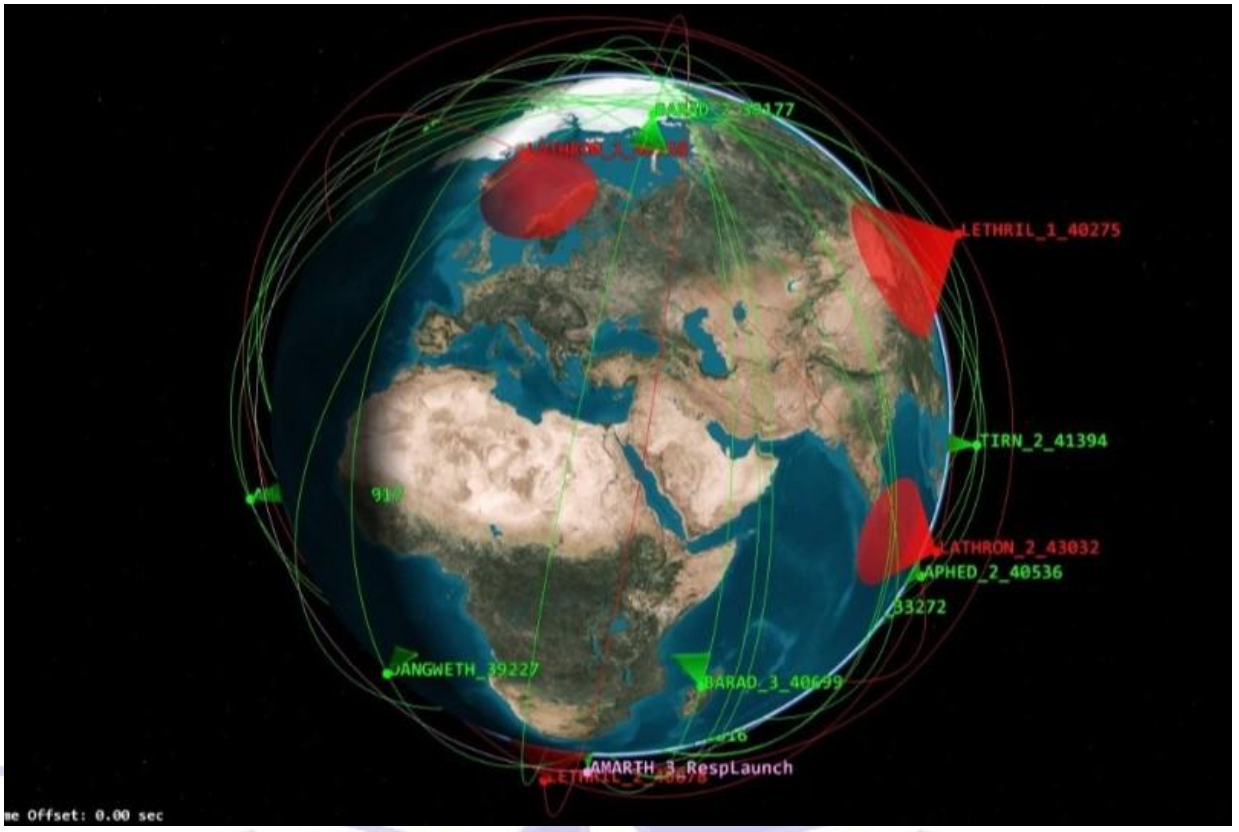
Nevertheless, since the registration of outer space objects can only be done by one state without further changes, this may lead to unfortunate situations probably standing in the way of any military intervention especially if a non-NATO member state is involved. This may be in the case of ownership transfer in orbit (after its registration). The new state owner does not have the right to exercise jurisdiction and control, even if needed for the right of self-defence. This has consequences on further diplomatic strategic considerations. Indeed, if a non-NATO state is in conflict with a NATO member state and is destroying the functioning of one of the satellites of this NATO member state, who no longer owns it, this state could nevertheless be considered to have the right to exercise its right of self-defence. This may be a very ambiguous situation, so that a state is the new owner of a satellite but has not the right of self-defence. However, its first owner has this right, but may not have the interest to act in self-defence since it has good relations with the aggressor. This could also be used as a tactical manoeuvre to turn two states against each other through a third by attacking a satellite that has changed ownership.

Conclusion

However, with an increasing number of space satellite missions and constellations, the rights of the owners will be more detailed. The upcoming space resources projects of private companies already exhibit a new approach and reading of Art. II OST which, in former days, was considered as the guarantee for non-appropriation in outer space. More and more national legislations in favour of space resource activities are advocating a different approach. The same may be experienced with increasing numbers of in-orbit-transfers of satellites. The registration system for satellites may be changed due to factual situations taking into account new needs and challenges. Then other bi-lateral agreements establishing the course of transfer of ownership for a satellite in detail will address the questions around the right of self-defence to ensure the well-functioning of a satellite system.

***

January 1998 in Washington D.C.) TIAS 12927 (International Space Station Intergovernmental Agreement – IGA) Art 5.2



Source : https://ac.nato.int Photo based on screenshot from AGI

Security-by-Design Approaches for Critical Infrastructure: Mapping the Landscape of Cyber and Space Law[1]

by Avv. Antonino Salmeri, Adv. LL.M[2] and
Mr. Antonio Carlo[3]

Introduction

After more than half a century of space activities, scientific and technological progress has led to the blossoming of new technologies that have deeply impacted both civil and military spheres. Since the launch of the first artificial satellite, the cyber and space domains have gradually become

[1] **DISCLAIMER**: The views expressed in this article are solely those of the authors and may not necessarily represent the views of NATO, Allied Command Operations, or Allied Command Transformation, or of their affiliated organizations.

[2] Doctoral Researcher in Space Law at the University of Luxembourg and registered attorney at the Italian BAR, antonino.salmeri@uni.lu

[3] PhD Candidate at Tallinn University of Technology, ancarl@taltech.ee

two faces of the same coin and now one could not exist without the other. The strengthening of relations between these two domains holds the potential to bring disruptive changes to both environments, as showcased by the 'big data' phenomenon as well as by the emergence of cyber-attacks as a new category of threats. In recent years, the space sector has witnessed a new, fourth industrial revolution[4] resulting in the development of new emerging disruptive technologies (EDTs) and breakthroughs like artificial intelligence. The development of these new technologies further influenced the interconnection between the cyber and space domains and ultimately led to their "democratisation", with a multitude of public and private actors currently conducting activities in these fields. On the one hand, the interrelations between cyber and space allow for their mutual support in terms of defence and resilience. On the other one, the close interconnection of the cyber and space domains has aggravated the threat that EDTs pose to their respective critical infrastructure. This context is further complicated by the legal status of outer space as enshrined in Articles I and II of the Outer Space Treaty (OST)[5], as well as by the fragmented nature of international law, which pose additional challenges to the effective enforcement of existing national and international regulations. In this situation, the dependence of North Atlantic Treaty Organization's (NATO) military operations on cyber and space technologies exposes the organization to new types of vulnerabilities. In light of the critical strategic importance of cyberspace and outer space for warfare, security-by-design approaches in the early stages of their conjunct development are not only desirable but indispensable. As part of this process, particular attention should be given to cyber cooperation as an indispensable tool for the mitigation of cyber threats. Ultimately, given the ultra-hazardous nature of space activities, security concepts should extend beyond cyber security to cyber defence and eventually also cyber resilience.

Building on the above premises, this article evaluates and analyses the interrelations between outer space and emerging cyber technologies from the legal and policy viewpoints. Throughout the analysis, particular attention is given to what role could be played by organisations like NATO for the peaceful, sustainable and strategic use of these interconnected domains.

---

[4] Also known as Industry 4.0. It refers to the correlation of physical assets and advanced digital technologies. K. Schwab, *The Fourth Industrial Revolution* (Penguin 2017).

[5] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, entered into force 10 October 1967, 610 U.N.T.S. 205 (hereinafter referred to as "OST").

The context: targets and threats

Over the years, modern Western states have created a model of society that is characterised by a high quality of life, meaning the possibility of accessing a set of 'basic' services and opportunities that are made available to each citizen to express their attitude and fulfil their needs. From this perspective, the quality of life is defined by, for example, energy supply services, health protection, the transport system, the banking system and in recent years, space and cyber activities. Therefore, it is important to better understand the real dependence of society on those infrastructures that allow the provision of services that characterise the quality of life. These infrastructures have been called 'critical' and the need to protect their existence and correct functionality is synonymous with the need to safeguard the quality of life. To this end, critical infrastructure can be defined as "an asset, system or part thereof located in [a state] which is essential for the maintenance of vital societal functions [...] and the disruption or destruction of which would have a significant impact in a [state] as a result of the failure to maintain them".[6] Critical infrastructure has therefore become a natural target of malicious attacks, as the impact produced is relatively high compared to the effort needed to generate the event itself.

For these reasons, critical infrastructure has become increasingly vulnerable to the rise of EDTs. As mentioned, EDTs include those technologies that are cutting-edge and that have potential opportunities in the Information and communications technology (ICT) sector.[7] For instance, in October 2019, the NATO Defence Ministers identified eight EDTs in the areas of data, quantum, artificial intelligence (AI)[8], autonomy, space, hypersonic, biotechnology, and materials.[9] These areas tend to be extremely broad and have significant

---

[6] Council Directive (EC) 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

[7] NATO, 'NATO Advisory Group of Emerging and Disruptive Technologies' (Annual Report 2020). https://www.nato.int/nato_static_fl2014/assets/pdf/2021/3/pdf/210303-EDT-adv-grp-annual-report-2020.pdf accessed April 2021.

[8] The first definition of AI appeared in 1956 during a workshop on AI at Dartmouth University. Since then, many definitions have followed. John McCarthy, also known as the father of AI, defined AI as "the science and engineering of making intelligent machines". LIAO Matthew, *Ethics of Artificial Intelligence* (Oxford University Press 2020) 3.

[9] NATO Science & Technology Organization, 'Science & Technology Trends 2020-2040: Exploring the S&T Edge' https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf accessed April 2021.

overlaps. In this context, data, AI, autonomy, space and hypersonics are regarded as 'disruptive' while developments in quantum, biotechnology and materials are seen as 'emergent' as they still require more time to mature.[10] The development of new EDTs has led to the rise of new threats. The growing sophistication of the tools and techniques available to malicious actors, combined with the increasing digitisation, has resulted in new challenges to security. These threats can be classified as kinetic and non-kinetic. Kinetic threats are those that attempt to strike directly or detonate a weapon near a satellite or other space stations.[11] Non-kinetic threats involve weapons that have physical effects on space systems without any physical contact such as in electronic and cyber warfare.[12] Since this article explores the connections between the cyber and space domains, the present analysis will focus mainly on non-kinetic threats, particularly in the cyber field. In this respect, while cyberattacks are not a new threat to the space industry, malicious cyber actors have become much more sophisticated. These cyber actors usually stem from one of the following four categories:[13] nation state actor, private economic actor, hacktivists/natural persons and international entities.[14] These actors can either be the instigator of an attack, responsible for the attack, the victim or collateral victim of the attack. As technology continues to evolve, so do the opportunities and challenges it poses. In particular, the ever-increasing dependence on technologies exposes us to a whole set of risks associated with cyberattacks. Hostile cyber actors are continuously trying to break into close and highly secure systems while the cyber threat landscape continues to expand and evolve rapidly. To counter these issues, space systems' security and defence need to be constantly updated, secured, and monitored. Many governments, companies, and international organisations have created ad hoc Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) coordinated by Security Operational

[10] They are expected to mature in a timeframe of 20 years, *supra* nota 9.
[11] A. Carlo, L. Lacroix, L. Zarkan, 'The challenge of protecting space-based assets against cyber threats' (71st International Astronautical Congress 2020).
[12] A. Carlo, N. Veazoglou, 'ASAT Weapons: Enhancing NATO's Operational Capabilities in the Emerging Space Dependent Era' (6th International Conference Modelling and Simulation for Autonomous Systems 2019).
[13] P. Wallace, R. J. Schroth, W. H. DeLone Cybersecurity Regulation and Private Litigation Involving Corporations and their Directors and Officers: A Legal Perspective (Kogod Cybersecurity Center. Kogod School of Business, American University 2015).
[14] Supra note 11.

Centres (SOCs) in order to pre-empt and, if necessary, confront possible cyber events.[15]

The cyber domain is vast and presents different subcategories such as cyber-security, cyber-crime, cyber-terrorism, cyber-sabotage, cyber-attack, cyber-war, information warfare, cyber-espionage, etc. These are just some of the terms denoting the criminal use of the cyber network. They go hand in hand with the evolution of these phenomena and with the legislative developments that attempt to regulate them while it becomes increasingly difficult to cope with the protection of critical infrastructure, or the complexity deriving from the combination of Information and Communication Technology (ICT) with the key management systems of the functions of modern companies.[16] The online market now offers highly specialised products and services to commit criminal activities and / or carry out cyber threats (crime-as-a service), modifying the more traditional and hierarchical forms of organised criminal groups, in favour of networks characterised by fluidity, changeability and transience.[17] These networks are formed on the basis of limited actions and projects that are limited in time and objectives, thanks to the work of professional freelance cyber-criminals who sell their skills and tools (malware, zero-day exploits, or access to botnets) to criminal and terrorist groups. Furthermore, the growing specialisation of cybercriminals exponentially increases the offensive capabilities of other traditional criminals who do not possess this technological know-how. There are various organised underground markets (with sellers, buyers and intermediaries) implemented through online forums and characterised by different degrees of accessibility and technology. For instance, 80-90% are cyber-criminals with basic skills who essentially sell financial or counterfeit goods, while 10-20% make up highly qualified individuals who sell products and sophisticated tools, suitable for targeting individuals, companies, organisations, government bodies, etc.[18] This market can be further divided into single 'cyber-professionals' or those structured in small groups (70%), criminal organisations (20%), cyber-terrorists (5%), cyber-criminals hired by government agencies (4%), and activists (1%).[19] Although this is a global

[15] Samuele De Tomas Colatin, 'National Cybersecurity Organisation: Italy', in National Cybersecurity Governance Series (CCD-COE 2020).
[16] Schmitt N. Michael, Brian T. O'Donnell, *Computer Network Attack and International Law* (Naval War College 2002) (hereinafter referred to as "CNAIL").
[17] European Cybercrime Centre, *The Internet Organised Crime Threat Assessment* (Europol 2014).
[18] Stefan Fafinski, *Computer Misuse. Response, Regulation and the Law.* (Routledge 2013).
[19] ibid.

market, the most prominent cybercriminals that conduct malware attacks come from China, Latin America, and Eastern Europe. Russia, Romania, Lithuania, Ukraine and other Eastern European countries feature more prominently for those targeting financial institutions.[20] Vietnam is most known for threats related to e-commerce, and the United States of America (a more recent trend) for financial crimes.[21] In total, 1670 cyber-attacks were carried out in 2019 – an increase of 7.6% from 2018 and 91.2% compared to 2014.[22] Today, cyber-crime is the main cause of attack, while malware is the most used medium.[23]

The overall landscape seems to be heading towards the creation of a new generation of sophisticated criminal cyber-organisations, with larger and more specialised dimensions. These are transformations that will have consequences on traditional organised criminal groups, terrorist groups and activist groups, while the recruitment of freelance cyber-criminals will be replaced by the birth of structured and solid joint ventures, and with the development of internal cyber resources within criminal groups. The greatest risk is posed by the possibility of a significant convergence of criminal interests with a wider exchange of skills and services between these groups.[24] The trends that can be deduced from the current developments of cybercrime shows an increase in more sophisticated and multipurpose attacks, in the number and types of attacks, but also in the number of targets and victims and the related economic damage.

A first trend regards theft and manipulation of sensitive data.[25] Sensitive data is an asset that is increasingly abused by cybercriminals to perpetrate their criminal activities. The increasing digitisation of information and the increase in the collection, processing and storage of data (resulting from the growth of cloud services, hosting, Internet of Things) increases the risk associated with intrusions or identity theft. The abuse of this data ranges from the traditional fraud scheme (of credit cards or bank credentials), to extortion or cyber-

[20] Centre for Strategic and International Studies, 'Significant Cyber Incident' https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents accessed April 2021.
[21] A. Antonielli et al, *Rapporto Clusit 2020: sulla sicurezza ITC in Italia* (CLUSIT 2020).
[22] ibid.
[23] ibid.
[24] CNAIL, supra note 16.
[25] European Union Agency for Cybersecurity, *Physical Manipulation/Damage/Theft/Loss: From January 2019 to April 2020* (ENISA Threat Landscape 2020).

espionage (industrial / government).[26] In addition, 'crime as a service' allows for the purchase of clean data resold in blocks and customised to the needs of the buyer(s). In this context, there is an increase in intrusions within the infrastructures of logistics and transport companies, often perpetrated to facilitate traditional criminal activities. Some analysts further suggest that the increasing introduction of automated systems that are managed remotely will result in more attention being paid to crime and related attempts to use systems for illicit purposes.[27]

A second trend concerns counterfeiting activities.[28] The varied illegal markets on the Surface Web and the Deep Web will lead to the almost exclusive placement of the sale of counterfeit products online, increasingly targeted at the current and future needs of consumers: from toothpastes to detergents, from medicines to vaccines, from medical equipment to professional services in general, there will be more and more counterfeits. This has already resulted in increasingly sophisticated illegal marketplaces, accurate replicas of legal websites to deceive potential buyers.[29]

A third trend includes cryptocurrencies and money laundering.[30] Cryptocurrencies, most prominently Bitcoin, are an expanding payment system caused by a growing number of companies offering e-commerce services and Bitcoin-ATMs. On the one hand, this type of currency exposes those who use it to the risk of having their e-wallets or 'exchanges' (the entities that convert cryptocurrency into 'fiat' currency) violated. On the other hand, it could facilitate criminal activities. The possibility of carrying out monetary exchanges protected by a pseudonym and outside of the controls of traditional financial circuits, creates greater possibilities for the development of illicit trade of material or professional services (including 'crime as a service'), with both online and offline exchanges. In addition, 'niche' cryptocurrencies, unlike traditional ones, offer even greater security and, above all, anonymity, and have proven to be even more efficient in covering up criminal activities.[31]

---

[26] European Union Agency for Cybersecurity, Cyber Espionage: From January 2019 to April 2020 (ENISA Threat Landscape 2020).
[27] J.B. Hill, N.E. Marion, *Introduction to Cybercrime* (Praeger 2016).
[28] Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA [2019] OJ L123/18.
[29] CNAIL, supra note 16.
[30] R. Houben, A. Snyers, *Cryptocurrencies and Blockchain: Legal context and implications for financial crime, money laundering and tax evasion*, (European Parliament 2018).
[31] M-H Maras, *Computer Forensics* (Jones & Bartlett 2014).

The growing specialisation of cybercriminals goes hand in hand with the creation of a network of increasingly differentiated and personalised services for criminal activities by actors without specific IT skills.[32] For example, it has become comparatively easy to not only acquire (for sale or rent) packages of malware, especially banking Trojans and Zero-day exploits, but also receive tutorials and online advice for their implementation at a reasonable price: in 2013, exploit kits cost between $1,000 and $2,000, and could be rented for $200 to $600 per week or $600 to $1,200 per month. It is also possible to access Botnet to facilitate the implementation of distributed 'Denial of Service' attacks aimed at compromising the functionality of different types of online services (banking, e-commerce, etc.).[33] Botnets can also be used to send spam and phishing emails, or to anonymise attacks and fraud on the web.[34]

These trends underline the objectives of recent cyber threats, especially if considering developments in ICT, namely the 'Internet of Things', the 'Internet of Everything' and 'Bring Your Own Device' (BYOD). Due to these, more and more people will be connected to the network of their companies or institutions, making the systems more prone to large-scale attacks. For example, combinations of malware that can infect computers and mobile devices are spreading as a result of the increasing use of smartphones to authenticate online services. Similarly, fake apps, service applications, games, etc., which contain misleading malware, are becoming more and more widespread.[35]

Legal Shortcomings

The development of international space law dates back to the late 1950s. Even before the Sputnik satellite was launched on 4 October 1957, the entire international community worried about the results of a possible expansion of the rivalry between superpowers in outer space. They expressed the idea that space constituted a dimension beyond the sovereignty of states, not susceptible to appropriation, where terrestrial rivalries could not be translated: a *res communis* characterised by a substantial freedom of passage,

---

[32] SIMARGL, *"Nexus of Cyberspace Actors" in Work Package 3: Legal, Social Sciences and Humanities Aspects of the SIMARGL Toolkit to Detect and Counter Malware and Stegomalware* (European Commission 2019).
[33] Supra note 30.
[34] European Union Agency for Cybersecurity, 'Botnets', https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/botnets accessed April 2021.
[35] U. Kohl, A. Charlesworth, *Information Technology Law* (Routledge 2016).

similarly to what is established for the high seas.[36] While involving the overflight of the territory of numerous states, the launch of the first satellite did not cause any protest from the underlying countries, which never claimed their sovereignty could extend to the space covered by the satellite's orbits. The passage into space therefore appeared free from the first moment as long as it was conducted 'for peaceful purposes'.[37] Between 1958 and today, space was the subject of several resolutions by the United Nations General Assembly. During the XIII session of the UN General Assembly (UNGA), on 13 December 1958, 'questions on the peaceful use of Outer Space' were discussed: during the debate, almost all states used the term 'peaceful' as opposed to 'military'.[38] The General Assembly, underlining the innovative nature of activities in space, stigmatised the need for international cooperation so that the exploration and use of space were preserved "solely for peaceful purposes."[39] For this purpose, the UNGA established a Committee on Peaceful Uses of Outer Space (COPUOS),[40] a political body further composed of two sub-committees: scientific and legal. The mandate of COPUOS is to promote international cooperation in space and develop its regulations through a series of recommendations for the consideration of the UNGA.[41] Following, UNGA Resolution 1472 (XIV) of 13 December 1959 introduced the principle that the peaceful use of space and its exploration should be directed for the sake of humanity and the progress of all states.[42] To complement that, UNGA Resolution 1721 A (XVI), adopted unanimously by the General Assembly in 1961, established that Outer Space and celestial bodies are open to the exploration and to the use of all states, in accordance with international law, and are not subject to national appropriation.[43] These resolutions have been the first legal documents addressing outer space and have defined a regulatory framework based on programmatic principles expressing the desire to maintain international peace and security, but deliberately leaving the normative content to be attributed to each of these terms undefined.[44] It was believed

[36] P.M. Martin *Droit des Activités Spatiales* (Masson 1992).
[37] F. Francioni, F. Pocar, *Il regime Internazionale dello Spazio* (Giuffré 1993).
[38] Institute of Air and Space Law, *Air and Space Law* (vol. XL 2015).
[39] M. Cervino, B. Corradini, S. Davolio "Is the 'Peaceful Use' of Outer Space Being Ruled Out?", 19 Space Policy 231-237.
[40] UNGA Res 1348 (XIII), (13 December 1958)
[41] Sergio Marchisio,) "Il ruolo del Comitato delle Nazioni Unite sugli usi pacifici dello spazio extra-atmosferico (Copuos)" in P.A. Pillitu (ed) *Scritti in onore di Giorgio Badiali*, (Aracne 2007).
[42] UNGA Res 1472 (XIV) (13 December 1959).
[43] UNGA Res 1721 (XVI) (20 December 1961).
[44] M. Gestri, "Portata e limiti del principio dell'uso pacifico nel diritto dello spazio", in F. Francioni, F. Pocar (eds) "Il regime internazionale dello spazio" (Giuffré 1993).

that they could be specified later, taking into account political and technological developments.

On 10 October 1967, the "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies", also known as the Outer Space Treaty,[45] entered into force providing the foundational basis of international space law. This treaty regulates the exploration and use of the space domain, including the moon and other celestial bodies, by states. The treaty notes that space is free to be explored by all states and is not subject to national claims of sovereignty.[46] It prohibits the deployment of nuclear weapons in space,[47] although strategic and geopolitical competition has always been a driving force for space exploration. It should be noted that the treaty does not place a legal ban on the placement of conventional weapons in space, and anti-satellite weapons have been successfully tested by the United States, USSR and China.[48] The treaty was approved by the UNGA in 1963 and signed in 1967 in the USSR, United States and the United Kingdom. As of June 2020, 110 countries are parties to the treaty, while another 23 signed the treaty but did not ratify it.[49] Four other treaties have been negotiated and drafted by the United Nations Commission on the Peaceful Use of Outer Space, namely the 1968 Astronaut Rescue Agreement[50], the 1972 Space Liability Convention (LIAB),[51] the 1975 Convention on registration of objects launched into space[52] and the 1979 Treaty on the Moon.[53] As briefly showed, the current framework regulating human activity in outer space dates back to a historical period in which the concept and use of space itself was different from that of today. This makes this framework less adequate to regulate and protect cyberspace activities,

[45] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, entered into force 10 October 1967, 610 U.N.T.S. 205 (hereinafter referred to as "OST").
[46] ibid Article I.
[47] Ibid Article IV.
[48] Supra note 12.
[49] ibid.
[50] Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space (entered into force 3 December 1968) 672 U.N.T.S. 119 (hereinafter referred to as "Rescue Agreement").
[51] Convention on International Liability for Damage Caused by Space Objects (entered into force 9 October 1973, 961 U.N.T.S. 187 (hereinafter referred to as "LIAB").
[52] Convention on Registration of Objects Launched into Outer Space (entered into force 15 September 1976) 1023 U.N.T.S. 15 (hereafter referred to as "Registration Convention").
[53] Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (entered into force 11 July 1984) 1363 U.N.T.S. 3 (hereinafter referred to as "Moon Treaty").

requiring an increasingly urgent update and integration with the strategic and economic issues at stake.

From a strategic-military point of view, space proves to be a vital sector for defence and security, the importance of which is becoming increasingly clear for many countries. Faced with an ever less distant and increasingly indispensable space for citizens' lives, the European institutions have recognised its importance in supporting their policies, for industrial, economic and political reasons, and for security and defence purposes.[54] The recognition of the duality of EU-ESA cooperation programmes has even led to the assumption of a different interpretation of the latter's mandate, in a sense more suited to the expansion of intrinsically dual-space products.[55] Following the innovations introduced by the Lisbon Treaty,[56] which attributes explicit competence to the Union in Space matters, albeit in accordance with its own Member States, an architecture of relations between the two international organisations has also been established, consolidating their independence and specifying the terms of their partnership.[57] This does not, however, exclude the possibility that their relationship may not evolve towards greater integration in the future. From a strictly political-diplomatic and strategic perspective, space appears as a stage for relations between states and an economic, political, military and cultural centre of gravity, in which a growing number of players are making their way. The space dominance of the United States therefore seems to be threatened on the one hand by the expansion of Russian and European Space activities, and on the other by the growth of space activities in emerging countries. These are determined to use their political-diplomatic and symbolic potential and acquire technologies capable of accelerating their economic development. Among these, China poses a particular challenge, due to a lack of transparency and reliability, especially following the anti-satellite test of 2007, and the lack of separation between its civil and military space activities.[58]

---

[54] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions EU Space Industrial Policy Releasing the Potential for Economic Growth in the Space Sector, COM/2013/0108.
[55] European Commission, 'EU funding for Dual Use: Guide for Regions and SMEs' (Enterprise and Industry 2014).
[56] EU Treaty (Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community).
[57] ibid.
[58] Supra note 12.

These aspects underline a series of shortcomings in the current regulation of space activities when integrated with cyber operations. One of them concerns the risks of an uncontrolled transfer of technology. Establishing a framework for the export of space products and technologies is particularly critical and, in some cases, may require a sacrifice of commercial interests for the benefit of states' national security. At the same time, it is important to establish a balanced framework. As demonstrated by the case of the United States International Traffic in Arms Regulation (ITAR),[59] which is currently under review, where too strict frameworks may pose significant obstacles to the transfer of technology between countries cooperating on space projects. Further shortcomings affecting the suitability of international space law to regulate and address cyber-threats are the notions of damage, space object and space activities. Under Article VII OST, damage caused by a space-object triggers international liability: "each State Party from whose territory or facility an object is launched is internationally liable for damage to another State Party to the Treaty."[60] According to LIAB, damage means the "loss of life, personal injury or other impairment of health; or loss of or damage to property of States or of persons, natural or juridical, or property of international intergovernmental organizations".[61] The question is therefore whether electronic damage, impeding the correct functioning of a given space infrastructure, qualifies as compensable damage under international space law. Further to that, to be compensated, damage needs to be caused by a space object.[62] The LIAB defines this term as including "component parts of a space object as well as its launch vehicle and parts thereof".[63] Therefore, the question is whether electronic communications constitute or not 'component parts' of Internet of Things satellites. Lastly, the lack of a definition of space-activities raises the question whether the use of satellites for malicious cyber operations qualifies as illegal use of space in breach of Articles I, III, IV and IX of OST.

In addition to this, both cyber and space normative systems are also addressed in general public law, as well as in various domestic legal frameworks.[64] In this complex multi-level context, and in light of the rapid evolution of cyber and space activities, developing precise laws and policies

[59] 22 CFR §§121-130.
[60] Article VII OST, supra note 5.
[61] Article I LIAB, supra note 51.
[62] ibid.
[63] ibid.
[64] A. Carlo, 'Cyber Threats to Space Communications: Space and Cyberspace Policies' in *Outer Space and Cyber Space: Similarities, Interrelations and Legal Perspectives* (Springer & European Space Policy Institute 2021).

that would perfectly address all the relevant issues may very well be a vain attempt. Hence, the abovementioned shortcomings could be addressed through evolutionary interpretation of general principles and international harmonisation of policies.

Policy Approaches

For NATO, cyber challenges play an increasingly critical role, as an alliance is 'only as strong as its weakest link', especially in the cyber space and on policy areas that require a high degree of cooperation and communication. In recent years, the number of actors involved in cyberattacks has increased. Identifying the perpetrator and/or the victim of the attack is essential and international cooperation is required. In the space sector, and particularly for projects related to the development of observation capabilities, two actors cooperating internationally are of particular note: France, through the Centre national d'études spatiales (CNES), and more recently Italy, through the Agenzia Spaziale Italiana (ASI).[65] The signing of the first agreement[66] with the European Space Agency (ESA) is also recent, which opens up cooperation on space technology in areas such as astrophysics, satellite engineering, environmental monitoring, the prevention of natural disasters, and telecommunications. Last but not least, there is the question of the use and security of the management information systems of all related tools. In 2019, ESA launched the 'Funding & support of Space-based services for cyber security' project, aimed at companies that develop innovative products and services in the ITC field. In particular, the project focuses on initiatives, based on satellites that can mitigate the risks to cyber security and increase the resilience of existing services, infrastructures and operations.[67] In addition, products are sought that improve end-to-end cyber security of space-based applications. The key areas of the project "are transport (sea, land and air, including autonomous vehicles); energy, utilities and critical infrastructures; finances and, public safety".[68]

---

[65] Agenzia Spaziale Italiana "Galileo: il nuovo programma europeo di navigazione in Mediaplanet, Space" Il Sole 24 ore, 3.

[66] European Commission and European Space Agency sign agreement to support innovation in the space sector, https://ec.europa.eu/growth/news/european-commission-and-european-space-agency-sign-agreement-support-innovation-space-sector_en accessed April 2021.

[67] ESA, "Funding & support of Space-based services for cyber security", in Business Applications (2019).

[68] F. Bussoletti, "Spazio: ESA guarda alle aziende per migliorare la cyber security", in Difesa & Sicurezza (2019).

In the past decade, the United States has developed various strategy documents covering the improvement of cybersecurity in the space domain, including the 2017 National Security Strategy,[69] 2018 National Cyber Strategy,[70] Space Policy Directive-3,[71] and Space Policy Directive-5 (SPD-5).[72] The latter directive is the most relevant, as it promotes the development of a government framework that incorporates cybersecurity into all phases of space systems.[73] This directive aims to increase cyber protections for critical space infrastructure. The SPD-5 requests space operators to consider developing a culture of prevention, active defence, and sharing of best practices. This is done by "safeguarding command, control, and telemetry links using effective and validated authentication or encryption measures" and by adopting cybersecurity "hygiene practices, physical security for automated information systems, and intrusion detection methodologies".[74] Moreover, SPD-5 encourages operators to share information, best practices and analysis through the Space Information Sharing and Analysis Centre (S-ISAC).[75]

The sharing of best practices and unique know-how to prevent, strengthen, and reconstruct a system following a cyber-event can only be achieved through strong national and international cooperation. To guarantee strong and efficient sharing of information, ISACs have been established to make data on cyber threats and events, as well as best practices to counter them, more accessible internationally. In this sense, ISACs provide a central resource for gathering information on cyber threats and events related to critical infrastructure.[76] Leveraging on this role of ISACs, constant monitoring of the activities and risk assessment may lead to the reduction of such events. Strong cooperation between different international organisations is fundamental to build a resilient cyber and space

[69] United States, "National Security Strategy of the United States of America" (The White House 2017).
[70] United States, "National Cyber Strategy of the United States if America" (The White House 2018).
[71] United States, "Space Policy Directive-3, National Space Traffic Management Policy" (The White House 2018).
[72] United States, "Space Policy Directive-5, Cybersecurity Policy for Space Systems" (The White House 2020).
[73] ibid.
[74] Executive Office of the President, (2020) Space Policy Directive-5: Cybersecurity Principles for Space Systems, FR Doc. 2020-20150.
[75] Supra note 11.
[76] ITU, "Guide to developing a National Cybersecurity strategy. Strategic Engagement in Cybersecurity" (Geneve 2018).

infrastructure.[77] In 2003, the European Union (EU) and NATO signed the Berlin Plus Agreement[78], which allows for the EU to use NATO forces if and when necessary. Based on the same principle of cooperation, in 2016, the EU and NATO signed a Technical Arrangement to facilitate technical info-sharing between the European CERT and the NATO Computer Incident Response Capability.[79] Currently, the NATO Cooperative Cyber Defence Centre of Excellence[80] is liaising with the European Defence Agency by exchanging information on common topics of concern.

In 2020, the UK proposed a draft UN resolution calling for a "global discussion on what would constitute responsible behaviour in space"[81] following wide-ranging consultations with international actors. As Foreign Secretary Dominic Raab stated, "a new approach is urgently needed to increase trust and confidence between countries operating in space to prevent an arms race or a conflict that could have catastrophic consequences".[82] To construct a strong and resilient system, public and private cooperation, cyber diplomacy, as well as the establishment of CERTs and SOCs that monitor and organise cyber operations, are essential.

Conclusion

Current satellite capabilities allow the management of ever greater portions of civilian and military critical infrastructure management systems through IT systems. However, computer systems are susceptible to attacks by cybercriminals (individual or organised) at national and, especially, transnational level, which requires the coordination of actions against such criminals. In addition, distinguishing 'non-military' from 'military' roles has become more challenging in the cyber and space domains, as many dual-use technologies can be used for both civil and military purposes.[83] This makes it

---

[77] B. Boutros-Ghali, "International Cooperation in Space for Security Enhancement" (10 Space Policy 265-276).
[78] EU-NATO Berlin Plus Agreement, 16 December 2002. https://www.nato.int/cps/en/natolive/official_texts_19544.htm accessed April 2021.
[79] NATO, 'NATO and the European Union enhance cyber defence cooperation' (10 February 2016) https://www.nato.int/cps/en/natohq/news_127836.htm accessed April 2021.
[80] P. Meyer, "Outer Space and Cyberspace. A tale of Two Security Realms", in Osula A.M, Roigas H (eds), *International Cyber Norms: Legal, Policy & Industries Perspectives*, Tallinn, NATO CCD-COE, 115-169.
[81] UK 'UK push for landmark UN resolution to agree responsible behaviour in space' (26 August 2020) https://www.gov.uk/government/news/uk-push-for-landmark-un-resolution-to-agree-responsible-behaviour-in-space accessed April 2021.
[82] ibid.
[83] Caroline Baylon, 'Challenges at the Intersection of Cyber Security and Space Security' in

more difficult to define key terminology, contributing to a lack and inadequacy of internationally agreed definitions. In turn, this lack has impeded the development of multilateral arms control agreements and has discouraged cooperation, fostering an "ambiguity of intent" and adding to the cycle of escalation.[84] Dual-use technologies also mean that a complete ban on certain technologies and the implementation of adequate measures to verify compliance are often impractical. This further adds to existing difficulties in reaching arms control agreements. Moreover, due to this dual-use aspect, it has become more challenging to determine whether a country engages in military activities beyond its civilian programme. As Caroline Baylon states, this "has a direct impact on ambiguity of intent surrounding countries' actions and thus further stimulates the escalatory cycle".[85]

As a matter of security, the regulation of space and cyber always requires a strong involvement of states seeking autonomy and strategic independence. This need for independence is by all means a new 'stake' in international relations, insofar as it represents an attribute of power and is the subject of negotiation. This is exemplified by Europe's path towards the acquisition of independent access to space and of an autonomous satellite navigation system. Here, too, some questions still remain unanswered. It remains to be clarified what use should be made of Galileo's encrypted positioning signal, how the 2004 Agreement for compatibility with GPS[86] will be implemented, and how to solve the problem of overlapping frequencies with the Chinese Beidou system. As for access to space, it will be necessary to understand how to face the increasingly aggressive competition in the international launcher market, and how to ensure the effectiveness of the liability discipline.

In this context, there are two particularly pressing issues that should be addressed immediately: the verification and implementation of the assets that are adopted in this area, and the implementation of the current perspectives for coordinating the cybersecurity policies of satellite communication systems. Both space and cyber activities have their own national and international regulatory framework which, although often lacking with respect to the demands that gradually arise and poorly integrated into the international arena, forms the basis for desirable future developments. What is missing is the

Country and International Institution Perspectives (Chatham House 2014).

[84] ibid. p.8

[85] ibid. p.10

[86] Agreement on the Promotion, Provision and Use of Galileo and GPS Satellite-Based Navigation Systems and Related Applications [2011] OJ L348/3.

overall vision: a formal coordination between the two areas in terms of policies and assets that has not yet been achieved. A first step in this direction can be seen in the UK draft proposal to the UN on responsible behaviour in space. This has created a new movement to develop more responsible and sustainable space international policies. However, international cooperation is only as strong as the need to exchange and share particular benefits. This cooperation is put at risk with many private businesses entering the space market, creating competition that may ultimately result in less cooperation between state actors. Analysts and specialists in their respective fields and in international politics have highlighted the interconnections between space and IT activities, finding various replies in national programmatic documents and guidelines, but not in a univocal nor uniform and coordinated way among the global players. Therefore, the development of close relationship between space and cyber policies and diplomacy emerges as necessary tool to preserve and strengthen their continuing relevance in the future.[87]

***

[87] Attila Mesterhazy, NATO-*EU Cooperation after Warsaw*, (NATO Parliamentary Assembly, Defence and Security Committee Report 2017).

Source: www.nato.int

The threat of cyber-attacks to space-based assets affecting NATO's communications and weapons systems[1]

by Paula Raboso Pantoja[2] and Rodrigo Vazquez Benitez[3]

1. Introduction

Since Sputnik's first launch, space-based assets have become an essential part of military operations, to the extent of becoming indispensable to a missions' success. Space has enabled communication capabilities, intelligence collection, navigation through gathering of global positioning data and environment supervision, among other enterprises.[4] With the

[1] **DISCLAIMER**: The views expressed in this article are solely those of the authors and may not necessarily represent the views of NATO, Allied Command Operations, or Allied Command Transformation, or of their affiliated organizations.

[2] MA in International Peace and Security, King's College London War Department; Intern at the ACO Office of Legal Affairs at the NATO Supreme Headquarters Allied Powers Europe.*

[3] Assistant Legal Advisor at the ACO Office of Legal Affairs of the NATO Supreme Headquarters Allied Powers Europe.*

[4] Beyza Unal, 'Cybersecurity of NATO's Space-based Strategic Assets,' (Chatham House 2019)

establishment of satellites, the military is able to communicate over extended distances, determine the exact location of their personnel and be on the receiving end of space-based intelligence in the form of meteorological data and weapons warning systems.

However, this data is provided through field-based, 'computer-operated information' structures, in other words, cyber capabilities.[5] The space domain should be differentiated from traditional arenas such as land, air and sea, due to its natural connection to cyberspace. Computerized networks, and digital elements such as software and hardware, act as intermediaries between the receiving operational end and space-based intelligence. It is an intrinsic relationship that enables the utilization of space-based assets for military purposes. Furthermore, it is an environment where the classical concept of terrestrial borders does not apply, while sovereignty is still expected to be honoured. This in and off itself alters the context and thus the notion of "warfare".[6] In this sense, the realms of cyber and outer space may engage different dimensions of warfare and different versions of conflict that we need to be prepared for.

Space-based assets' crucial dependency on cyber means has resulted in new cyber menaces, affecting missions' success, and having a deep operational impact for military organisations such as the North Atlantic Treaty Organization (NATO). NATO's operations are managed through land, sea, air and cyber domains, for which space-based structures are essential to obtaining information and services. It is therefore of utmost importance for NATO to ensure a risk-free cyber environment that enables secure functioning of space systems.

The correlation between cyberspace and space is often overlooked, particularly by international treaties and legislation and not managed properly, leaving space-based assets' vulnerabilities open to external cyber threats. In that sense, the following paper will consider how cyber threats to space infrastructure affect NATO's military capabilities, especially its communications and weapons systems. Additionally, it will focus on analysing the existing legal framework linking cyber-attacks to space law and assessing the possibility of

---

https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf accessed 28 April 2021.

[5] Jerry Drew, 'Space, Cyber and Changing Notions of War,' (*Small Wars Journal*, August 2017) https://smallwarsjournal.com/jrnl/art/space-cyber-and-changing-notions-of-war accessed 28 April 2021.

[6] Ibid.

using international law to provide outer space assets with cybersecurity. Thus, the purpose of this article is to determine ramifications of space-based assets' exposure to cyber-attacks and set forth the need for effective space legislation in order to prevent third parties from eluding or even bending international law in outer space to its will.

2. Cyber threats to Space-based assets

As mentioned above, NATO's strategic military capabilities depend on space-based structures for the transmission of information and different services, ranging from communications, intelligence, surveillance and reconnaissance (ISR), global positioning system (GPS), missile detection, space situational awareness (SSA), environmental supervision, as well as positioning, navigation and timing (PNT).[7] In relation to NATO weapons systems, space-based assets enable operational effectiveness of missile defence systems and precision-guided weapons through precision targeting and tracking data.[8] The majority of these systems are connected to each other, some relying on satellites and others on other technological devices. Thus, influencing one capability may trigger ramifications for others. Simultaneously, space-based architectures, on which all these systems depend, are conveyed through cyberspace, placing an immeasurable responsibility of assuring mission effectiveness and success on the functionality of cyberspace infrastructure.[9]

Nonetheless, there might be those who wonder why focus should be shifted from traditional safeguards against kinetic attacks in space systems to cyber protection. The clearest answer is, the approach should not be shifted, but expanded. The liaison between space and cyberspace facilitates less sophisticated attack strategies. Sufficient hacking knowledge, target identification and access to the Internet is often enough to process an attack against a space asset, enabling a large number of malefactors to proceed

---

[7] Liina Lumiste, 'Chatham House report: Space – NATO cyber security's weak spot,' (*Chatham House*, 2019) https://ccdcoe.org/library/publications/chatham-house-report-space-nato-cyber-securitys-weak-spot/ accessed 1 February 2020.

[8] Commission on the Roles and Capabilities of the United States Intelligence Community, 'Space Reconnaissance and the Management of Technical Cooperation,' Federation of American Scientists, *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*, (1996) https://irp.fas.org/offdocs/int015.html accessed 28 April 2021.

[9] John E. Hyten, 'Presentation to the House Armed Services Committee Subcommittee on Strategic Forces,' (25 March 2015) 4, https://docs.house.gov/meetings/AS/AS29/20150325/103106/HHRG-114-AS29-Wstate-HytenUSAFJ-20150325.pdf accessed 28 April 2021.

with such endeavours.[10] Cyber weapons ease the difficulty of locating and reaching remote targets, such as satellites, as they do not require the manufacture and use of advanced anti-satellite precision weapons to obstruct space-based architectures. Compared to conventional weapons, cyber capabilities render satellites accessible to anyone with reasonable coding capabilities and access to the Internet, not needing to permeate defended air spaces. Moreover, cyber weapons and electronic warfare (EW) are usually easier, cheaper and often faster alternatives than traditional kinetic weapons. Counter-space operations based on the latter imply lengthy, expensive programs of visible development, of easy sighting for potential adversaries.[11] Additionally, cyber-attacks come with attribution problems, and are often ambiguous and more arduous to unearth, trace and ascribe in an assured manner, hampering responsive actions. Finally, cyber capabilities are by far the most flexible counter-space assets, as they provide an enemy with a full range of different reversible and non-reversible effects, ranging from alteration, theft, espionage, obstruction, denial of data, to destruction of essential infrastructure elements or even the satellite itself.[12] No other set of capabilities is simultaneously capable of compromising and altering information, accomplishing surveillance tasks and effecting reliable kinetic repercussions of varying sternness.[13]

Cyber-attacks directed at space-based structures are therefore popular belligerent options, often chosen by state and non-state actors alike, especially as they are not fully regulated, or not in a clear-cut manner or in sufficient detail, by international law. Recently, China expressed its desire to establish offensive cyberspace methods as a key element for military space-based operations support.[14] In the same vein, Russia has favoured cyber methods as

---

[10] Eric Sterner and Jennifer McArdle, 'Cyber Threats in the Space Domain,' (2016) 15 The American Foreign Policy Council, Defense Technology Program Brief 4 https://www.afpc.org/uploads/documents/Defense%20Brief%20Issue%2015.pdf accessed 28 April 2021.

[11] Brian Weeden and Victoria Samson, 'Global Counterspace Capabilities: An Open Source Assessment,' (*Secure World Foundation*, April 2018) 7-12, https://swfound.org/media/206118/swf_global_counterspace_april2018.pdf accessed 28 April 2021.

[12] Danny Palmer, 'Cyberwarfare in space: Satellites at risk of hacker attacks,' (*ZD Net*, 2019) 9 https://www.zdnet.com/article/cyberwarfare-in-space-satellites-at-risk-of-hacker-attacks/ accessed 28 April 2021.

[13] Weeden and Samson, 'Global Counterspace Capabilities,' 7-11 (n 11).

[14] Office of the Secretary of Defense, 'Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2018,' (2018) 40-41 https://media.defense.gov/2018/Aug/16/2001955282/-1/-1/1/2018-CHINA-MILITARY-POWER-

a means to weaponise information in counter-space operations.[15] In general, cyber-attacks as counter-space measures tend to be more attractive to warring parties as the obstruction of a satellite is always preferable to its physical destruction and consequent debris generation. Consequently, non-kinetic counter-space capabilities are gaining momentum in China and Russia's militaries, two countries highly experienced in waging warfare through hybrid means, a relatively low cost alternative to traditional mechanisms.[16]

3. Types of threats

Space assets can be divided in three fundamental sections: firstly, space components, namely satellites; secondly, ground-based infrastructure that holds space systems, such as end-users, control systems, terminals and ground stations; and finally, the linkages among them. Each of these sections can be a potential target of offensive cyber activities.[17] Such offensive cyber activities can be varied in objectives and consequent effects. They may involve the usage of hidden 'back doors' in purchased software packages, enabling a secure access for future cyber activities, as found in Chinese and Russian electronics acquired by United States' (US) aerospace enterprises.[18] They may also involve man-in-the-middle (MITM) offensive cyber activities, consisting of belligerent activities towards the connection between satellites and their controlling ground stations through the interpolation between the sending and receiving end. This action enables the attacker to filter all passing information and modify it at his or her will.[19] Additionally, one could encounter pernicious GPS signals, which, when attempting to decode, impregnate the equipment

REPORT.PDF accessed 28 April 2021.

[15] Defense Intelligence Agency, "Russia Military Power: Building a Military to Support Great Power Aspirations," 2017, 35, https://www.hsdl.org/?view&did=801968 accessed 28 April 2021.

[16] Paul Ferrillo and Chuck Brooks, 'Protecting Space-Based Assets from Cyber Threats,' *(Homeland Security Today*, 17 October 2020) https://www.hstoday.us/subject-matter-areas/infrastructure-security/protecting-space-based-assets-from-cyber-threats/ accessed 28 April 2021.

[17] Sterner and McArdle, 'Cyber Threats in the Space Domain,' 3 (n 10).

[18] Steven Musil, 'Experts Dispute Threat Posed by Backdoor Found in Chinese Chip,' (*CNET*, 29 May 2012) https://www.cnet.com/tech/services-and-software/experts-dispute-threat-posed-by-backdoor-found-in-chinese-chip/ ; Gordon Lubold and Shane Harris, 'Russian Hackers Stole NSA Data on U.S. Cyber Defense,' *The Wall Street Journal*, (New York, 5 October, 2017) https://www.wsj.com/articles/russian-hackers-stole-nsa-data-on-u-s-cyber-defense-1507222108 accessed .

[19] Adam Ali.Zare Hudaib, 'Satellite Network Hacking & Security Analysis,' (2016) 10 International Journal of Computer Science and Security, Issue 1, 48 https://www.cscjournals.org/library/manuscriptinfo.php?mc=IJCSS-1200 accessed 28 April 2021.

with malware, forcing it into a constant 'reboot loop' and resulting in a temporary denial of the device's utility and service. This action could potentially cause denying an enemy's PNT systems, rendering its operation futile.[20]

All in all, cyber-attacks directed at space-based assets tend to take the form of four further offensive cyber activities, namely, deception, disruption, degradation and, ultimately, destruction.[21] A deceitful attack usually involves misleading measures that alter, falsify and manipulate information to cause the desired detrimental adversary's behaviour. Such attacks include GPS signal spoofing, a method that inserts false data in the GPS signal, deceitfully leading users to believe the GPS works as intended, thus, not breaking the user's trust in the device and causing them to follow the malicious information blindly.[22] By disrupting space systems, one temporarily compromises a service, delaying the access to crucial and perishable information to a potential adversary. Finally, by degrading or destroying space structures through attacks on its ground-based stations, terminals and linkages, one seeks to permanently impair, partially or completely, the device's service and utility. These 'soft-kill' actions disable space-based assets without further debris generation.[23]

In sum, cyber threats to space-based assets range from malicious deceitful actions to physical damage, both of which could potentially disable a satellite's utility permanently. In relation to NATO, one cannot help but notice that a few keyboard clicks on a computer have the potential to subdue NATO's and the Allies' military capabilities, communications and weapons systems.

4. International Law

[20] Weeden and Samson, 'Global Counterspace Capabilities,' 7-6 (n 11).
[21] Sterner and McArdle, 'Cyber Threats in the Space Domain,' 3 (n 10).
[22] Gregory Falco, 'Job One for Space Force: Space Asset Cybersecurity,' (*Harvard Kennedy School, Belfer Center for Science and International Affairs*, July 2018) 8 https://www.belfercenter.org/sites/default/files/files/publication/CSP%20Falco%20Space%20Asset%20-%20FINAL.pdf accessed 29 April 2021; James K. Sanborn, 'Drone Aircraft Vulnerable to Disruptive GPS "Spoofing" Technique,' *Space News*, 16 July 2012 https://spacenews.com/drone-aircraft-vulnerable-disruptive-gps-spoofing-technique/ accessed 29 April 2021.
[23] John Grady, 'U.S. Dependence on Space Assets Could be a Liability in a Conflict with China,' *USNI News,* 29 January 2014 https://news.usni.org/2014/01/29/u-s-dependence-space-assets-liability-conflict-china accessed 29 April 2021.

While the current threat of cyber-attacks to space-based architectures is clear to NATO, evidenced by its decision to declare cyber and outer space as the fourth and fifth operational military domains,[24] international law seems to have missed the connection. Despite the existence of different international legal instruments and (draft) manuals[25] on the international law applicable to military uses of cyber and outer space, these conventions and soft-law publications focus on each domain separately, not addressing their inevitable connection.

Despite recent initiatives, such as the Outer Space Treaty (OST) and the draft Manual on International Law Applicable to Military Uses of Outer Space, international law on Outer Space has not evolved much since its development in the late sixties and early seventies.[26] The task of creating this body of law was undertaken by the United Nations Committee on the Peaceful Use of Outer Space, who fostered the conclusion of the five multilateral treaties that regulate this domain. Among the five UN treaties on space, the OST, introduced in 1967, is perhaps the most important. It created and codified a set of basic principles aiming to limit the use of outer space as a battleground in armed conflict. Perhaps the most important principle agreed to in the OST is that outer space may only be used for peaceful purposes.[27]

However, drawing a parallel with the UN Convention on the Law of the Sea (UNCLOS) regulation of the high seas,[28] it is now generally accepted that 'peaceful use' does not mean 'exclusively civilian use'. For instance, intelligence, surveillance and reconnaissance (ISR) activities, or the use of space for self-defence, may be regarded as military activities compatible with a 'peaceful use' of space. Moreover, the treaty imposes the need to carry out activities in outer space in accordance with international law, which brings into

---

[24] Bradley Bowman and Andrew Gabel, 'NATO declares space "operational domain," but more work remains," (*DefenseNews*, 16 December 2019) https://www.defensenews.com/opinion/commentary/2019/12/16/nato-declares-space-operational-domain-but-more-work-remains/ accessed 29 April 2021.

[25] Michael N. Schmitt (Ed.), 'Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations' (CUP 2017); 'Manual on International Law Applicable to Military Uses of Outer Space', a McGill Project; and others.

[26] Setsuko Aoki, 'Law and military uses of outer space,' in Ram S. Jakhu, Paul Dempsey (eds), *Routledge Handbook of Space Law* (Routledge 2016).

[27] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies (27 January 1967) 610 UNTS 205 (Outer Space Treaty), Art. 3.

[28] See United Nations Convention on the Law of the Sea, (10 December 1983) 1833 UNTS 397 (UNCLOS), Article 88: "The high seas shall be reserved for peaceful purposes".

the equation the basic principles of the law of armed conflict. In short, military use of outer space is recognised as a legitimate activity as long as it is conducted in accordance with international law.[29] Nevertheless, the question remains 'what precisely this entails' regarding military activities.[30]

For instance, while the OST forbids the placement of weapons of mass destruction (WMD) in space, it does not account for other types of weapons, suggesting that non-WMD systems in outer space do not violate international law. At the same time, the treaty introduced the norm of the peaceful use of celestial bodies, but not of space as a whole (or of 'void space'), leaving the debate open as to the opportunity for belligerent actions to be carried out in this domain.[31] Therefore, offensive actions, pertinent to the cyber domain, are not regulated by the OST, as cyber means are not recognised as weapon systems in the first place. In conclusion, the OST not only includes vague concepts, allowing broad interpretations, but it also leaves many clear paths to carry out military activities throughout space.

Regarding the regulation of cyberspace, there is no current, legally binding international treaty or legislation fully dedicated to this arena. There are only a few conventions which briefly mention cyber activities and only in relation to children's rights and criminal conduct, leaving cyber-attacks unaddressed. The Tallinn Manual, published in 2013, and the Tallinn Manual 2.0 of 2017, are the most comprehensive -- yet non-legally-binding -- documents to successfully focus on the governance of cyberspace and the use of force from the optics of international law.

Moreover, while the Tallinn manual arrived at the conclusion that cyber operations fall below the use of force threshold and in some cases do not contravene the concept of non-intervention, it established pertinent statements on the notion of cyber-attacks. According to the Tallinn Manual, a cyber-attack constitutes the act of using force whenever its ramifications are equivalent to non-cyber-attacks that amount 'to the level of use of force.'[32]

---

[29] See Aoki, 'Law and military uses of outer space,' (n 25).
[30] Cassandra Steer, 'Global Commons, Cosmic Commons: Implications of Military and Security Uses of Outer Space,' (Winter/Spring 2017) 18 Georgetown Journal of International Affairs 13, https://georgetownjournal-internationa-4d3r.squarespace.com/online-edition/tag/technology .
[31] "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space," 610 UNTS 205.
[32] Michael Schmitt (ed.), 'Tallinn Manual on the International Law applicable to Cyber Warfare,' (Cambridge University Press, 2013), Rule II.

That is to say, according to the Tallinn Manual, a cyber-attack whose scale and effect is equivalent to an armed attack is forbidden under article 2(4) of the United Nations (UN) Charter.[33] However, the manual does not attend to the aspect of soft kill cyber-attacks that could invalidate satellites and, thus, a country or NATO's military operations. Hence, leaving certain offensive cyber means, once again, arguably unaddressed.

At a regional/national level, the European Union adopted the 'Directive on Security of Network and Information Systems,'[34] and the US adopted the 'Internet of Things Cybersecurity Improvement Act.'[35] While they may arguably provide standards of protection against certain types of cyber threats and security breaches, they are markedly insufficient to regulate the full spectrum of cyber threats, and it has not yet been established whether these laws may apply in outer space.[36]

In 2014, China and Russia put forward a draft treaty on the 'Prevention of the Placement of Weapons in Outer Space and the Threat or Use of Force against Outer Space Objects' (PPWT) in the framework of the 'Prevention of an Arms Race in Outer Space' (PAROS) resolution in the UN Conference on Disarmament (CD). The draft treaty firstly defines the notions of 'weapons in outer space,' 'outer space objects' and the 'use of force' and subsequently announces the prohibition of the placement of any weapons and the threat or use of force against 'space objects of state parties.'[37] While, at first a glance, it may seem that the Sino-Russian draft treaty successfully addresses all kinds of offensive activities in space, it appears to carefully leave cyber means out of its definitions.

Correspondingly, the treaty describes space objects as any device placed and designed to operate in outer space.[38] Additionally, it defines space weapons as objects or components engineered to 'eliminate, damage

---

[33] Charter of the United Nations (24 October 1945) 1 UNTS 16 (UN Charter), Article 2(4).
[34] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.
[35] H.R.1668 - Internet of Things Cybersecurity Improvement Act of 2020, on the 14th of December 2019.
[36] Dimitra Stefoudi, 'The Relevance and Applicability of Cybersecurity Laws with Regard to Data Storage on Board Satellites and on the Ground,' (2019) 44 Air and Space Law Issue 4/5.
[37] "Treaty on the Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force against Outer Space Objects (Draft)," (*Ministry of Foreign Affairs of the People's Republic of China*, 16 June 2014) Art. 1, accessed 29 April 2021.
[38] Ibid.

or disrupt' space-based assets. Lastly, it determines the use of force to be an action that inflicts damage to space infrastructures.[39] Conveniently for potential perpetrators, cyber-attacks are usually directed from earth, ergo not originated by a space object in orbit. Consequently, aggressive cyber activities are not considered space objects as such, hence they do not fall within the definition of space weapons, and are thus, not addressed in the above-mentioned treaty.

Furthermore, in order for a perpetrator's offensive intentions to manifest, the elimination, damage or disruption of a satellite is not necessarily implied. In some cases dazzling or jamming space-based assets, meaning obscuring or confusing a country's radar or communications, is enough to compromise a country's military activities. Under the Sino-Russian draft treaty, offensive cyber means do not necessarily constitute weapons nor use of force, and are as so, not foreseeably banned from space. In other words, if a potential perpetrator where to attack a space object through cyber means, its offensive would not be deemed illegal according to the existing international legal instruments.

Hence, there is an urgent need to regulate the potential offensive capabilities of the cyber domain in outer space in order to encounter and restrain aggressive cyber-space warfare scenarios. Cyber means can be both offensive and defensive in nature, with the potential to inflict critical internal and external damage on space-based assets. Therefore, they should be at least regarded as soft-kill measures and correspondingly regulated in future or existent weapons treaties in outer space, such as the OST. All in all, there are existing treaties, manuals and conventions under development to regulate and address warfare in cyber and outer space, but they all seem to miss the opportunity to effectively address the connection between these two domains, either because they could not have anticipated such connection or because they purposefully decided to exclude it.

Moreover, it is important to note that certain state actors, such as China, are beginning to use lawfare (legal operations) strategies[40] in order to shape international law and exploit vacuums and ambiguities in this fluid legal environment as a means of countering the (superior) space power of the United States and its allies.[41] This circumstance makes it the more imperative to

[39] Ibid.
[40] Rodrigo Vazquez Benitez, 'Legal Operations: the use of law as an instrument of power in the context of hybrid threats and strategic competition,' (2020) in NATO Legal Gazette, Issue 41.
[41] Orde Kittrie, *Lawfare. Law as a Weapon of War* (Oxford University Press, 2016); *see also* John

develop truly common international rules to regulate the intersection between these two domains.

5. Implications for NATO

When it comes to NATO, the challenges derived from the interplay of cyber and space domains is accentuated by the fact that the organisation does not own satellites by itself, and is therefore dependent on member states' services and devices. NATO only owns and operates ground stations, such as 'satellite communication (SATCOM) anchor stations and terminals', therefore having to request access to member state's orbiting satellites for further services.[42] As a result, NATO relies on different types of space assets, may they be military, civilian, commercial or multinational ones. NATO's space-based assets' effectiveness is, thus, in its members' hands. The organisation is therefore confined to encouraging its member countries to strengthen their cyber protection capabilities and promote communication and mutual effort regarding cyber security applied to space-based objects,[43] as well as promoting and fostering the creation of common national and international rules.

NATO heavily relies on space-based assets for a wide range of critical operations, such as territorial defence, peacekeeping operations, counterterrorism, humanitarian relief and conflict prevention. These operations require 'beyond-line-of-sight (BLOS) communication' capabilities via satellite, meteorological reports, reconnaissance systems, precision air strikes and, thus, precision-guided munitions and unmanned aerial vehicles (UAV) among others.[44] Cyber-attacks against any of these capabilities could compromise communications and intelligence gathering and provide inaccurate information, leading to confusion, loss of connection with the command centre and, ultimately, mission failure. In addition, attacks could jam the GPS system, which is crucial for precision guided weapons manoeuvring and location of troops on the ground, consequently changing a missile's route or misleading the armed forces.[45] In this sense, in 2018, according to Norway

W. Bellflower, 'The influence of law on command of space,' (2010) in 65 Air Force Law Review 107.

[42] Unal, 'Cybersecurity of NATO's Space-based Strategic Assets,' 8-9 (n 4).

[43] Lumiste, 'Chatham House report,' (n 7).

[44] Unal, 'Cybersecurity of NATO's Space-based Strategic Assets,' 9-10 (n 4).

[45] Paul G. Kaminski, 'America Needs To Stay the Course on GPS Security,' (*Space News*, 19 November 2015, https://spacenews.com/op-ed-america-needs-to-stay-the-course-on-gps-security/ accessed 29 April 2021.

and Finland, NATO experienced consistent GPS jamming by Russia during the organization's Trident Juncture exercise in northern Europe, disrupting allied communication and intelligence.[46] The question is, if future potential attacks could be prevented if NATO profited from complete cyber security on its employed space-based assets. However, at present, NATO's military capabilities, such as communication and weapons systems not only lie in the hands of the member states, but also in the less credible cyber security protection of commercial and civilian space systems.

For its part, NATO recognises the legal challenges that cyber operations may pose due to 'the variety of effects' that such operations can create.[47] NATO goes even further, to acknowledge that some cyber activities can amount to an armed attack or to the use of force under the UN Charter, giving thus 'rise to the inherent right of individual or collective self-defence'.[48] In that sense, the organisation prioritises the promotion of a 'free, open, peaceful, and secure cyberspace', while 'enhancing stability and reducing the risk of conflict by supporting international law and responsible state behaviour in cyberspace'.[49]

Regarding outer space, in June 2021 in the NATO Summit Communiqué in Brussels, the organisation recognised the importance of this domain for the 'Alliance's operations, missions and activities.[50] Furthermore, NATO went on to endorse the fact that 'attacks to, from, or within space' imply an unequivocal challenge to the security, prosperity and stability of the Alliance and the Euro-Atlantic region.[51] Finally, the organisation compared outer space attacks to conventional offensives and declared that these activities could lead to the invocation of Article 5 of the North Atlantic Treaty.

In conclusion, while it seems that NATO recognizes the importance and

---

[46] Brooks Tigner, 'Electronic jamming between Russia and NATO is par for the course in the future, but it has its risky limits,' (*Atlantic Council,* 15 November 2018) https://www.atlanticcouncil.org/blogs/new-atlanticist/electronic-jamming-between-russia-and-nato-is-par-for-the-course-in-the-future-but-it-has-its-risky-limits/ accessed 29 April 2021.

[47] "NATO Standard AJP-3.20 Allied Joint Doctrine for Cyberspace Operations" (North Atlantic Treaty Organization), January 2020, 3.6, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf .

[48] Ibid.

[49] 'Brussels Summit Communiqué,' Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 14 June 2021, Art. 32, https://www.nato.int/cps/en/natohq/news_185000.htm .

[50] Ibid, Art. 33.

[51] Ibid.

challenges that the domains of outer space and cyberspace pose separately, prima facie it does not seem to recognize, or acknowledge, the threat that the connection of both domains represent.

6. Prospects for NATO

After analysing NATO's infrastructure with regard to space-based assets' cyber threats, one can only wonder what the organisation's future prospects are and how it can manage to address its space vulnerabilities. First, NATO should begin to acknowledge the imperative to protect its space infrastructure from cyber threats. The focus of member states and of the organisation remains fundamentally in the acquisition and improvement of conventional counter-space defensive and offensive assets. There is a general lack of seriousness and urgency in relation to space systems' cyber threats that, in the near future, could cost the alliance's operational effectiveness. There has been no significant legal advancement on space security issues since the Conference on Disarmament in Geneva since 1994.[52] It is therefore relevant for the alliance to enhance its cyber security and try to adapt its strategy to an ever changing domain, by prioritising its defensive capacities and safeguarding its most critical systems and networks.[53] Space systems' cyber security should be regarded as an integral part of national security and be dealt with accordingly.[54]

Moreover, in terms of recommendations for NATO's future cyber-space infrastructure, data encryption should be enforced as a means of protecting communication integrity from cyber interference, especially given that NATO is forced to share space systems with civilian and commercial enterprises.[55] Additionally, NATO should promote the implementation of a set minimum cyber security standards to ensure safe usage of shared space systems, as well as promoting public and private sectors' mutual cooperation in advancing

---

[52] Dr Patricia Lewis and David Livingstone, "What to Know about Space Security," Chatham House (27 September 2016), https://www.chathamhouse.org/2016/09/what-know-about-space-security .

[53] This has been the US DoD's position since 2015, see U.S. Department of Defense, "The DOD Cyber Strategy," (April, 2015), 13. The US DoD's position was again repeated in 2018, yet not real changes have been witnessed since its first mention in 2015, see U.S. Department of Defense, "DoD Cyber Strategy," (2018), 1, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF .

[54] Mike Gruss, 'Six Space Questions the Senate Asked Gen. James Dunford,' (*Space News*, 9 July 2015) https://spacenews.com/six-space-questions-the-senate-asked-gen-james-dunford/ accessed 29 April 2021.

[55] Falco, "Job One for Space Force: Space Asset Cybersecurity," 20 (n 22).

space-based assets' cyber security and resilience. At the same time, the organisation should strive to promote the necessity of introducing international outer space and cyber security treaty-based regulation. Finally, NATO should aim to identify potential vulnerabilities and risks in their space architecture and concentrate on strengthening those weaknesses.[56]

7. Conclusion

In the late nineteenth and early twentieth century, Alfred Thayer Mahan, Julian Corbett and other military strategist exposed the idea that whoever commanded the sea enacted power over land. Thereupon, following both World Wars, governments realised that whoever mastered the domain of air controlled the land and sea beneath. Nowadays, this notion has not changed, whoever controls space, has the surface of the earth at its feet.[57]

It is for this reason that NATO needs to be at the leading edge of cyber technologies and their appliance to space systems. The alliance relies heavily on external space-based assets, having to resort to the use of services and devices of member states and civilian or commercial shared space assets. In the same fashion, space-based systems are increasingly vulnerable to cyber threats, as they constitute easy and accessible targets for attackers. Consequently, the alliance's military capabilities that depend on space infrastructures, such as communication and weapons systems, are heavily exposed to cyber threats. It is for this reason that NATO is in urgent need of acknowledging its vulnerabilities and promoting cooperation for the establishment of credible cyber security capable of denying cyber-attacks in space systems, and the promotion of adequate national and international legal frameworks to enhance cyber security in the fluid legal framework of outer space. This will enable NATO to counter both cyber and legal operations (lawfare) offensive activities in outer space. Ignoring such essentiality will expose the vulnerability of the alliance's operational military effectiveness, communications and weapons systems, questioning NATO's trustworthiness as a reliable security organisation. Space systems are the cornerstones of military capabilities. Their loss would imply allied war effort incapacitation on the

[56] David Livingstone, 'Cyberattacks in Space: We Must Defend the Final Frontier,' (*Newsweek*, 26 November 2014) Unal, "Cybersecurity of NATO's Space-based Strategic Assets," 25-27 (n 4).

[57] Thomas White, 'Address to the National Press Club on November 29, 1957,' quoted in David E. Lupton, *On Space Warfare: A Space Power Doctrine* (Maxwell AFB, AL: Air University Press, 1988), 21.

ground and acute obstruction of operational success.[58]

Protection of space-based assets against cyber threats must become a priority for NATO and for international law. International treaties pertaining to warfare were written at a time when the domains of cyber and outer space were not defined as such. And yet, as military activities continue to increase, establishing the permitted behavioural parameters in these arenas, would aid the de-escalation of ongoing tensions and prevent future conflicts. Historically, law has always followed social changes and events. It would be desirable, if for once, international legislation went in unison or even prevented future critical situations caused by cyber-attacks on space architectures.

***

[58] Jason Wood, 'Strategic Security: Toward an Integrated Nuclear, Space, and Cyber Policy Framework,' in 'Nuclear Scholars Initiative Project on Nuclear Issues: A Collection of Papers from the 2010 Nuclear Scholars Initiative,' (*Center for Strategic and International Studies,* 2010) 95, https://csis-website-prod.s3.amazonaws.com/s3fs-public/110916_Wood.pdf .

Source : www.nato.int @ ESA

Cybersecurity Policy and Standards for Offworld Operations[1]

by Dr Roy Balleste[2] and Gilles Doucet[3]

The present-day executive and military commander may obtain

[1] **DISCLAIMER**: The views expressed in this article are solely those of the authors and may not necessarily represent the views of NATO, Allied Command Operations, or Allied Command Transformation, or of their affiliated organizations.

[2] Dr Roy Balleste is Assistant Professor of Law at Stetson University. Professor Balleste has focused his scholarship on the evolving regulatory challenges of internet governance, cybersecurity law and policy, cybersecurity in outer space, cyber operations, and cyber conflict. Balleste is currently a core expert and member of the editorial board of the Manual on International Law Applicable to Military Uses of Outer Space (MILAMOS). Balleste holds a J.S.D. in Intercultural Human Rights (analysing internet governance, St. Thomas University); LL.M. in Air and Space Law (McGill University); LL.M. (St. Thomas University); J.D. (St. Thomas University); and M.S. in Cybersecurity (Norwich University, expected August 2021). Professor Balleste is also a member of the International Institute of Space Law (IISL) and Director of Information Security for ABH Aerospace.

[3] Gilles Doucet is an independent space security consultant and President of Spectrum Space Security Inc. Doucet's consultancy focuses on the convergence of satellite technology, national security applications, space governance and international space security cooperation. Doucet is Technical Lead of the drafting committee for the Manual on International Law Applicable to Military Uses of Outer Space (MILAMOS) and also a technical expert for the McGill Encyclopaedia of International Space Law project. Through his consulting company, Doucet provides instruction and training in space technology fundamentals and space security to Canadian government departments and agencies. Mr. Doucet spent 35 years as a research scientist with the Canadian Department of National Defence. Doucet holds Bachelors and Masters degrees in engineering and a Graduate Certificate in Air and Space Law (McGill University).

significant tactical rewards because of the confidence in new standards that mould the boundaries of technological developments. In the modern world of space industries, the potential for a cyberattack with devastating consequences should not be underestimated. Satellite systems, consisting of cyber-enabled space, link, and ground segments, are prone to severe vulnerabilities and could potentially suffer ruthless disruptions in their critical infrastructure. There are no standards for securing these vital nodes. Space systems also provide integral support to cyber operations and represent critical infrastructure that enables ongoing strategic and tactical operations in all domains, including space. As a result, senior leaders and commanders are encouraged to improve the security of their organizations. Air Marshal Giulio Douhet once noted that "[v]ictory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur."[4] The space industry's relation to cyberspace is one of those changes that need consideration and precisely represents the grey area that now challenges future everyday perceptions. In that context, and in relation to the Soviet first satellite, Sputnik, the chief judge of the International Court of Justice, Manfred Lachs, noted that the "fundamental issue that arose on the day the first man-made instrument was launched into outer space concerned the law that should be applied to this domain and activities directed towards it: the identity, nature, and framework of that law."[5] In essence, users of outer space cannot define that law's framework without first identifying the concepts and their nature in relation to human activity.

The purpose of this article is to raise awareness and survey selected aspects of satellite systems, link and ground segments, cyber interference, and disruptions to this critical infrastructure. This paper will assess selected aspects of securing satellite control systems and operations and provide guidance on much needed standards and best practices. The role of standards cannot be underestimated for the cybersecurity of satellites. Other similarly situated infrastructure industries that rely on automated control systems were slow to recognize cyber vulnerabilities. Lack of planning and failure to protect against cyberattacks cost some public infrastructure companies millions of dollars in losses and most likely millions of dollars in legal fees. The space infrastructure is in greater need of assessment. The question of the security of critical infrastructure systems for the space industry has not been fully assessed—and

[4] Giulio Douhet, *The Command of the Air* (Joseph Patrick Harahan and Richard H. Kohn, eds, Tuscaloosa: AL; University of Alabama Press, 1921; 2009) 30.
[5] Manfred Lachs, *The Law of Outer Space: An Experience in Contemporary Law-Making* (Leiden: The Netherlands, Martinus Nijhoff Publishers, 1972, 2010) 125.

possibly—hardly assessed at all by many governments or commercial sector actors. Since the cyber threat landscape continues to evolve with high unpredictability, security risk management should be a continuous process. In particular, this article acknowledges the rising aerospace market and highlights areas where senior executives and commanders should focus their attention. The paper examines how the evolving commercial industry's uses of outer space and potential cyberattacks affect operational security. The paper explores how space-based capabilities provide integral support to commercial applications, enabling space exploration. The article notes the lack of a unified formal awareness program for organizations in the industry to share or promote acceptable standards.

Thoughts of Cislunar Space

Today, information-driven organizations and the consumers they serve live in an intriguing time of new space ventures. These ventures are intertwined with cyber operations. The new satellite organizations will succeed or fail, in significant part, by their serious consideration of security awareness. The organization's security awareness must tackle vulnerabilities and, at the same time, apply needed controls to counter potential issues.[6] The outer space industry's first line of defence should be associated with all employees' need to acquire the necessary training.[7] These exciting technological endeavours beyond our atmosphere belong to a new era of space exploration and one in which "private access to space is becoming almost routine."[8]

It is safe to state that cybersecurity best practices are expected of any industry, even beyond the organization's boundaries, as long as there is proper communication of these policies and there is no conflict with modern work processes.[9] Just as on land, in outer space, vulnerabilities can materialize due to third-party contractors' shortcomings. Last year, Visser Precision, a manufacturer of space and defence parts for SpaceX, confirmed a

---

[6] Bob Allin, 'How to Implement a Security Awareness Program at Your Organization' (*Threat Stack*, 21 March 2017) https://www.threatstack.com/blog/how-to-implement-a-security-awareness-program-at-your-organization

[7] William Stallings, W. and Lawrie Brown, *Computer Security, Principles and Practice* (3rd Edition, Pearson 2014) 558.

[8] Piers Bizony, *New space frontiers: Venturing into Earth Orbit and Beyond* (Zenith Press, 2014) 1.

[9] Grayson Kemper, 'How Employees Engage with Company Cybersecurity Policies' (*Clutch*, 15 May 2018) https://clutch.co/it-services/resources/how-employees-engage-company-cybersecurity-policies

ransomware incident.[10] The incident involved access to data or data theft caused by the 'DoppelPaymer' ransomware.[11] Still, it is difficult to ascertain SpaceX staff's actions, its cybersecurity policy in relation to third parties, and whether there was human error. "Among the space industry community, the lack of attention to cybersecurity is acknowledged."[12] While an audit of NASA in 2015 demonstrated the lack of up-to-date cybersecurity standards and protocols, it also served as a reminder that smaller satellite organizations seek out NASA's examples of standards and best practices.[13] Yet, the more significant challenge continues to be with established organizations such as SpaceX and Blue Origin, which have not made available their cybersecurity policies.[14] This challenge has been highlighted as a matter of notice given that experts outside the industry fear their lack of preparedness.[15]

Thoughts of cislunar operations remind stakeholders of the steps required to draft policy-oriented standards centred on the best combination of risk management techniques for the benefit of cybersecurity in outer space. The Aerospace association introduced in 2011 its "Policies and Codes of Conduct for the Use of Social Networks."[16] While centred on social networking, this comprehensive document offers useful recommendations indigenous to acceptance use policies found in other industries, including use behaviour, data protection, and other relevant subjects.[17] Possibly the most important and more news-worthy related document drafted to date in the United States is the "Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems." Any future recommended policy should be based or at least acknowledge the elements of this document. Directive-5 is also known as the

---

[10] Zack Whittaker and Kirsten Korosec, 'Visser, a parts manufacturer for Tesla and SpaceX, confirms data breach' (*Techcrunch*, 1 March 2020) https://techcrunch.com/2020/03/01/visser-breach/?guccounter=1

[11] ibid.

[12] Gregory Falco, 'The Vacuum of Space Cybersecurity' (*AIAA SPACE Forum*, 17 September 2018) https://www.researchgate.net/publication/327678396_The_Vacuum_of_Space_Cyber_Security

[13] ibid at 7.

[14] ibid.

[15] Zulfikar Abbani, 'SpaceX's Starlink satellite internet: It's time for tough talk on cyber security in space' (*DW*, 21 February 2018) <https://www.dw.com/en/spacexs-starlink-satellite-internet-its-time-for-tough-talk-on-cyber-security-in-space/a-42678704>

[16] E-Business Steering Group. 'Policies and codes of conduct for the Use of Social Networks' (*Aerospace Industry Association*, December 2011) https://www.aia-aerospace.org/wp-content/uploads/2016/05/report_social.pdf

[17] ibid.

policy for cybersecurity principles for space systems.[18] This policy could easily be an annex to the "Information Security Handbook: A Guide for Managers" (NIST SP 800-100) as sections 4 and 5 of Directive-5 do relate back to the handbook's chapters 8 and 9.[19] While it may take a few years for various government policies to catch up to the space technologies, it will be up to those engaged in space operations to adopt the appropriate risk management measures. Another source normally consulted, the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, is an excellent guide for cyber-outer space legal issues, yet there is much of cybersecurity that falls outside the purview of that resource.

Cyber vulnerabilities of space system networks

Space systems are susceptible to a number of cyber threats, some of which are similar to terrestrial networks, but also some which are unique. From a cyber-threat perspective, most space system networks can be divided into the following four components:[20]

- The space segment consisting of the satellite(s) in Earth's orbit;
- The operator ground segment consisting of one or more stations that control the satellite(s);
- The user segment consisting of ground stations or terminals required for receiving the space service being provided (e.g. communications, remote sensing, navigation); and
- The link segment which connects the satellite with operators and users on the ground using radio-frequency signals. This segment is often divided into the operator and user segments since they serve different functions and have different cybersecurity requirements.

All of the space system components may be vulnerable to cyber interference in one form or another and require protection. The degree of protection required will depend on multiple factors. Some of these factors are the specific segment being protected, the risk to the system, the nature and

[18] White House, 'Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems' (4 September 2020) https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/
[19] National Institute of Standards and Technology. SP 800-100-information security handbook: A guide for managers (U.S. Department of Commerce, October 2006) 67, 78
[20] National Air and Space Intelligence Centre. 'Competing in Space' (December 2018), 18, https://media.defense.gov/2019/Jan/16/2002080386/-1/-1/1/190115-F-NV711-0002.PDF

sensitivity of the service and the nature of the operator and users.

Satellite on-board computers (also known as command and data handling systems) usually run Real Time Operating Systems. These operating systems are generally used in mission critical enterprise systems, such as SCADA systems, where timeliness of execution of certain functions is paramount.[21] In this sense the IT networks within satellites are similar to many industrial control IT systems. Some common operating systems used in western satellites are Vx Works (proprietary software by Wind River Systems), RTEMS (open source freeware) and special adaptations of Linux. When used in satellite systems, these operating systems are generally not configured to provide cybersecurity protection. In the case of satellites, there is an assumption of protection from intrusion and malware by the cybersecurity measures inherent in the communications with the operators and the command processes. This was a realistic assumption in the past when satellites were individually designed and manufactured by a few aerospace firms with mostly proprietary hardware and software. However, increasing use of COTS electronics, the commoditization of satellite components and assembly line production places the validity of this assumption in doubt. Future satellite IT networks may need to implement internal cybersecurity measures.

The operator station (often called the TT&C[22] station) is the most critical node. It ensures the health, safety and operations of the satellite. The stations normally operate standard IT networks and may be vulnerable to the full gamut of cyber-attacks techniques depending on connectivity to other terrestrial networks and level of cybersecurity protection. The consequence of cyber intrusion into the operator station may be the loss of the satellite.

The user segment may be the least protected since its compromise will not generally threaten the health of the satellite. However, compromise of the user segment can impact services and, importantly for commercial operators, result in significant financial losses. For this reason, commercial providers should be highly motivated to protect this segment. However, cybersecurity measures also have a financial and efficiency cost so operators may use a cost/risk analysis to decide on security measures to implement.

The link segment may be protected by encryption and satellite access may be additionally protected by authentication protocols. These cybersecurity measures impose additional costs, complexity and may reduce

[21] SCADA stands for supervisory control and data acquisition
[22] TT&C stands for Telemetry, Tracking and Command

data transfer rates. Harmful interference or jamming in the radio-frequency spectrum can result in a denial of service. The operator links are in particular need of protection in order to ensure that control of the satellite is not lost.

National Regulations & Licensing

Pursuant to article VI of the Outer Space Treaty, States Parties are obligated to authorize and supervise the national space activities of their non-governmental entities.[23] As a result, many States have established regulatory regimes that include licensing for private space activities. This provides an opportunity for States to insist on cybersecurity measures to protect the operations of space systems and ensure resilience of critical infrastructure services. However, while many States do insist on some degree of cybersecurity protection planning involving plans or strategies, the practice is uneven and there are few specific recognized international standards for space systems that can be explicitly imposed.

The United States has a complex and evolving licensing regime for private space operators but lacks an overall approach to cybersecurity protection. According to a recent study by The Aerospace Corporation, "The vulnerability of satellites and other space assets to cyber-attack is often overlooked in wider discussions of cyber threats to critical national infrastructure,"[24] Worse yet, requirements or standards for cybersecurity for the majority of commercial satellites do not exist. With the exception of national security considerations, there are no United States governmental cybersecurity standards that private operators must meet. The motivation for the cybersecurity standards that do exist have been developed to address national security concerns and not for the assurance of civil critical infrastructure.

Space systems, governmental and private, that support national security missions are subject to cybersecurity requirements set out by Policy 12 of the Committee on National Security Systems ("National Information Assurance Policy for Space Systems Used to Support National Security Missions").

---

[23] *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the moon and Celestial Bodies,* opened for signature at London, Moscow and Washington on 27 January 1967, 610 UNTS 205, 18 UST 2410, TIAS 6347, 6 ILM 386, entered into force on 10 October 1967.

[24] Brandon Bailey, Ryan J. Speelman, Prashant A. Doshi, Nicholas C. Cohen, Wayne A. Wheeler, 'Defending Spacecraft in the Cyber Domain' (*The Aerospace Corporation Centre for Space Policy and Strategy*, November 2019) https://csps.aerospace.org/papers/defending-spacecraft-cyber-domain

The Department of Commerce (acting through the National Oceanic and Atmospheric Administration), licenses remote sensing space systems and can insist on cybersecurity measures to protect the space system and the remote sensing data from a national security perspective. Commerce policies have been evolving recently to reduce the licensing and compliance burden on private operators and is easing cybersecurity requirements. For Tier 1 systems (the least sensitive) the only cybersecurity requirement is that licensees operating spacecraft with propulsion affirm that they have measures in place to ensure positive control of those spacecraft. For more sensitive Tier 2 and 3 systems, the licensee may be required to protect data as specified in the directive, which may include encrypting satellite TT&C and mission data transmissions. The Department of Commerce is not mandating any specific cybersecurity standard. Operators will self-develop a cybersecurity risk management plan using best practices.[25] However, those "best practices" can be difficult to identify in a diverse group of space operators and missions.

The United Kingdom's Space Industry Act 2018 regulates all spaceflight activities carried out from the UK and requires the licensing of any such activity.[26] The implementing regulations address cybersecurity requirements for commercial spaceflight operators.[27] Chapter 3 (articles 173 and 174) compels a licensee to "draw up and maintain a cyber-security strategy for the network and information systems ("the systems") used in relation to spaceflight operations".[28] The cybersecurity strategy must meet a number of conditions, among which include: to be based on a risk assessment, to be proportionate and appropriate for the type of systems operated and comply with the United Kingdom's international obligations. No specific standards are mandated for the licensee and the regulator will (presumably) assess their adequacy on a case by case basis.

Unlike the United Kingdom, Canada has no overarching legislation regulating space activities and thus no generic ability to impose cybersecurity standards on private operators of space systems, with the exception of remote sensing systems. The Remote Sensing Space Systems Act regulates the

---

[25] National Oceanic and Atmospheric Administration, '15 CFR Part 960 - Licensing of Private Remote Sensing Space Systems' (Department of Commerce) https://www.govinfo.gov/content/pkg/CFR-2020-title15-vol3/pdf/CFR-2020-title15-vol3-part960.pdf

[26] Space Industry Act 2018, c. 2.

[27] The Space Industry Regulations 2020, Draft Regulations laid before Parliament under section 68(6) of the Space Industry Act 2018, for approval by resolution of each House of Parliament.

[28] Id at 173.

operation of space remote sensing activities, including data collection, processing and distribution.[29] The RSSSA regulations and subsequent interpretations require the operator to develop and submit a command data protection plan that includes cybersecurity in order to prevent loss of satellite control and loss of data.[30] However, no specific satellite cybersecurity standards are referenced and the final approval of the license application rests with the Minister of Foreign Affairs, which retains discretion to decide on the adequacy of the protection plan on a case by case basis.

National licensing legislation provides the mechanism for States to implement cybersecurity standards on their national space activities, both governmental and private. However, the absence of recognized international standards impedes this outcome.

Cybersecurity Framework

The security of critical infrastructure systems for the space industry has not been fully assessed—and possibly—hardly understood by many governments and commercial sector actors. Since the cyber threat landscape continues to evolve with high unpredictability, security risk management should be a continuous process. While traditional domains may apply the practices contained in the confidentiality, integrity, and availability (CIA) triad model, if an attack were to occur, this practice would necessitate a reversal of order. In other words, managers are encouraged to improve their ability to mitigate risks. A malfunction of the electrical grid—for example—would raise serious consequences for the human operators and the general public counting on their services. One anticipated vulnerability would be the potential tampering of data integrity or data availability.[31] However, while critical infrastructure organizations operate with similar systems, would these have the same set of baselines controls to mitigate risk? To answer this question, consider that "[g]oing above and beyond further ensures that customers have a great experience."[32] The Standards for Security Categorization (FIPS Publication 199),

---

[29] Remote Sensing Space Systems Act, SC 2005, c 45.
[30] Global Affairs Canada, Non-Proliferation, (Disarmament and Space Division), REMOTE SENSING SPACE SYSTEMS ACT, Operating Licence Application Guide, Version 1.1, March 8th, 2021. https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/RSSSA-guide-LSTS.aspx?lang=eng .
[31] Clay Wilson, 'Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress' (*Congressional Research Service*, 29 January 2008) https://sgp.fas.org/crs/terror/RL32114.pdf
[32] Jason Maynard, 'Baseline Cybersecurity Controls for Small and Medium Organizations' (*Cisco Canada Blog*, November 8, 2019) https://gblogs.cisco.com/ca/2019/11/08/baseline-

as an example, provide the necessary delineation to highlight the objectives of the data.[33] These observations, in turn, return the assessment to the CIA triad model. The SCADA industry is particularly interested in availability: "Ensuring timely and reliable access to and use of information."[34] Furthermore, the security categorization process would offer additional information.[35] This process would continue into the NIST Special Publication 800-53, and in particular, Appendix F. It is due to its characteristics that industrial control systems present a homogeneous environment.

A holistic approach requires an understanding of the architecture, attack methodologies, along with the guiding light of standards. This is the foundation for securing the 'availability' of data. This foundation begins with a cybersecurity framework. "Created through collaboration between industry and government, the voluntary Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk."[36] Thus, this holistic approach returns the practitioner to Directive-5, section b (iv):

"Protection of ground systems, operational technology, and information processing systems through the adoption of deliberate cybersecurity best practices. This adoption should include practices aligned with the National Institute of Standards and Technology's Cybersecurity Framework to reduce the risk of malware infection and malicious access to systems, including from insider threats. Such practices include logical or physical segregation; regular patching; physical security; restrictions on the utilization of portable media; the use of antivirus software; and promoting staff awareness and training inclusive of insider threat mitigation precautions…"[37]

Conclusion

The purpose of this article was to raise awareness and survey selected

cybersecurity-controls-for-small-and-medium-organizations/

[33] National Institute of Standards and Technology. *Standards for Security Categorization of Federal Information and Information Systems (FIPS 199)*, (U.S. Department of Commerce, February 2004) 1.

[34] ibid at 2.

[35] ibid at 4.

[36] National Institute of Standards and Technology, 'New to Framework" (23 September 2020) https://www.nist.gov/cyberframework/getting-started

[37] White House (n 17).

aspects of policies, practices, and standards useful for space operations that involve cyber activities. In particular, this article acknowledged the rising aerospace market and highlights areas where senior executives and operators should focus their attention. The article addressed technical considerations for industry operators. It also noted the lack of guidance on acceptable polices, while observing emerging new trends within the aerospace sector. The security of the space infrastructure is in greater need of assessment.

***

Source : https://ac.nato.int

Intersections of International Legal Rules in Cyberspace and Outer Space[1]

by Dr Adina Ponta[2]

After NATO foreign ministers officially declared both cyberspace and outer space operational domains for the Alliance, it became even clearer that scientific and technological advances often test the limits of international law. Both domains lack a proper "territorial" area, solid understanding of applicable rules and norms, and borrow general international law principles. Outer space and cyberspace are emerging into the 21st century as an increasingly interlinked governance regime, which is imprecisely addressed in international law and in the few existing national Space Policy Directives.

First, this paper will offer an outline of the current status of some international law issues in cyberspace and outer space while examining common features and shared concerns relevant for NATO as an Organization and for its members. While sovereign control of outer space is impeded by legal

[1] **DISCLAIMER**: The views expressed in this article are solely those of the author and may not necessarily represent the views of NATO, Allied Command Operations, or Allied Command Transformation, or of their affiliated organizations.

[2] Adina Ponta is a postdoctoral teaching fellow at the Babes-Bolyai University in Romania and an attorney. She was the 2020 Detlev F. Vagts International Law Fellow at the American Society of International Law in Washington, D.C. Prior to that, she was a legal intern in NATO HQ SACT and Assistant Legal Advisor at HQ NATO AEW&CF GK. She has an LL.M. in international law and a Ph.D. in business and technology law.

and practical limits, the cyber realm presents some unique particularities which affect attribution, liability, and due diligence issues. Corollary questions include the scope of aggression in space and whether the right to self-defence under the U.N. Charter and collective defence under the North Atlantic Treaty could be triggered outside the terrestrial domain. The above-mentioned questions are equally important in cyberspace, for which NATO members have already agreed that Article 5 could be triggered in response to a cyberattack.

Second, this article will address international law questions related to cyber operations on space related infrastructure. Common challenges of weaponisation in outer space and cyberspace derive from the fact neither of these areas beyond national jurisdiction is governed by an arms control treaty, but operations which traverse both domains merit a deeper examination.

I. Relevant legal aspects applicable to cyberspace, outer space and common features

1. Relevant international law applicable to cyberspace

After states, international organizations, and international coordinating fora endorsed the application of international law to cyberspace, the debate shifted to questions of how existing principles, rights, and obligations should be interpreted in the cyber realm. Various exercises have attempted to identify the applicable international law in addressing cyber intrusions against foreign states, possible state responses, and legal consequences of cyber operations, both during war and during peacetime. Fragmentation is most visible with respect to the scope of notions such as the prohibition of the use of force, the principles of sovereignty and non-intervention. Each of these will be discussed below.

Early analysis of the legal implications of cyber operations that rise to the threshold of **use of force** or an armed attack mostly focused on the prohibition of the use of force in Article 2(4) of the U.N. Charter. Most states regard the threshold for the use of force to be lower than that required for an armed attack, an approach reflected by the International Court of Justice (ICJ).[3]

[3] The ICJ *Military and Paramilitary Activities in and against Nicaragua case* is a useful tool to differentiate the two terms, as the Court held that an armed attack "only exists when force is used on a relatively large scale, is of a sufficient gravity, and has a substantial effect", and is therefore "most grave forms of the use of force". *See* Nicaragua v United States of America (Merits, Judgment) [1986] ICJ. The U.S. embraces a different view, namely that the armed attack threshold is equal to that of the use of force, U.S. Dep't. of Defense, Law of War Manual, ¶ 16.3.3.1.

Determining if a cyber-operation reaches the level of an armed attack under *jus ad bellum* has proven to be challenging in practice and legal opinions differ as to whether cyber operations that do not physically destroy or damage military or civilian infrastructure can be considered an expression of use of force governed by IHL, in absence of kinetic hostilities.

After the cyber realm demonstrated the imminent peril of operations which fall short of acts of war and are, therefore, outside the scope of international humanitarian law (IHL), focus shifted to low-intensity cyber aggression.[4] There are two schools of thought about how international law applies to state-sponsored cyber activity that takes place below the threshold of use of force.[5] The first group argues that the **principle of non-intervention** applies to certain state-sponsored cyber intrusions, and that below the threshold set by this principle, cyber activity may be unfriendly, but does not constitute a breach of international law giving rise to state responsibility. According to this approach, **sovereignty** is a principle of international law that may guide state interactions, but it does not amount to a standalone primary rule.[6] The second view holds that such cyber operations may be unlawful as violations of the target state's sovereignty, a rule of international law.[7] To date, no international tribunal has associated an intrusive cyber operation with a physical violation of a state territory[8] and customary international law does not provide a clear answer to whether any unauthorized cyber intrusion would violate the target state's sovereignty.[9]

Under international jurisprudence, general principles of law further imply

---

[4] Kristen Eichensehr, 'The Law & Politics of Cyberattack Attribution' [2020] 67 UCLA Law Review; Liis Vihul, 'International law of cyber defence', in J. Rehrl (ed.), *Handbook on Cybersecurity: The Common Security and Defence Policy of the EU* (2019).
[5] Harriet Moynihan, 'The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention' (2019), Chatham House Research Paper.
[6] Gary P. Corn, Robert Taylor, 'Sovereignty in the Age of Cyber' [2017] 111 Ajil Unbound 207.
[7] The Tallinn Manual 2.0. endorses the general application of the principle of sovereignty to cyberspace and the exercise of internal state sovereignty over cyber activity, actors, and infrastructure located within its territory; *See* Michael N. Schmitt, Vihul Liis, 'Respect for Sovereignty in Cyberspace'[2017] 95 Texas L. Rev. 1639.
[8] Even though most legal scholars regard state-sponsored cyberoperations involving a physical intrusion against another state as violations of sovereignty, they only partially agree that this is also the case for remote operations causing physical damage or loss of functionality. *See* Sean Watts, Theodore T. Richard, 'Baseline Territorial Sovereignty and Cyberspace' [2018] 22 Lewis & Clark L. Rev. 771.; Michael N. Schmitt, Vihul Liis, 'Sovereignty in Cyberspace: Lex Lata Vel Non?' [2017] 111 Ajil Unbound 213.
[9] Moynihan, *supra* note 4; François Delerue: *Cyber Operations and International Law* (Cambridge Univ. Press 2020).

an obligation of states to take affirmative action to ensure that their territory or objects over which they maintain sovereign control are not used for internationally wrongful purposes.[10] Deriving **due diligence** duties in cyberspace from the principle of equal state sovereignty, Rule 6 of the Tallinn Manual 2.0. notes states' obligation to ensure that the "territory or cyber infrastructure under their control is not used for operations that affect the rights of, and produce adverse consequences for, other states".[11] The preventive aspect of due diligence in this context is still unsettled.[12] By analogy with international environmental law, the adoption of the precautionary principle in cyberspace would rely on the ICJ affirmation that prevention is reflective of customary international law, as part of the due diligence principle.[13] This parallel could develop a state obligation to assess cyber activity within its jurisdiction, similar to environmental impact assessments, if there is a likelihood of transboundary harm.[14]

Attribution is central for establishing state accountability for cyber conduct that affects other sovereign nations. In general, acts of private actors are only attributable to states if they qualify as state organs or are lawfully empowered to exercise governmental authority. To date, three main types of state-proxy relationships have been identified: delegation, orchestration, and sanctioning (i.e., approving or permitting).[15] If a cyber-act is not followed by

[10] United States v Netherlands, Award, [1928] II RIAA 829, ICGJ 392 4th April 1928, PCA.
[11] According to the Manual, this principle covers remote operations and operations conducted from or through state territory, that affect the legal rights, not mere interests, of other states. The director of the Tallinn Manual Process explains that this includes, for example, the right to be free from intervention from another state. This principle can be expanded to apply to operations that are not ongoing, but imminent, though the results have not yet materialized, *See* NATO CCDCOE 10th International Conference on Cyber Conflict (CyCon 2018) at https://www.youtube.com/watch?v=YOIuiNfaZU8 accessed 24 April 2021; Michael Schmitt, 'France's Major Statement on International Law and Cyber: An Assessment' (*Just Security*, 16 September 2019), https://www.justsecurity.org/66194/frances-major-statement-on-international-law-and-cyber-an-assessment/, accessed 24 April 2021.
[12] Prevention, an element of due diligence, is reflected in the General Data Protection Regulation (GDPR), and has been endorsed by the World Trade Organization (WTO), by the International Tribunal for the Law of the Sea (ITLOS) and, in the environmental context, by the ICJ.
[13] Peter Z. Stockburger, 'From Grey Zone to Customary International Law: How Adopting the Precautionary Principle May Help Crystallize the Due Diligence Principle in Cyberspace" (2018) 10th International Conference on Cyber Conflict (T. Minárik, R. Jakschis, L. Lindström eds.), NATO CCD COE Publications.
[14] Przemysław Roguski, 'Application of International Law to Cyber Operations: A Comparative Analysis of States' Views' (2020) https://www.thehaguecybernorms.nl/research-and-publication-posts/application-of-international-law-to-cyber-operations-a-comparative-analysis-of-states-views, accessed 21 April 2021.
[15] Article 8 of the International Law Commission's Draft Articles on Responsibility of States for

formal attribution, and there is no demonstrated violation of international law, the target state can resort to three types of reactions,[16] i.e., mechanisms for international cooperation and dispute settlement, acts of retorsion,[17] and exceptional mechanisms of self-protection, such as invoking the state of necessity, distress, or force majeure in order to engage in more concrete responses.

If unlawful cyber operations can be attributed to a state, the possible reactions are different. First, victim states can engage in peaceful countermeasures, but it is still debated whether these deterrence mechanisms, developed for the physical world, are as credible, or lawful, in the cyber domain.[18] In the absence of clear rules to distinguish lawful from unlawful state behaviour in cyberspace, target states are reluctant to firmly respond to hostile cyber operations, and usually resort to minimal public action, such as "naming and shaming" strategies. Though countermeasures do not need to mirror the nature of the underlying internationally wrongful act that legitimizes them, assessment of proportional responses can be challenging.[19]

While most states seem to agree on the application of general international law to transboundary cyber operations, the precise translation and the practical limits of the rules developed in the physical world to cyberspace are widely debated.[20] Numerous cyber policy fora have proliferated in diverse formats, such as the U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE)[21], the subsequent U.N. Open-Ended Working Group on Developments in the Field of ICTs in the Context of

---

Internationally Wrongful Acts assimilates *de facto* actions by persons or entities acting on the instructions of, or under the direction or control of, a state in carrying out the conduct, as state-sponsored actions; *See* also Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge University Press, 2019).

[16] Karine Bannelier, Theodore Christakis, 'Cyber-Attacks – Prevention-Reactions: The Role of States and Private Actors' [2017] Les Cahiers de la Revue Défense Nationale.

[17] Jeff Kosseff, 'Retorsion as a Response to Ongoing Malign Cyber Operations' (2020) 12th International Conference on Cyber Conflict, NATO CCDCOE.

[18] Gary Corn, Eric T. Jensen, 'The Use of Force and Cyber Countermeasures' [2018] 32 Temple Int'l &Comp. L. J.

[19] Michael N. Schmitt, 'Below the Threshold Cyber Operations: The Countermeasures Response Option and International Law' [2014] Virginia J. of Int'l L.54.

[20] Ido Kilovaty, 'The Elephant in the Room: Coercion' [2019] 113 Ajil Unbound 87.

[21] UNGA 'Developments in the field of information and telecommunications in the context of international security. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' UN Doc A/70/174 (22 July 2015).

International Security (OEWG), and other industry-focused norm processes. However, though states have identified the referent principles of the cyber legal order, the content and scope of the applicable rules still need to be determined. This is further confirmed by the failure of the 2017 GGE to produce a report. It is nonetheless true that although rule consolidation is gradual and slow, certain nonbinding norms endorsed in the 2015 GGE report and in other instruments can progressively attain customary law status.[22]

2. Relevant international law applicable to outer space

While technical experts disagree on whether mankind should prioritize a return to the Moon or the exploration of Mars, lawyers have analysed international law grounds for space activities.[23] The drafters of the five primary binding space treaties[24] assumed that space would be dominated by states rather than private entities, a situation that is rapidly evolving. While Article II of the Outer Space Treaty (OST) prohibits sovereign territorial claims or national appropriation of a celestial body, including the Moon, this prohibition is widely regarded to also apply to the private sector.[25]

A distinct feature of space law, compared to other areas beyond national jurisdiction (ABNJ), is direct attribution.[26] Damage caused by the collision of space objects in outer space is governed by the mechanism for compensation under the Liability Convention.[27] While being a fault-based

---

[22] Efforts to reach global consensus on these issues have so far failed, mostly because states' views are poorly aligned. *See* for e.g. NATO CCD CoE, 'A surprising turn of events: UN creates two working groups on cyberspace' https://ccdcoe.org/incyder-articles/a-surprising-turn-of-events-un-creates-two-working-groups-on-cyberspace/ , accessed 21 April 2021; *See also* Duncan B. Hollis, Martha Finnemore, 'Constructing Norms for Global Cybersecurity' [2016] 110 AJIL 425.

[23] Louis Friedman, 'For the United States, a second race to the moon is a second-rate goal' (*Spacenews*, 2020) https://spacenews.com/op-ed-for-the-united-states-a-second-race-to-the-moon-is-a-second-rate-goal/; Giulio Prisco, 'The United States won't go back to the moon, I'll follow China there instead' (*Spacenews*, 2020), https://spacenews.com/op-ed-the-united-states-wont-go-back-to-the-moon-ill-follow-china-there-instead/, both accessed 21 April 2021.

[24] These are: The 1967 Outer Space Treaty, The 1968 Rescue and Return Agreement, The 1972 Liability Convention, The 1976 Registration Convention, The 1979 Moon Agreement.

[25] The non-ratification of the OST by several states is most relevant in relation to space resources. *See* Mariam Yuzbashyan, 'Legal Regime of Natural Resources of the Moon and Other Celestial Bodies' (2019), 12th RISA Convention, Section 2.1. Int'l L. and Security.

[26] Event 'Live from L 2020 - Space Law' (2020) Georgetown University, Washington D.C., https://www.youtube.com/watch?v=FtpQOdm85LQ&t=413s , accessed 21 April 2021.

[27] Attribution can be determined through traditional principles of territorial and personal jurisdiction. Additionally, the OST established space object registration as third basis for states' jurisdiction and control over space objects and their personnel. *See* Manal Cheema, "Ubers

international liability regime, the term "fault" is not defined by the Convention. There is therefore a lack of clarity as to whether it includes fault in the specific "context of a liability regime or as understood within the regime of state responsibility for wrongful acts. Customary law points toward the latter interpretation".[28]

In comparison to the customary law of state responsibility, the threshold for the attribution of a conduct to the relevant state is lower.[29] In this context, assessment of due diligence fault, whose complexity was highlighted in the area of cyberspace, becomes extremely relevant, especially due to modern transformation of actors, activities, technologies and liability issues in outer space.[30]

Militarization of outer space received special attention in legal literature and media after two important events. First, the establishment of a Space Force, as a separate branch of the U.S. military, and of a French rebranded "Air and Space Force", suggest the possibility that outer space is perceived as a future operational warfighting domain. The principle of peaceful use of outer space prohibits state parties from stationing weapons of mass destruction, including biological, chemical, and nuclear weapons in orbit around the Earth, on celestial bodies, or in outer space; building military bases; weapons testing; and conducting military manoeuvres. This exhaustive exemplification clearly indicates that sending or stationing other types of weapons in space other than those of mass destruction, including cyber-weapons is not prohibited.[31] Therefore, the prohibition of "weapon placement in space does not necessarily prevent use of weapons in space such as Anti-satellite weapons (ASAT)", designed to disable or destroy satellites for strategic or tactical purposes. [32]

---

of Space: U.S. Liability Over Unauthorized Satellites' [2020] J. Space L.

[28] Joel A. Dennerley 'State Liability for Space Object Collisions: The Proper Interpretation of 'Fault' for the Purposes of International Space Law' [2018] 29 Eu. J. Int'l L. 281.

[29] Elina Morozova, 'Limits imposed by outer space law on military operations in outer space' (2019), 42nd Round Table on Current Issues of IHL on the 70th Anniversary of the Geneva Conventions Sanremo.

[30] Due diligence fault, as well as other unregulated space law issues, will very likely be interpreted through soft law instruments. See Thomas Kirchberger, Sigmar Stadlmeier, 'Soft Law in Outer Space: The Function of Non-binding Norms in International Space Law' [2015] 17 Austrian Rev. Int'l. & Eur. L. Online. However, not all scholars agree that soft law should play a role in this regard. *See , e.g.*, Jack M. Beard, '**Soft Law's Failure on the Horizon: The International Code of Conduct for Outer Space Activities**' [2017] 38 U. Pa. J. Int'l L. 335.

[31] *See supra* 25.

[32] Rajeswari Pillai Rajagopalan, 'Electronic and Cyber Warfare in Outer Space' [2019], Space Dossier 3; *See* Mozorova, *supra* 28.

Peaceful use of outer space is generally understood as non-aggressive, rather than non-military, as most states' space programs are linked to some degree with their militaries. For example, early U.S. astronauts and Soviet cosmonauts have been members of their respective countries' armed forces, and GPS is a development of the U.S. Department of Defense.[33]

Second, after national concerns about satellite use for military or sabotage purposes, NATO leaders officially declared outer space an "operational domain" for the alliance.[34] This statement opens many questions related to the possibility of NATO using space weapons with an ability to destroy satellites and missiles. While outer space is not governed by any arms control treaty, several 2019 U.N. resolutions might serve as a vehicle to push for negotiations on disarmament. Although negotiations in the U.N. Committee on Peaceful Uses of Outer Space (COPUOS) on guidelines "for the long-term sustainability of space activities considered but did not adopt proposed guidelines on information-security policies for the terrestrial and orbital parts of space systems" [35], the U.N.G.A. approved in 2019 seven draft resolutions on conventional weapons, and four resolutions on the promotion of transparency and preventing an arms race in outer space.[36] The principles of space law are generally applicable to military operations, with a notable exception found in international telecommunications law. According to the International Telecommunication Union (ITU) Regulations, member states have a wide freedom with regard to military radio installations.

Legal efforts have not kept pace with the rapid development of space

---

[33] NASA, *Global Positioning System History* (updated 7 August 2017), https://www.nasa.gov/directorates/heo/scan/communications/policy/GPS_History.html accessed 24 April 2021.

[34] NATO, 'London Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in London' (3-4 December 2019), https://www.nato.int/cps/en/natohq/official_texts_171584.htm accessed 24 April 2021.

[35] UN COPUOS, Scientific and Technical Subcommittee (55th Session), 'Long-term sustainability of outer space activities', UN Doc A/AC.105C.1/2018/CRP.19 (7 February 2018).

[36] UNGA First Committee (47th Session), 'First Committee Approves 11 Drafts Covering Control over Conventional Arms, Outer Space Security, as United States Withdraws Text on Transparency', https://www.un.org/press/en/2019/gadis3642.doc.htm . A recent attempt to regulate responsible behaviour in outer space was initiated in the UNGA Resolution 'Reducing Space Threats Through Norms, Rules and Principles of Responsible Behaviours' (7 December 2021), UN Doc A/C.1/75/L.45/Rev.1, which seeks to identify current and potential threats to develop "norms, rules and principles of responsible behaviours and on the reduction of the risks of misunderstanding [..] with respect to outer space." See also David P. Fidler, *infra* 44.

technologies.[37] The failure at U.N. level to agree on new legal instruments to regulate "military uses of outer space mirrors similar patterns of division witnessed in other contexts, such as attempts to develop international regulations in cyberspace."[38]

3. Intersections between legal regimes

The traditional power race is reflected both in outer space and cyberspace and determines advanced security risks,[39] such as shutdowns of satellites or their conversion to weapons, multiple use of space objects, and military espionage in space. Given different interpretations of states to relevant terms, the need for cybersecurity standards became an actual concern and a new treaty has been proposed to prevent an arms race and its unforeseen consequences in space.[40]

Both regimes developed before the current commercial opportunities, and struggle to keep pace with technological progress. The OST requires state parties to carry out activities in accordance with international law, including the U.N. Charter, but in the absence of agreed reconciliation rules with *lex specialis,* discretionary application of international law principles is unavoidable. Common challenges of weaponisation in outer space and cyberspace derive from the fact that neither of these ABNJ is governed by an arms control treaty. While application of IHL could be justified by previous affirmations of applicability of general international law in both domains, there

---

[37] The Woomera Manual on the International Law of Military Space Operations, an initiative led by universities in Australia, the U.S. and the U.K. proposes a possible framework of legal rules and norms relevant to military space operations. The Manual aims at clarifying the application of existing international law, especially IHL, to military space activities both during times of rising tension and armed conflict in outer space, *See* https://law.adelaide.edu.au/woomera/ accessed 24 April 2021. Another project was launched at McGill University in 2016, the Manual on International Law Applicable to Military Uses of Outer Space, which also intends to clarify the rules applicable to the military use of outer space by state and non-state actors.

[38] See *infra* 68. In the space realm, states are suspicious of hostile space capabilities, and, indeed, several countries are known to have been experimenting with anti-satellite capabilities and proximity operations against satellites. Disagreements about the role of space objects in military operations exist even among NATO members.

[39] P.J. Blount, 'Peaceful Uses of Outer Space', in Tanja Masson-Zwaan & Mahulena Hofmann (eds.): *Introduction to Space Law* (Kluwer Law International 2019); Matthew T. King, Laurie R. Blank, 'International Law and Security in Outer Space: Now and Tomorrow' [2019], 113 Ajil Unbound.

[40] Proposed Prevention of an Arms Race in Space (PAROS) Treaty (*NTI Blog*, 5 April 2021), https://www.nti.org/learn/treaties-and-regimes/proposed-prevention-arms-race-space-paros-treaty/ accessed 25 April 2021.

is only one international instrument that expressly mentions the application of IHL to outer space, i.e., the Convention on the Prohibition of Military or any other Hostile Use of Environmental Modification Techniques.[41] In both areas, determination of the use of force is closely linked to a physical destruction. An important step will be determining the scope of "peaceful purposes" in space, and the principles applicable to an attack, such as distinction.[42]

The cyber realm has some unique particularities in this regard: while it is not a physical ABNJ, it includes physical hardware and state jurisdiction applies to hardware, software, and actors.[43] Moreover, most sovereignty questions related to cyberspace ultimately refer to liability issues and not to consumable resources, like in outer space.[44] Territoriality and sovereign claims are not part of the outer space or cyberspace vocabulary, with the exception of the above-mentioned cases of national sovereignty violations by cyber means. However, Rule 1 of the first Tallinn Manual, entitled "Sovereignty", which is often overlooked, mentions states' inability to control or limit cyberspace as a whole, and it to oceans and outer space. Suggesting that cyberspace can also be integrated into the *res communis* category highlights the distinction that should be made between cyberspace and the objects or private services that function within it, very similar to outer space.

Enforcement of international law is weakest with respect to cyberspace, especially as its application is not monitored by a specialized international organization or an international tribunal. Violations of international law applicable to cyberspace are rarely solved within a single area of law, as the cyber domain lacks domain-dedicated treaty law, state practice, and *opinio juris*.

II. International law questions regarding cyber operations on space

[41] Convention on the prohibition of military or any other hostile use of environmental modification techniques (adopted 10 December 1976), Ch_XXVI_1: 26.1, https://treaties.un.org/doc/Treaties/1978/10/19781005%2000-39%20AM/Ch_XXVI_01p.pdf accessed 25 April 2021.

[42] Dale Stephens, 'The International Legal Implications of Military Space Operations: Examining the Interplay between International Humanitarian Law and the Outer Space Legal Regime' [2018] 94 Int'l L. Stud. 75.

[43] Observers of "de-territorialization" in cyberspace, the law of the sea, and environmental law, claim that law is increasingly detached from territory and should instead pursue a functional, global order, which promotes fundamental human values, and accommodates pluralism and cultural diversity. Unsettled boundaries are relevant for several environmental liability and other legal issues. *See* Lorenz Langer, 'The South China Sea as a Challenge to International Law and to International Legal Scholarship' [2018] 36 Berkeley J. Int'l L. 362.

[44] Kristen Eichensehr, 'The Cyber-Law of Nations' [2015], 103 Geo. L.J. 317.

related infrastructure

In the early beginnings of space missions, states envisioned outer space as an area free of armed conflict. Soon, legal, military, and security implications of space activities became more obvious as warfare increasingly shifted from physical to virtual realms, which made cybersecurity and space security inextricably linked. Internet networks rely on space-enabled communication and information services, but the corollary is use of internet-based networks for the operation of space objects, including satellites. Both state and commercial space activities use these technologies and are vulnerable targets for political, economic cyber espionage, and cybercrime.[45]

A key difficulty to assess the applicable international legal regime on cyber operations against space objects relies in the different stages of development of both regimes. "Space law" is a distinct body of international law which addresses *ratione geographiae* all major aspects of outer space, comprises five treaties adopted under the auspices of the U.N. and numerous other norms and interpretations provided by the U.N. COPUOS, a permanent committee of the U.N.G.A. The cornerstone of the applicable legal regime, the 1967 Outer Space Treaty, is considered to represent customary international law, whereby it provides the legal framework for all activities in or directed at, the realm of outer space.[46] Nevertheless, this treaty generally encompasses vague provisions and provides no explicit prohibition against launching attacks against outer space objects, through cyber means or otherwise. On the other end of the spectrum, the legal regime applicable to cyber operations is fragmented, it does not include any treaty providing a generally accepted overarching framework applicable to state-sponsored cyber-operations[47] and an insignificant body of customary international law.

Satellite cybersecurity "encompasses the satellite itself, transmissions to and from Earth, and ground stations."[48] Communication between the ground

---

[45] David P. Fidler, '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 accessed 24 April 2021.

[46] Frans G. von der Dunk, 'Armed Conflicts in Outer Space: Which Law Applies?' [2021] 97 Int'l L. Stud. 188, 191.

[47] In the cyberspace context, the most relevant regulatory instrument is the Budapest Convention on Cyber-crime, the only binding multi-lateral instrument in force. Mainly covering criminal justice issues, this instrument is not applicable to state actors. *See* https://www.coe.int/en/web/cybercrime/the-budapest-convention accessed 24 April 2021

[48] See David P. Fidler, *supra* 44. Outer-space infrastructure is separated into three primary segments: the space segment, the user segment, and the ground segment. There are

control on earth and space objects, including satellites, are ensured by wireless signals, also known as radio communication. Given that software lies at the heart of all complex space systems, both space-based and ground-based space components are vulnerable to cyber operations. These can enable unrightful access and collection of satellite information, disruption of the transmission of information or hack (manipulate or destroy) a satellite's computer software and hardware, or weaponise it.[49]

Cyber operations against radio signals or services are generally referred to as "interference", although no commonly agreed term exists to date.[50] Satellites could be targeted through electronic warfare, such as jamming and spoofing, microwave weapons, laser dazzling and even cyberattacks. A particular vulnerability is present in case of Global Navigation Satellite Satellites (GNSS). These assets are of crucial importance "for military operations, for critical national infrastructure and key economic sectors"[51], such as communications, emergency services, energy, finance, national defence, food and agriculture, weather forecasting, air-, road-, rail-, and marine positioning, navigation and transport. Jamming refers to deliberate or unintentional interference with radiofrequency communication transmitted to or by GNSS, by altering the signals receiver and causing temporary, usually reversible, disturbance and disruption. These operations primarily target civil GPS signals, as military signals are more robust.[52] Spoofing refers to actions of deluding a GNSS receiver by transmitting incorrect signals or rebroadcasting genuine signals captured at a different time or location, i.e., by imitating the characteristics of a genuine signal so that the user receives the modified signal instead of the authentic one.[53] A common example is hijacking a satellite

generally five types of systems that are common for any satellite architecture. These include an onboard computer system (OBCS), actuators, sensors, a power system and a communications system. *See* Gregory Falco, 'When Satellites Attack: Satellite-to-Satellite Cyber Attack, Defense and Resilience' [2020], ASCEND 2020 The American Institute of Aeronautics and Astronautics.

[49] *Id.*

[50] *See* definition at *infra* 79 and *infra* 56.

[51] See Baumann at *infra* 58.

[52] Mohamed Tamazin et al., 'GNSSs, Signals, and Receivers' in Rustam B. Rustamov and A. M. Hashimov (eds.), *Multifunctional Operation and Application of GPS* (*Intechopen* 2018).

[53] See Baumann at *infra* 58. Although cyber means are presently more preferred means of interfering in satellite operations, they are built on older strategies such as radiofrequency interference. *See* Intertanko, *Jamming and Spoofing of Global Navigation Satellite Systems (GNSS)* (2019) https://www.maritimeglobalsecurity.org/media/1043/2019-jamming-spoofing-of-gnss.pdf accessed 24 April 2021.

command and control and feeding it with fake data.

1. Cyber operations on space objects which rise to the threshold of use of force

This section refers to the application of existing legal regimes to potential or actual armed conflicts, more specific to space activities undertaken for strategic, security, or military purposes, either in support of terrestrial operations or as independent activities with their own purposes in outer space. Cybersecurity conversations have long overlooked space activities' vulnerability to cyberattacks[54] and convergence of the agendas of the U.N. GGE on outer space and the GGE on cyberspace still seems to be a distant goal.

In 2019, a Group of Governmental Experts (GGE PAROS)[55] discussed the variety of possible threats to outer space activities and addressed for the first time the issue of cyberattacks on space objects. Without reaching any consensus, the GGE concluded that although the applicable legal instrument is the OST, this treaty lacks absolute prohibitions required to protect such assets and offers little clarification on the consequences of violation.[56] An interesting observation is that GGE PAROS refrained from analysing the applicability of IHL to outer space, expressing concern that this could suggest a tacit approval of conducting armed conflict in outer space.[57]

Nevertheless, it is currently widely accepted that application of general international law to outer space, as prescribed by Article III OST includes the relevant IHL regime. Article III expressly provides for compliance of space activities with international law and the U.N. Charter, therefore, including the baseline prohibition on the use of force and its two principal exceptions found in Articles 42, 51, and 53. Although territorial sovereignty is not an inherent part of the space law vocabulary, by virtue of Article II OST, similar to registered ships and aircraft, Article VIII of the OST and the Registration Convention confer a

---

[54] Beyza Unal, 'Cybersecurity of NATO's Space-based Strategic Assets' (2019) Chatham House Research Paper https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf accessed 24 April 2021.

[55] Press release UN Office for Disarmament Affairs 'Group of Governmental Exerts on further effective measures for the prevention of an arms race in outer space', https://www.un.org/disarmament/topics/outerspace/paros-gge/ accessed 21 April 2021.

[56] UNGA (47th session) 'Group of Governmental Experts on further practical measures for the prevention of an arms race in outer space' UN Doc A/74/77 (9 April 2019), https://undocs.org/A/74/77 accessed 24 April 2021.

[57] Mike D. Bilodeau, 'The risk that Cyber-attacks pose to Outer Space Assets: How can international dialogue and cooperation help?' (2019) Thesis submitted to McGill University, Institute of Air and Space Law.

territorial protection to registered space objects. The difficulties that arise regard whether space objects represent legitimate targets for the use of force and whether other domain-specific rules, such as the immunity of warships, can be translated to the space realm.

Qualifying a hostile cyber operation (or a threat with such an operation) against a satellite as an illegal use of force or a threat with use of force, is a complex task which needs to be considered on a case-by-case basis. Although cyber-weapons don't fall into the category of traditional weapons, the scale and effects of cyber operations can cause effects "comparable to non-cyber operations rising to the level of a use of force"[58]. The Tallinn Manual provides some guidelines for this assessment, explaining in Rule 69 that "in the cyber context, it is not the instrument used that determines whether the use of force threshold has been crossed, but rather (…) the consequences of the operations and its surrounding circumstances." Therefore, qualifying a cyber-operation as an expression of the use of force shall take into account the severity, immediacy, invasiveness of the operation and an assessment of the effects.[59] Article 36 of AP I to the 1949 Geneva Convention provides for states' obligation to conduct a review prior to the development and deployment of new weapons, understood in their widest sense[60], to ensure that the new weapon complies with IHL principles. The interpretation of the principles of discrimination, proportionality, and precaution already proved to be extremely challenging when referring to cyberattacks on terrestrial assets.

Assessing compliance of cyberattacks on outer space objects with these principles is even more complex, as most targets, such as GNSS, serve both military and civilian purposes. First, the potential reverberating effects of cyberattacks on space objects, such as satellites, are still unknown and current technological limits permit an element of surprise, as the exact functions of satellite are often unknown by the attacker. Second, although the number of satellites is growing, these often serve double purposes – such as aerial imaging for military exercises, but also for disaster (flood, hurricane) mitigation[61]. A

[58] See Tallinn Manual, Rule 69.
[59] Ingo Baumann, 'GNSS Cybersecurity Threats: An International Law Perspective' (*Inside GNSS*, 3 June 2019), https://insidegnss.com/gnss-cybersecurity-threats-an-international-law-perspective/ accessed 24 April 2021.
[60] ICRC, 'Commentary to Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977' https://www.loc.gov/rr/frd/Military_Law/pdf/Commentary_GC_Protocols.pdf accessed 24 April 2021.
[61] *See* Baumann *supra* 58.

cyberattack against a legitimate military target could potentially have significant and immediate destructive, often indirect effects, on large civilian populations, such as power cuts to medical facilities, interruption of water management, disturbance to civilian air traffic control, and therefore distinction and proportionality assessments required before attacking dual-use objects in space present significant challenges.[62] Although a satellite with dual purposes would be a military objective by virtue of its nature, location, purpose, or use, the indirect effects of its malfunction may complicate the proportionality assessment.[63] Consequently, the threshold for an armed attack, paired with the victim state's right to self-defence is subject to individual consideration and analysis. The majority view is that "GNSS "jamming and spoofing are clear cases of interference, since these cause performance degradation, misinterpretation, or loss of information."[64] As described below, this language is also reflected in the ITU's legal framework regarding harmful interference.

Another relevant factor for assessing the effects of hostile cyber operations against GNSS is the reversibility of the temporal and geographical effects of the operation. Minor degradation of service or limited "interruption of non-essential services would usually not qualify as an armed attack"[65]. The analysis becomes relevant in cases when jamming or spoofing occurs against satellites that serve essential infrastructure "in a manner that causes severe effects on national security, economy, public health, traffic safety, or environment".[66]

While Article III OST is able to project various international law rules of into outer space, in the absence of an agreed legal regime, there is a risk of "cherry-picking" convenient legal provisions.[67] For example, a state might publicly regard satellite jamming as an armed attack in order to ensure future legitimization of exercising the right of self-defence, or to the contrary, adopt a public position that satellite jamming does not amount to a use of force, in order to create legal fragmentation and justify its own potential interference with

---

[62] Jack M. Beard, 'The Principle of Proportionality in an Era of High Technology' in Christopher M. Ford and Winston S. Williams (eds.), *Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare* (OUP 2018).

[63] *Id.*
[64] See Baumann, *supra*58.
[65] *Id.*
[66] *Id.*
[67] Hitoshi Nasu, 'NATO Recognizes Space as an "Operational Domain": One Small Step Toward a Rules-Based International Order in Outer Space' (*Just Security*, 4 March 2020) https://www.justsecurity.org/68898/nato-recognizes-space-as-an-operational-domain-one-small-step-toward-a-rules-based-international-order-in-outer-space/ accessed 21 April 2021.

foreign satellites. A homogenous understanding of legal qualifications, thresholds, and applicable responses is critical among NATO members, in order to define collective self-defence scenarios able to trigger Article 5 of the North Atlantic Treaty.

The importance of clearly assessing whether a cyberattack on a satellite falls into the scope of Article 2(4) is relevant for determining whether this action would trigger the right to self-defence. In a view expressed by the U.S. Air Force, the right to self-defence is generally applicable in the context of hostile cyber operations against space objects.[68] Even when the "source of the attack can be located and attributed to a state, additional conditions must be fulfilled for the exercise of self-defence".[69] The attack must still be ongoing and the conditions of proportionality and necessity for repelling of an armed attack must be met. Whenever a hostile cyber operation does not reach the threshold of an armed attack, victim states can resort to countermeasures or measures compatible with the plea of necessity.

The principle of proportionality of a self-defence response to an armed attack on a space objects, such as a satellite, can be particularly challenging when a counterattack targets a terrestrial asset of the attacker instead of, or in addition to, its space objects. Nevertheless, many scenarios present complex features which complicate their legal framing, such as for example, disruption of satellite communication in support of air traffic control towers, which can disturb data on airplane traffic and navigation, and may ultimately cause accidents and even loss of life.[70]

If the U.N. Security Council determines that hostile cyber operations against satellites represent a threat to peace, a breach of peace or an attack, it can take measures to preserve or restore international peace and security under Chapter VII of the U.N. Charter. These measures could also include cyber operations.[71]

After NATO officially declared space as its fifth operational domain along air, land, sea and cyberspace, the international legal community started to

---

[68] See Baumann, *supra* 58; See also Sandra Erwin, 'Sorry sci-fi fans, real wars in space not the stuff of Hollywood' (*Spacenews*, 2 January 2018), https://spacenews.com/sorry-sci-fi-fans-real-wars-in-space-not-the-stuff-of-hollywood/ accessed 21 April 2021.
[69] See Baumann, *supra* 58.
[70] Deborah Housen-Couriel, 'Cybersecurity threats to satellite communications: Towards a typology of state actor responses' [2016] 128 Acta Astronautica, 409, 411.
[71] *See* Baumann, *supra* 58.

speculate on a possible application of Article 5 of the North Atlantic Treaty. Until the 2021 NATO Summit in Brussels, when the Alliance recognized the application of the collective defence clause to attacks to, from or within space[72], no public document clarified whether an invocation of the collective defence clause in outer space is possible. First, the language used in Article 5 refers to geographical application i.e. "The Parties agree that an armed attack against one or more of them *in Europe and North America*", corroborated with the territorial protection to registered space objects conferred by Article VIII OST detailed above, would suggest that targeted national space capabilities can fall under the scope of Article 5. Similar to cyberspace, sovereign rights of states over their national infrastructure may include outer space architecture, which, in consideration of the previously exposed IHL rules, may represent military targets. Another analogy with cyberspace is the absence of any territorial boundaries of both domains (cyberspace and outer space), which didn't preclude an extension of applying Article 5 in cyberspace, considering jurisdictional rights of states over distant cyber capabilities. Second, another question is whether cyberattacks on NATO members' space capabilities are already covered by Article 5. NATO leaders agreed in the Wales Summit Declaration in 2014 that a cyberattack could trigger, under certain conditions, the collective defence clause. Therefore, there is no reason why cyberattacks on national space architecture should not be included in this mechanism.

Geographical considerations may be problematic. As mentioned, when referring to application of international law to cyberspace, a difficult question is whether a hostile cyber-operation is required to have direct kinetic consequences on space objects in order to be considered as an armed attack. Moreover, extension of the scope of Article 5 beyond kinetic attacks on space objects might be questionable, as Article 6 only refers to armed attacks over allied territory, or on their forces, vessels, or aircraft of any of the Parties. Nevertheless, invocation of Article 5 in response to a cyberattack "would be taken by the North Atlantic Council on a case-by-case basis".[73]

---

[72] NATO, 'Brussels Summit Communiqué, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 14 June 2021, https://www.nato.int/cps/en/natohq/news_185000.htm, accessed 17 Septmeber 2021.

[73] NATO, 'Wales Summit Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales" (05 September 2014) https://www.nato.int/cps/en/natohq/official_texts_112964.htm?mode=pressrelease accessed 24 April 2021. For further discussions of applicability of the collective defense clause, *See* Cornelia A. Baciu, 'Collective security and Art. 5 in space: Jus gentium, oversight, resilience

If hostile cyber operations against satellites are considered as a threat or use of force in accordance with Art. 4 (2), states' right to self-defence is not limited to only cyber operations, but these hostile acts can also trigger countermeasures or reprisal by the victim state. As currently outer space is still dominated by the presence of states and less by private actors, countermeasures seem a feasible response to low impact hostile cyber operations on satellites. Regarding the possibility of using countermeasures in response to hostile cyber operations against space objects, a U.S. Air Force official stated that "below an armed attack, the most applicable response is a countermeasure".[74]

Countermeasures can of course include hostile cyber operations, such as jamming or spoofing GNSS signals of the attacking state. As the existence of an obligation to provide prior notice before responding with countermeasures is still debated in relation to the cyber realm, an issue on which the Tallinn Manual is also silent, another open question is whether countermeasures involving cyber operations on satellites are subject to the obligation of notification and if the victim state is under the obligation to offer negotiations. The majority view endorses this obligation.[75]

As countermeasures may only be taken against states, though states may also be responsible for acts of non-state actors, comprehensive assessment of the oversight duty, including the due diligence principle, is of particular concern. The creation of robust space attribution process is not a main focus of current space strategies and policies. Therefore, lacking the ability to trace the origin of hostile actions in space hinders the ability to respond appropriately and lawfully.[76]

In absence of a clear prohibition on cyberattacks on outer space objects, clarification of permissible conduct and commonly used terms would be useful. Lessons learned could perhaps be drawn from aviation cyber policy,

---

and the role of NATO' (*Atlantic Forum*, 2020), https://www.atlantic-forum.com/content/collective-security-and-art-5-space-jus-gentium-oversight-resilience-and-role-nato and Aurel Sari, NATO in Outer Space: A Domain Too Far? (*Articles of War,* 1 October 2020) https://lieber.westpoint.edu/nato-outer-space/ accessed 21 April 2021.

[74] *See* Housen-Couriel, *supra* 69.

[75] *See* Baumann *supra* 58. Of course, countermeasures may also be employed in response to hostile cyber operations against satellites if these violate any other international obligation and therefore represent an internationally wrongful act.

[76] John Klein, 'To deter attacks on satellites, U.S. needs a strategy to identify bad actors' (*Spacenews*, 5 June 2020), https://spacenews.com/op-ed-to-deter-attacks-on-satellites-u-s-needs-a-strategy-to-identify-bad-actors/ accessed 21 April 2021.

where non-binding provisions are broadly applied.[77] In cases of jamming or spoofing, the International Civil Aviation Organization (ICAO) recommended States to collaborate with the ITU and other appropriate U.N. bodies to create procedures of addressing specific cases of harmful interference of GNSS signals.[78]

2. Cyber operations on space objects which do not rise to the threshold of use of force

The legal regime applicable to hostile cyber operations against satellites, which do not reach the level of the use of force, is associated with international telecommunications law, mainly comprising regulations for the registration of satellite network frequency assignments and their use, adopted under the auspices of the International Telecommunication Union (ITU)[79]. The main instruments are the 1992 ITU Constitution, the 1992 ITU Convention, and the 2016 Radio Regulations.

The functioning of GNSS relies on dedicated radio frequencies, being "limited natural resources", according to Art. 44 (2) of the ITU Constitution, which "must be used rationally, efficiently and economically". Radio frequencies are governed and allocated by the ITU and its legal framework. Under Art. 45 (1) of the ITU Constitution these "must be established and operated in such a manner as not to cause harmful interference to the radio services or communications of other Member States". Nevertheless, although Article 45 prohibits harmful electromagnetic interference, it does not prohibit unauthorized cyber activities. Moreover, the applicable body of law only regulates the use of the radio frequencies, but not the information that is

---

[77] *See* Bilodeau *supra* 56.

[78] *See* ICAO 'Recommendation 6/7 on assistance to States in mitigating GNSS vulnerabilities' (2012), 12th Air Navigation Conference, at 2.1.4. Moreover, even binding instruments such as the Chicago Convention, contain recommendations that "each Contracting State should develop measures in order to protect information and communication technology systems used for civil aviation purposes from interference that may jeopardize the safety of civil aviation." *See* Annex 17 to the Convention on International Civil Aviation: Security: Safeguarding International Aviation Against Acts of Unlawful Interference (ICAO, 10th Edition, April 2017) at 4.9.; *See* also Bilodeau *supra* 56.

[79] The ITU is a specialized UN agency for information and communication technologies, which regulates the use of radio frequencies, by allocation and assignment of segments of the spectrum to different services. Although ITU is a strong actor in the fight against cybercrime, the work of agency focuses on norm-setting and capacity building regarding outer space and cyberspace, and not on creating binding obligations on states. *See* Baumann *supra* 58.

transmitted.[80]

Without specifically distinguishing between deliberate and unintentional harmful interference, the ITU Radio Regulations define harmful interference as "interference[81] which endangers the functioning of a radio navigation service or of other safety services or seriously degrades, obstructs, or repeatedly interrupts a radio communication service operating in accordance with Radio Regulations."

A clear expression of the principle of due diligence can be found under Article 15 (4) of the ITU Constitution, which provides that "It is essential that Member States exercise the utmost goodwill and mutual assistance in the application of the provisions of Article 45 of the Constitution and of this Section to the settlement of problems of harmful interference."[82] The ITU Radio Regulations provide an obligation for states to halt harmful interference to space stations belonging to other countries, independent of whether the interference is caused by public or private stations.[83]

Liability for hostile cyber operations against space objects, damages, and possible sanctions

The legal regime applicable to cyber operations targeting space architecture is unsettled and such actions do not qualify as "space activity" and do not fall under the scope of Articles III and VI OST. Article VI OST, imposing state oversight over private actors, is another expression of the due diligence principle, as it provides "that states bear international responsibility for national activities in outer space, including the Moon and other celestial bodies,

---

[80] Martha Mejía-Kaiser, 'Space Law and Unauthorised Cyber Activities' in Katharina Ziolkowski (ed.), *Peacetime Regime For State Activities In Cyberspace*, (NATO CCD CoE Publication, 2013) 349, 355.

[81] The Radio Regulations (RR) represent a binding treaty on radiocommunication and orbital frequencies. According to Art 1.166 of the ITU RR, interference means: "The effect of unwanted energy due to one or a combination of emissions, radiations, or inductions upon reception in a radio communication system, manifested by any performance degradation, misinterpretation, or loss of information which could be extracted in the absence of such unwanted energy".

[82] In case of disagreements, the Radiocommunication Bureau can provide assistance upon request, by supporting the identification of "the source of the interference and *See* k the cooperation of the responsible administration in order to resolve the matter" (Article 13 RR). Although the Radio Regulations Board (RRB) can intervene upon request, it had no power to enforce any measures or sanctions in case of intentional harmful interference, such as for e.g. when Iran caused harmful interference to communications satellites operated by EUTELSAT in 2012.

[83] See Baumann at *supra* 58.

whether such activities are carried on by governmental agencies or by private entities". Therefore, states have the primary international responsibility to authorize and continuously supervise activities carried out in outer space by their governmental and non-governmental institutions. Sole violation of these supervision obligations triggers the secondary international responsibility of states, i.e., to respond the international community through compensation or sanctioning responsible individuals.[84]

As a general rule, a launching state is internationally liable for damage caused by space objects under its jurisdiction on Earth, in air space, or in outer space. This rule is only relevant to military operations in peacetime and does not apply to armed conflicts.[85] The jurisdiction over space objects is prescribed in accordance with Article 1(c) of the Liability Convention, which defines the term "launching State". The applicability of the Liability Convention, that addresses damage and compensation, has a limited application, as it applies only to *damage* caused *by* space objects[86]. Therefore, state liability for causing *loss of service to* a space object is more problematic. The rules applicable to the payment of damages are not applicable to the use of the radio-frequency spectrum or regarding direct damages caused by hostile cyber activities against a space object, resulting in loss of service or loss of the space object itself.[87] However, as the Liability Convention covers physical damage caused by space objects due to unlawful cyber activity, it may nevertheless apply to indirect damage arising from direct physical damages caused by another space object or parts thereof, such as a satellite, which provoked the damage due to a malfunction in the aftermath of a cyber-operation. If the cyberattack ultimately causing damage to a foreign space object is perpetrated under the sovereign control of the first state, this state is responsible for the hostile cyber activity. In the scenario when the attack cannot be attributed to the state which owns the destructive space object, Article 1(c) of the Liability Convention conditions liability on the proof of fault. In the absence of binding space traffic rules, fault can be proven either by violation of a protective rule,

---

[84] *See* Mejía-Kaiser *supra* 79, at 356. Some countries adopted national space legislation to implement the obligation of authorization and continuous supervision of private entities, provided in Article VI OST.

[85] *See* Morozova, *supra* 28.

[86] According to Article 1(d), "space objects include component parts of a space object as well as its launch vehicle". Article 1(a) of the Liability Convention defines the term damage as "loss of life, personal injury or other impairment of health; loss of or damage to property of States or of persons, natural or juridical, or property of international intergovernmental organizations"

[87] *See* Mejía-Kaiser *supra* 79, at 360.

or an intentional or negligent act that caused the damage.[88] The principle of due diligence is therefore an important scale in assessing states' negligent actions or omissions to thwart or stop hostile cyber interference with its own national space objects, which are able to cause damage to foreign space architectures as a result of a cyber-operation. If a hostile cyber act was at the origin of a chain of events that eventually caused physical damage to space objects of another state, the responsible state, whether directly or by failing to exercise proper control over its actors, should be liable for the damage caused.[89]

The possibility of expanding the scope of states' international responsibility and liability under the Liability Convention, by including damage caused by hostile disruption to satellite transmissions was already raised in the U.N. COPOUS.[90] The same expansive interpretation of Article VII OST is embraced by the 2014 EU Draft Code of Conduct for Outer Space Activities and advocated by various scholars.[91] This interpretation would assimilate satellite transmissions and data as "property" of a state or private actor, performing an activity attributable to a state. The expansion of the Convention's concept of "loss or damage to property" is supported by precedents, such as in application of the World Intellectual Property Organization (WIPO) Convention to satellite transmissions, where these are perceived as assets capable of bearing proprietary rights.[92]

A relevant distinction is between the scenarios described above, when damages to space objects as a result of cyber interference with a space object are caused in outer space or in flight, and cases when damages result on Earth. In the latter case, Article 2 of the Liability Convention prescribes absolutely liability to the launching state to pay compensation for damages "caused by

---

[88] *Id.* at 364.
[89] *Ibid*.
[90] 'Report of the Chair of the Working Group on the Status and Application of the Five United Nations Treaties on Outer Space' (12 April 2016) UN Doc A/AC.105/C.2/2016/TRE/L.1.
[91] *See supra* 72. The European Union's Draft International Code of Conduct for Outer Space Activities is a nonbinding soft-law instrument attempting to establish norms of responsible behaviour in outer space activities. So far, the Code failed to gain support from the international community and received mixed reviews, available at https://eeas.europa.eu/sites/default/files/space_code_conduct_draft_vers_31-march-2014_en.pdf ; *See* also Almudena Azcárate Ortega, 'Placement of Weapons in Outer Space: The Dichotomy Between Word and Deed' (Lawfare Blog 28 January 2021), https://www.lawfareblog.com/placement-weapons-outer-space-dichotomy-between-word-and-deed accessed 24 April 2021 and Jack Beard, *supra* 29.
[92] *See* Housen-Couriel *supra* 69 and accompanying footnote 44.

its space object on the surface of the Earth or to aircraft in flight" and requires no proof of fault.

On a regional level, the European Union addresses with the 2014 EU Cyber Defence Policy Framework the protection of satellite and terrestrial communications in the context of Common Security and Defence Policy actions. In this respect, the 2017 Cyber Diplomatic Toolbox enables the EU to apply sanctions against individuals responsible for cyberattacks, including a potential cyberattack against a European satellite.[93]

III. Relevant impacts for NATO and concluding thoughts

Legal and technological intersections between outer space and cyberspace materialized in activities that cross both realms, but sometimes strengthen their interdependence.[94] The greatest concern are low-level operations, such as jamming and spoofing of GNSS signals, which often do not result in significant damages to satellite systems, but very likely impact critical national infrastructures. Although the ITU body of law provides for states' obligation to thwart harmful interference, the ITU can hardly enforce these obligations and prevent intentional harmful interference.

Although Article VIII OST provides for state jurisdiction over space objects, the lack of explicit internationally binding rules and prohibitions clearly opens controversial interpretations of existing positive law. The interpretation of the universal principle of national sovereignty is subject to adjustment depending on the specifics of each domain,[95] whereas the sliding scale of due diligence standard of review is based on area-specific factors, and the only constant standard is the due diligence standard of conduct.[96]

---

[93] There is no dedicated EU legislation or policy to regarding cybersecurity of space systems. In 2019, the European Union (EU) established a sanction regime against cyberattacks in the broad sense, passing Council Decision (CFSP) 2019/797 and Council Regulation 2019/796, but the success of the new EU sanctions regime and its deterrence power are still to be tested. EUISS, *Guardian of the Galaxy. EU cyber sanctions and norms in cyberspace* (Patryk Pawlak and Thomas Biersteker eds., 2019), Chaillot Paper 155.

[94] Steven Freeland, 'The limits of law: challenges to the global governance of space activities' [2020] 153 Journal & Proceedings of the Royal Society of New South Wales, 70, 72.

[95] Corn and Taylor, *supra* note 5.

[96] The preventive principle in cyberspace operates differently from the environmental arena, where it derives from the "no harm" principle and refers to states' duty not to cause significant transboundary damage to the environment of another state. As it includes the obligation to undertake preventive measures to regulate third party pollution, this principle it is often more transparently manifested regarding environmental protection and responsibility is often easier to allocate. State authorization and supervision of private activity, also included

Policymakers and scholars disagree on the means of reaching legal clarity, and many fear risks of overlap and confusion. While some propose new instruments able to address the rapid changes, others prefer operationalization of existing rules and an adapted interpretation. Moreover, opinions are divided between the necessity of adopting legally binding measures and the sufficiency of voluntary transparency and confidence-building measures (TCBMs) on issues such as unauthorised cyber activities against space objects, international responsibility and liability of states that authorise or tolerate hostile cyber activities.

A solution-oriented implementation of NATO's space policy and strategy can better be achieved if interpretation of key concepts and general principles on space cybersecurity is clarified at least among the Alliance's members. Several States have already outlined their cybersecurity priorities regarding outer space and space-derived data, including the U.S. and the UK. [97] Lack of consensus and gaps in existing global mechanisms hamper not only planning and execution of NATO operations, but also allow third states to opt for broad interpretation of key terms of the OST and applicable international law, such as "peaceful use", "space weapon", and understanding of the thresholds when jamming, spoofing, and satellite destruction amount to a use of force. Increased presence of non-state actors in outer space requires new assessment of state responsibility, the nature of the due diligence principle, and a homogenous understanding of critical infrastructure.

So far, the biggest space faring nations "have not agreed on how to approach cybersecurity or address military activities in space" and diplomatic activities on space and cybersecurity "concluded without addressing space cybersecurity."[98] NATO members can undertake a comprehensive and integrative multi-stakeholder review of the measures available under international law in response to hostile acts directed at satellites and satellite transmissions.[99] NATO's coordination and mediation role between Europe and the U.S. and between state and private actors cannot be stressed enough in

---

in the OST, represents a pure oversight duty, and strongly depends on the capabilities of each state. *See* Scott J. Shackleford et. al., 'Unpacking the International Law on Cybersecurity Due Diligence: Lessons From the Public and Private Sectors' [2016] 17 Chi. J. Int'l L. 1.

[97] US Space Policy Directive 5 'Cybersecurity Principles for Space Systems' (4 September 2020) https://www.federalregister.gov/documents/2020/09/10/2020-20150/cybersecurity-principles-for-space-systems accessed 21 April 2021.

[98] See David P. Fidler *supra* 44.

[99] *See* Housen-Couriel *supra* 69.

almost every conversation about space security.[100] In this regard, the NATO Space Centre at Allied Air Command in Ramstein will play a crucial role.[101]

Although NATO does not possess its own satellites, it has a memorandum of understanding in place with Allies for use and access to their satellite capabilities. NATO as an Organisation and its member states depend on space-based systems for positioning, navigation and timing, early warning, environmental monitoring, secure satellite communications, and intelligence, surveillance and reconnaissance[102]. Although the work of the relevant U.N. GGEs does not intersect, this does not hinder NATO nations to agree among themselves on common understanding of applicable international law. In this regard, instead of focusing on the interpretation of Article 5, another possible approach to most recent Anti-satellite weapons ASAT tests and threats could be invoking Article 4 of the North Atlantic Treaty.

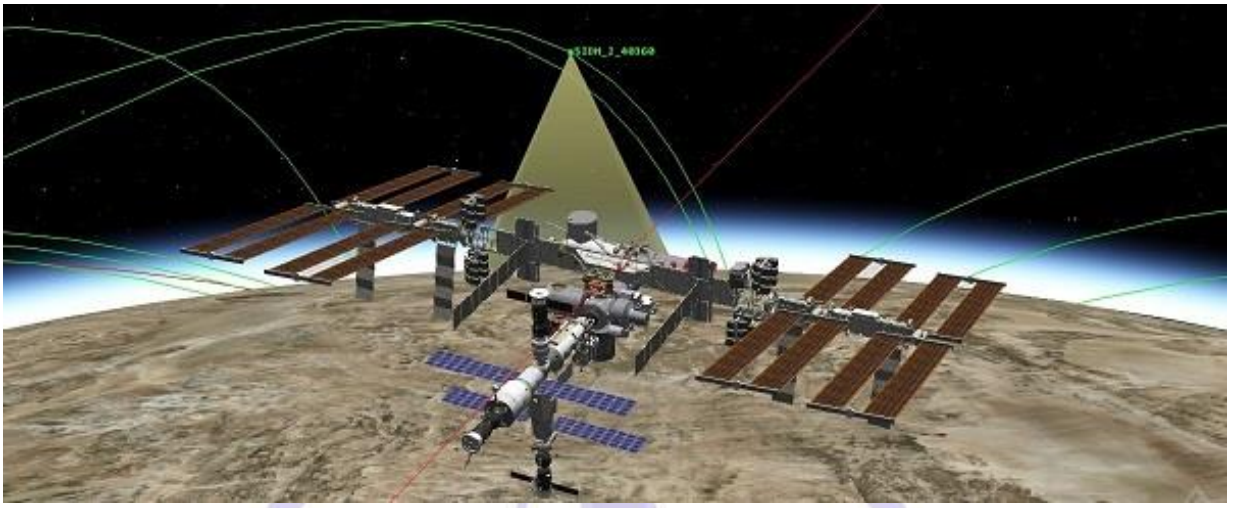
At the 2021 NATO Summit in Brussels, the Alliance recognized the application of the collective defence clause in Article 5 of the founding treaty to outer space, i.e., to attacks to, from or within space. Besides recognizing these operations as clear security threats to NATO and its members, in addition to traditional military attacks taking place on land, sea, in the air, and more recently, in the cyber domain, this important agreement highlights that NATO members realize the crucial role of space capabilities and the value of protecting and defending these key capabilities.

***

[100] Online event 'The future of US security in space' at https://www.atlanticcouncil.org/event/the-future-of-us-security-in-space/, accessed 25 April 2021.

[101] NATO, 'The Secretary General's Annual Report 2020' (16 March 2021) https://www.nato.int/nato_static_fl2014/assets/pdf/2021/3/pdf/sgar20-en.pdf; NATO, 'NATO 2030: United for a New Era Analysis and Recommendations of the Reflection' (25 November 2020) https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf

[102] 'NATO's approach to space' (22 April 2021) https://www.nato.int/cps/en/natohq/topics_175419.htm , accessed 24 April 2021. Reports show persistent jamming activities against civilian GPS signals under the jurisdiction of NATO members, including during NATO's 2018 Trident Juncture exercise. *See* Unal *supra* 53.



Source : https://ac.nato.int

Legal Solutions for the Peaceful, Sustainable and Strategic Utilization of Lunar Resources[1]

by Avv. Antonino Salmeri, Adv. LL.M[2] and Mr. Antonio Carlo[3]

Introduction

The utilisation of space resources holds the potential to significantly impact the future of space exploration by providing critical support for safe and sustainable operations.[4] Above all, the use of space resources will both reduce the costs and increase the scalability of activities on another celestial body, thus marking a new strategic dimension of space missions. Thanks to its favourable environmental conditions and significant availability of crucial resources such as hydrogen and oxygen, an unprecedented global interest in the Moon has dramatically surged.[5] Accordingly, our natural satellite is currently

[1] **DISCLAIMER**: The views expressed in this article are solely those of the authors and may not necessarily represent the views of NATO, Allied Command Operations, or Allied Command Transformation, or of their affiliated organizations.

[2] Doctoral Researcher in Space Law at the University of Luxembourg and registered attorney at the Italian BAR, antonino.salmeri@uni.lu

[3] PhD Candidate at Tallinn University of Technology, ancarl@taltech.ee

[4] Jim Brindestine, 'Space Resources Are the Key to Safe and Sustainable Lunar Exploration' (*NASA*, 10 September 2020).

[5] David Kornuta, Angel Abbud-Madrid & *et al*., 'Commercial lunar propellant architecture: A Collaborative Study of Lunar Propellant Production', (2010) 13 REACH 1 – 79.

being considered by public and private actors as the first target for the development and testing of innovative technologies for the use of space resources *in-situ*.[6] The combination of the scientific and cultural importance of the Moon with the abovementioned strategic advantages makes the competition for lunar resources a matter of high geopolitical interest.[7] In light of the unprecedented challenges brought by these activities, it is clear that the current system of international space law needs new solutions[8] to complement the fundamental principles provided by the Outer Space Treaty (OST).[9] While the United Nations Committee on the Peaceful Uses of Space (UNCOPUOS) works towards the development of global consensus on these aspects,[10] it is essential to find pragmatic solutions that can safeguard the stability of the system in the meantime. Based on the above, this paper discusses how to leverage the provisions of the OST to provide a minimum degree of international coordination among competing extraction activities on the Moon. Further, as applicable, the paper also considers what role could be played by organisations like NATO towards the peaceful, sustainable and strategic use of lunar resources.

Legal aspects of lunar resource activities

The fundamental rules of international space law are laid down in the *Corpus Iuris Spatialis,*[11] a collection of five treaties concluded between the 1960s and the 1980s within the diplomatic framework of UNCOPUOS.[12] For the

---

[6] Bryce Space, 'Projected Exploration Missions (2020-2030)', (*BRYCE*, 8 September 2020) https://brycetech.com/reports accessed March 2021.

[7] Open Lunar Foundation (OLF), 'Lunar Resources Policy' (*OLF*, 7 October 2020) https://uploads-ssl.webflow.com/5e4b7985a58df89b6c254001/5f67e8e085456939322e7b02_Lunar%20Resource%20Policy%20Comment%20Open%20Lunar%20Foundation.pdf accessed March 2021.

[8] Antonino Salmeri, 'Houston We Have a Law. A Model for the National Regulation of Space Resource Activities', (*Proceedings Of The 70th International Astronautical Congress* 2019), https://iafastro.directory/iac/archive/browse/IAC-19/D4/5/50830/ accessed March 2021.

[9] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, entered into force 10 October 1967, 610 U.N.T.S. 205 (OST).

[10] The latest update in UNCOPUOS saw states rejecting the proposal from Belgium and Greece to establish a working group but also agreeing on conducting informal consultations on this item at the following session. Report of the Committee on the Peaceful Uses of Outer Space, Sixty-Second Session (12–21 June 2019), UN DOC A/74/20, 32-33.

[11] For contemporary assessments on the *Corpus Iuris Spatialis*, *see:* Mahulena Hofmann & Tanja Masson-Zwaan, *Introduction To Space Law* (4th edn, Wolters Kluwer 2019); Francis Lyall & Paul Larsen, Space Law; A Treaties (2nd edn, Routledge 2018); Frans Von Der Dunk & Fabio Tronchetti (eds), Handbook Of Space Law (Edward Eldgar 2015).

[12] For an historical overview on the creation of international space law, *see* Bin Cheng, *Studies*

purposes of this paper, the present analysis primarily focuses on the most relevant source of international space law, the OST, which is considered to be the *Magna Charta* of space law.[13] Its universal recognition[14] makes it a crucial reference point for the conduct and regulation of all space activities, including space mining.[15] To this end, this section provides a snapshot of the fundamental legal implications brought by Articles I-IX of OST on the conduct and regulation of space resource activities. These provisions are at the core of the system of international space law and are universally considered to be declaratory of customary international law.[16] As such, the implications described in this section are applicable to the whole international community of states, and not just the parties to the OST.[17]

Our assessment begins with the first three Articles of the OST, which collectively determine the legal status of outer space and celestial bodies as global commons.[18] Under Article I OST, these domains can be freely explored and used by any state, for the benefit and in the interests of all of them.[19] Pursuant to the first two paragraphs of this provision, space activities shall be conducted as global endeavours promoting the development of all states in accordance with international law.[20] To preserve the exploration and use of

---

In International Space Law (Clarendon Press Oxford 2004) 150-211

[13] Peter Haanappel, *The Law And Policy Of Air Space And Outer Space. A Comparative Approach* (Kluwer Law International 2003) 9.

[14] UNGA Res 72/78 (29 December 2017) UN DOC A/RES/72/78.

[15] Frans Von der Dunk, 'International Space Law', in Frans Von Der Dunk & Fabio Tronchetti (eds,)*Handbook of Space Law*, 59.

[16] Ram S. Jakhu & Steven Freeland, 'The Relationship between the Outer Space Treaty and Customary International Law', in PROCEEDINGS OF THE 59th IISL COLLOQIUM ON THE LAW OF OUTER SPACE (Eleven Publishing 2016) 183 - 191; Valentina Vecchio, 'Customary International Law in the Outer Space Treaty: Space Law as Laboratory for the Evolution of Public International Law', 66 German Journal of Air and Space Law (2017) 491.

[17] On the formation and effects of customary international law, *see,* Paola Gaeta, Jorge E. Vinuales & Salvatore Zappalà, *Cassese's International Law* (Third Edition, Oxford University Press 2020 – hereinafter "CASSESE'S IL") 181 -192.

[18] Legally speaking, this expression indicates areas beyond the national jurisdiction of sovereign states, which as such must be respected and preserved for everyone's exploration and use. The high seas, outer space, Antarctica and cyberspace are generally considered to be global commons. Surabhi Ranganathan, 'Global Commons', 27 (3) European Journal of International Law (2016) 693; *see also* Ivaylo Angelov, 'Global Commons And Their Strategic Significance For The European Union And NATO', 2 (2) Security & Future (2018) 67 -71; Elizabeth Mrema, 'Protecting the Global Commons: The Challenge of Collective Action', 18 (1) Georgetown Journal of International Affairs (2017) 3 - 5.

[19] Article I OST, *supra* note 6.

[20] Stephan Hobe, 'Article I of the Outer Space Treaty', in Stephan Hobe, Bernhard Schmidt-Tedd & Kai-Uwe Schrogl (eds), *Cologne Commentary On Space Law: Vol. 1* (Carl Heymanns Verlag 2009 –36–40 (hereinafter referred to as "CoCoSL I").

space as "the province of all mankind",[21] there shall be no active barriers impeding their enjoyment by a particular country, while spacefaring and non-spacefaring nations shall constructively engage to ensure their conduct on a basis of equality.[22] The freedom of exploration and use of space is safeguarded by Article II OST, which forbids states to extend their sovereign influence thereby.[23] On celestial bodies, this prohibition builds upon the obligation to ensure free access to all their natural areas under Article I OST,[24] which essentially translates in a specular right of free passage.[25] Finally, the global relevance of space activities is consecrated by Article III OST, according to which states shall conduct them "in accordance with international law and in the interest of maintaining international peace and security and of promoting international cooperation and understanding".[26] As a consequence of this provision, the strategic use of a shared domain like outer space is allowed to the extent that it does not threaten the peaceful equilibrium established within the international community.

From this combined assessment of Articles I – III OST it is possible to develop some fundamental implications on the conduct and regulation of lunar resource activities. First and foremost, these activities are allowed as part of the freedom to use celestial bodies under Article I OST and are not covered by the prohibition of national appropriation under Article II OST.[27] Second, pursuant to the legal status of celestial bodies as global commons, lunar resource activities are naturally subjected to a series of limitations[28] that will evolve in accordance with the technologic and economic development of

---

[21] *Ibid.*

[22] In essence, the principle of equality refers to a scenario where all states become capable of conducting their own space activities by learning from, and participating to, the activities of the others. Timiebi Agaba-Jeanty, 'Realizing a Regional African Space Program', in Mahulena Hofmann & P.J. Blount (eds), *Innovation In Outer Space: International and African Legal Perspectives* (2018) 258-259 (hereinafter referred to as "IOS").

[23] The prohibition of national appropriation of outer space and celestial bodies is considered to be a cardinal rule of international space law. Fabio Tronchetti, 'The Non- Appropriation Principle Under Attack: Using Article II of the Outer Space Treaty in its Defence', in PROCEEDINGS OF THE 50TH IISL COLLOQUIUM OF THE LAW OF OUTER SPACE (2009) 526-536.

[24] P.J. Blount, 'Outer Space and International Geography: Article II and the Shape of the Global Order', 52 (2) New England Law Review (2018) 102 -103.

[25] Whose exercise will be subjected to appropriate consultations avoiding harmful interference under Article IX OST.

[26] Article III OST, *supra* note 6.

[27] Mahulena Hofmann, 'Space Resources: Regulatory Aspects', in IOS, *supra* note 19 at 202 – 203.

[28] Fabio Tronchetti, 'Legal Aspects of Space Resource Utilization', in Handbook Of Space Law, *supra* note 8 at 778 – 782.

the Moon. At the very minimum, lunar resource activities should be limited in size, time and manner.[29] In a time when global interest in lunar activities has prominently resurged, no single entity should be allowed to mine the entire south pool of the Moon or to exclusively "extract" solar energy from the lunar peaks of eternal light[30] for an indefinite amount of time. Based upon these fundamental considerations, the section will now collectively assess Articles IV – IX OST to determine further implications on the conduct and regulation of lunar resource activities.

Under Article IV (2) OST, celestial bodies shall be used for exclusively peaceful purposes.[31] While in general international space law the term "peaceful" can be interpreted either as "non-military" or "non-aggressive",[32] the use of the adverb "exclusively" before "peaceful purposes"[33] in Article IV (2) OST outlaws the direct or indirect use of celestial bodies for any military purposes.[34] At the same time, the provision further includes a list of allowed military activities like "the use of military personnel for scientific research or for any other peaceful purposes"[35] as well as "the use of any equipment or facility necessary for peaceful exploration".[36] As a consequence, every military activity that is not explicitly permitted under the terms of these exceptions is considered to be strictly prohibited. This complete demilitarization of celestial bodies serves the purpose of preserving them from conflicts,[37] to safeguard both international peace and security on Earth as well as international cooperation in space exploration.[38] For what concerns lunar resource activities, there is no doubt that the general prohibition to use celestial bodies for military purposes also covers the extraction and use of their resources.[39] As a consequence, only civilian

[29] Salmeri, *supra* note 5 at 5.
[30] On the potential usefulness of the peaks of eternal lights *see* Philippe Gläser *et al.*, 'Illumination Conditions at The Lunar South Pole Using High Resolution Digital Terrain Models From Lola', 243 Icarus (2014) 78–90.
[31] Article IV OST, *supra* note 6. For a comprehensive analysis on this provision *see* Kai-Uwe Schrogl & Julia Neumann, 'Article IV', in CoCoSL I, *supra* note 17 at 70 - 93.
[32] Stephan Hobe & Niklas Hedman, 'Preamble', in CoCoSL I, *supra* note 17 at 22. For a comprehensive analysis of the two interpretations proposed, *see* Cheng, *supra* note 9 at 513 – 522.
[33] Article IV OST, *supra* note 6.
[34] Fabio Tronchetti, 'Legal Aspects of the Military Uses of Space', in Handbook of Space Law, *supra* note 8 at 338-341.
[35] Article IV (2) OST, *supra* note 6.
[36] *Ibid.*
[37] Tronchetti, *supra* note 31 at 340; Schrogl & Neumann, *supra* note 28 at 82.
[38] Under the terms of Article III OST, *supra* note 6.
[39] Olavo De Bittencourt Neto, "Building Blocks For The Development Of An International Framework For The Governance Of Space Resource Activities: A Commentary" in Mahulena

entities shall engage in and benefit from these activities,[40] although military personnel could theoretically support civilian lunar resource activities for exclusively peaceful purposes. For organizations like NATO conducting both civil and military operations, compliance with Article IV OST will require full disclosure as to the exclusively peaceful nature of their involvement.

Moving to Article VI OST, pursuant to this provision states bear international responsibility for the space activities conducted by their nationals, whether of public or private nature, and for assuring their compliance with the rules of the OST.[41] To ensure a high-level of compliance, the central part of Article VI OST further requires states to authorize and continuingly supervise the space activities of their non-governmental entities.[42] As a consequence, every space activity is always guaranteed by the international responsibility of a state, which will have to actively verify and maintain its compliance with international space law.[43] For what concerns lunar resource activities, the obligations of Article VI OST lead to the enactment of domestic legislation on space mining[44] and will play a crucial role in ensuring that they will be compliant with the rules of international space law.

The principle of international responsibility for space activities under Article VI OST is followed by the principle of international liability for damage caused by space objects under Article VII OST.[45] Importantly, this provision creates a new category of states collectively referred to as "launching

---

Hofmann, Tanja Masson-Zwaan & Dimitra Stefoudi (eds), [Need name of book] (Eleven International 2020) 33 (hereinafter referred to as "BB Commentary").

[40] Recently, even the simple interest shown by the US Defense Advanced Research Projects Agency in funding research related to lunar mining raised strong criticism and oppositions, even from United States space experts. Theresa Hitchens, 'DARPA Space Manufacturing Project Sparks Controversy' (BREAKING DEFENSE, 12 February 2021) https://breakingdefense.com/2021/02/darpa-space-manufacturing-project-sparks-controversy/ accessed March 2021. For more information on this project, *see* Sandra Erwin, 'DARPA To Survey Private Sector Capabilities To Build Factories On The Moon' (SPACE NEWS, 7 February 2021) https://spacenews.com/darpa-to-survey-private-sector-capabilities-to-build-factories-on-the-moon/ accessed March 2021.

[41] Article VI OST, *supra* note 6.

[42] *Ibid.*

[43] Tanja Masson-Zwaan, 'Article VI of The Outer Space Treaty and Private Human Access To Space', in PROCEEDINGS OF THE 51st IISL COLLOQIUM ON THE LAW OF OUTER SPACE 537 (2009).

[44] At present, only three states in the world have enacted specific legislation allowing their nationals to engage in space resource activities: the United States of America, the Granduchy of Luxembourg and the United Arab Emirates.

[45] For a comprehensive assessment of Article VII OST, *see* Armel Kerrest & Lesley Jane Smith, 'Article VII', in CoCoSL I, supra note 17 at 126 – 145.

States",[46] which are those having directly performed, financially procured or materially organized the launch of an object into outer space.[47] In essence, this provision makes these states internationally liable for any damage caused by their space objects. Within the context of lunar resource activities, Article VII OST will probably play a residual role due to the applicability of the Liability Convention[48] (LIAB). The LIAB has been developed from Article VII OST and serves as *lex specialis* for damages caused by space objects.[49] Under Article III LIAB, the liability regime for collisions happening in outer space - including celestial bodies - is based on fault.[50] Unfortunately, the ambiguity of the term in itself, together with the lack of any practice under the LIAB, constitute a significant threat to the applicability of the LIAB to lunar resource activities. To solve this issue, it will be critical to develop relevant best practices that can serve as a reference point for the concrete determination of fault.

The liability regime for damage caused by space objects is complemented by the rules on jurisdiction and control provided by Article VIII OST.[51] Notably, also this provision is based on the concepts of launching state and space objects. However, while under Article VII OST all *launching states* are jointly liable for damage caused by their space object, pursuant to Article VIII OST only one of them is entitled to retain jurisdiction and control over it.[52] Under the terms of this provision, the identification of this state is done through the inclusion of the object within a national registry.[53] To better understand this mechanism, it is important to remember that already in 1961 the General Assembly of the United Nations (UNGA) had established a UN "Registry of Objects Launched into Outer Space"[54] in its Res. 1721B (XVI) of 20 December 1961.[55] Pursuant to this resolution, states were invited to provide information on their launches to the UN Secretary General (UNSG) with the goal to facilitate international cooperation in the exploration and use of outer space. As a

---

[46] Cheng, *supra* note 9 at 613.
[47] Article VII OST.
[48] Convention on International Liability for Damage Caused by Space Objects (entered into force 9 October 9 1973, 961 U.N.T.S. 187.
[49] Lesley Jane Smith & Armel Kerrest, Article I LIAB (Definitions), in Stephan Hobe, Bernhard Schmidt-Tedd & Kai-Uwe Schrogl (eds), *Cologne Commentary on Space Law: Vol. 2* (Carl Heymanns Verlag 2013) 101 – 103 (hereinafter referred as "CoCoSL II").
[50] Article III LIAB, *supra* note 45.
[51] See Bernhard Schmidt-Tedd & Stephan Mick, 'Article VIII', in CoCoSL I, *supra* note 17 at 147.
[52] Article VIII OST, *supra* note 6.
[53] *Id.*
[54] The UN Registry is publicly available at https://www.unoosa.org/oosa/en/spaceobjectregister/index.html, accessed April 2021.
[55] UNGA Res 1721B (XVI), (20 December 1961) UN DOC RES 1721B (XVI).

consequence, launching states began to setup parallel national registries to collect the information to be transmitted to the UNSG. When the OST was negotiated, states decided to refer to their own national registries rather than the UN one in order to secure more leverage on the registration process.[56] Therefore, the first state including a space object within its national registry will *retain* jurisdiction and control over it, including any personnel on board. Notably, the use of the term *retain* signifies that national registration is not the legal source of these powers, which are inherently vested in all launching states, but rather the formal mechanism to identify *which one* is entitled to exercise them.[57] As to the extent and scope of these powers, it is important to consider that Article VIII OST extends the jurisdiction and control of that the state registry exercises over a space object also to "any personnel thereof".[58] In light of the status of celestial bodies as areas subtracted to the national jurisdiction of any state, Article VIII OST will play a fundamental role in ensuring the lawful and ordered development of lunar resource activities. The attribution of both material and personal jurisdiction will in fact allow the state of registry to exercise the minimum powers needed to avoid the creation of a preoccupying legal vacuum for the activities conducted on the lunar surface.

The next provision considered within our snapshot on the applicability and impact of the fundamental rules of space law to lunar resource activities is Article IX OST.[59] According to some authors, this provision could be considered as the *systemic* clause of international space law,[60] since it is the only article of the OST practically bringing the states that are parties to the treaty *vis-à-vis* with one another. First, pursuant to the initial part of Article IX OST, states are obliged to conduct their space activities with due regard for the corresponding interests of all other states that are parties to the treaty.[61] In essence, *paying due regard* implies that a state shall not undertake activities that would threaten the exercise of the freedoms of exploration and use by other states.[62] As such, the principle of due regard is considered to be an important limit to the freedom of

---

[56] Bernhard Schmidt-Tedd & Stephan Mick, 'Article VIII', in CoCoSL I, *supra* note 17
[57] *Id.*, at 156 – 159.
[58] Article VIII OST, *supra* note 6. Notably, the jurisdiction and control of the state of registry overrides the personal jurisdiction based on the nationality criteria, and continues also when the relevant personnel get outside the space object. Cheng *supra* note 9 at 231 – 232.
[59] For a comprehensive analysis of this provision, *see* Sergio Marchisio, 'Article IX', in CoCoSL I, supra note 17 at 169 - 182.
[60] Antonino Salmeri, *The Multi-Level System of Space Mining: Regulatory Aspects and Enforcement Options*, (Doctoral Thesis, forthcoming) 125.
[61] Article IX OST, *supra* note 6.
[62] Sergio Marchisio, 'Article IX', in CoCoSL I, supra note 17 at 175.

exploration and use of outer space provided for in Article I (2) OST.[63] Second, the central part of Article IX OST requires states to conduct their space activities so as to avoid the harmful contamination of outer space and adverse changes in the environment of the Earth.[64] Building upon the principle of due regard, the interpretation of "harmful contamination" refers to those actions that - because of their impact on the outer space environment - would negatively affect the space activities conducted by other states.[65] Finally, the last part of Article IX OST requires states to undertake "appropriate international consultations in case they have reason to believe that their space activities may cause potentially harmful interference with those of other states".[66] If implemented in accordance with the general principle of good faith,[67] the duty to consult can concretely operationalize the principle of due regard by providing states with the opportunity to find an *ad hoc* solution that takes into account their respective interests. Within the context of lunar resource activities, the implementation of Article IX OST will be decisive in assessing their compatibility with international space law. For instance, a state authorizing a private company to mine all the available ice in the entire south pole of the Moon would be clearly breaching its obligation to pay due regard to the corresponding interests of other states. On the contrary, a state demanding the completion of an environmental impact assessment before authorizing lunar mining operations would be fulfilling its obligations under Articles VI and IX OST.

To conclude the present analysis, we will now briefly touch upon a provision which is usually neglected by scholars and mostly unknown by practitioners: Article XI OST. According to this provision, "States agree to inform the UNSG, the public and the scientific community, to the greatest extent feasible and practicable, of the nature, conduct, locations and results of their space activities".[68] Originally, the purpose of Article XI OST was to promote international cooperation through the sharing of essential information on the various space activities conducted by states.[69] Although the provision is explicitly mentioned only in rare cases, the public release of information has been increasingly implemented in practice by many space agencies within the

[63] Hobe, *supra* note 17 at 39-40.
[64] Article IX OST, *supra* note 6.
[65] Sergio Marchisio, 'Article IX', in CoCoSL I, supra note 17 at 176 - 177.
[66] Article IX OST, *supra* note 6.
[67] Sergio Marchisio, 'Article IX', in CoCoSL I, supra note 17 at 180.
[68] Article XI OST, *supra* note 6.
[69] Jean-Francois Mayence and Thomas Reuter, 'Article XI', in CoCoSL I, *supra* note 17 at 191.

context of their scientific space activities.[70] As such, Article XI OST has so far played an important role in connecting the space community, facilitating international cooperation and fostering the exploration and use of space as the province of all humankind. As it will be seen in the next section, within the context of lunar resource activities Article XI OST could be leveraged as a crucial tool of international coordination to safeguard their safe and peaceful conduct.

Proposed solutions for the regulation of lunar resource activities

Our analysis of the fundamental rules of international space law reveals a critical vulnerability currently affecting the regulation of lunar resource activities. Simply put, these rules are formulated in such broad terms that they can be used to develop potentially opposite but equally valid legal conclusions. For instance, a strict interpretation of the principle of free access under Article I OST and the prohibition of non-appropriation under Article II OST would find many planned lunar resource activities to be illegal under international space law, to the detriment of technological development.[71] Conversely, a broad interpretation of the freedom of use under Article I OST in conjunction with a restrictive interpretation of the prohibition of harmful contamination under Article IX OST would come to opposite conclusions and potentially even justify abusive behaviours. In the absence of any authoritative interpretation of the OST, this variety of conflicting regulatory options makes the future of lunar resource activities highly unpredictable. Having said that, there are ways to control the current uncertainty in a pragmatic but also legitimate and effective manner. Notably, this possibility is enabled by the fact that we are still in the early stages of lunar resource activities. Therefore, at present we can still leverage the existing rules to ensure their safe and ordered conduct. However, the rapid scalability of mining operations implies that these early stages will not last for a long time. Consequently, we must begin now to work towards the development of a dedicated legal framework that can guide the application of the principles of international space law to lunar resource activities.[72] Accordingly, this section proposes two sets of legal solutions: *de lex*

---

[70] Jim Brindestine, 'Life on Earth is Better Because of NASA' (NASA, 25 September 2020), https://blogs.nasa.gov/bridenstine/2020/09/25/life-on-earth-is-better-because-of-nasa/ accessed April 2021.

[71] Fabio Tronchetti and Liu Hao, "The American Space Commerce Free Enterprise Act of 2017: The Latest Step in Regulating the Space Resources Utilization Industry or Something More?", (2019) 47 Space Policy 1-6.

[72] Lunar Resources Policy, *supra* note 4. *See also,* albeit in more general terms for all space resource activities, BB Commentary, *supra* note 36 at 17 – 19.

lata[73] for the early stages and *de lege ferenda*[74] for the subsequent ones.

During the early stages of lunar resource activities the fundamental priority will be to ensure the safety of pioneering operations while also promoting their sustainability in view of future developments. Given the limited scale and numbers of planned operations, both goals can be achieved by leveraging the mechanisms foreseen in Article IX and Article XI OST. As seen, under Article IX OST states shall pay due regard to the corresponding interests of other States and internationally consult in case of potentially harmful interferences. On the Moon, compliance with both obligations will inevitably depend on the availability of information concerning the activities taking place thereby. If a state conducting a lunar activity does not inform the others about – at the very least - its nature, locations and duration, it cannot expect them to pay due regard or to consult in case of potentially harmful interference. Likewise, without this information it will be rather difficult for a state planning to conduct a lunar activity to pay due regard to, or avoid interferences with, previous activities already taking place thereby. In turn, this generalized lack of information would exponentially increase the risk of political conflicts and operational disturbances caused by uncoordinated lunar resources activities. Article XI OST could play a crucial role in preventing these conflicts and disturbances by providing a universally accepted procedure for sharing and updating essential information on lunar resource activities. Legally speaking, states actively implementing Article XI OST should be able to rely on a series of notable benefits. First, in making their planned activities known to the others, these states would enjoy the protection offered by the principle of due regard. As a consequence, states sharing information under Article XI OST would find themselves in a better position to avoid potentially harmful interferences, given that all actors would be well aware of their presence and would be under the obligation to take it into account. Further, these states would also approach any potential liability claim from a clear position of advantage, given that sharing information can be considered as proof of due diligence and thus impede any attribution of fault.

While certainly useful in the early stages, the combined application of Article IX and XI OST can keep the system stable only up to a certain point in time. The more lunar resource activities take place, the more difficult will be to coordinate and pay due regard on the sole basis of essential information. The more invasive these activities become, the more complicated will be to ensure

[73] "*De Lex Lata*" is a Latin expression meaning "based on the existing law".
[74] "*De Lege Ferenda*" is a Latin expression meaning "in light of the future law".

their sustainability and their harmonious integration with other lunar endeavours. Therefore, it is critical to begin working now for the development of a dedicated legal framework that can ensure the peaceful and safe development of the Moon. In accordance with the principles of proportionality and adaptive governance, this framework should not be conceived as a binding international system centralizing the regulation of lunar resource activities within a newly created global institution.[75] While this may certainly happen in the future, a fully-fledged international system is not what we should aim for at the moment. First, because we do not yet possess the information that would be necessary to develop proper international regulation that can remain useful and relevant through the passing of time. Second, because negotiating a fully-fledged international system will likely be a long process which in the meantime would condemn the world to either inaction or uncertainty. Consequently, we should aim for a middle-level framework that can guide the operationalization of the fundamental rules of international space law within the context of lunar resource activities.[76] In doing so, this framework could provide the necessary boundaries for the development of more specific regulation at the national level. In the Lunar Governance Report[77] recently developed by the E.A.G.L.E. Action Team of Space Generation Advisory Council,[78] this middle-level framework is proposed in the form of a Lunar Governance Charter.[79] By their own nature, charters provide a general but also coherent approach to the regulation of a given topic.[80] In particular, a Lunar Governance Charter would allow states to agree on a shared starting point that can then shape the future development of more detailed regulation at the national level.[81] In these authors' view, the enactment of a similar international instrument would provide the level of legal certainty needed at this time while also preserving the necessary flexibility for future regulatory adaptation.

---

[75] BB Commentary, *supra* note 36 at 17 – 19.
[76] Salmeri, *supra* note 57 at 189.
[77] Antonino Salmeri, Giuliana Rotola *et al.*, 'Effective and Adaptive Governance for a Lunar Ecosystem – Lunar Governance Report' (Space Generation Advisory Council 2021)) www.spacegeneration.org/eagle, accessed April 2021 (hereinafter referred as ""EAGLE Report").
[78] Space Generation Advisory Council ("SGAC") is the largest network organization of young professional and students from the space community. SGAC established the E.A.G.L.E. Team in July 2020 with the goal to develop the position of the organization within the global debate on lunar governance. Information on SGAC can be found on its website at https://spacegeneration.org/about (accessed April 2021).
[79] EAGLE Report, *supra* note 74 at 29.
[80] *Ibid.*
[81] *Ibid* at 30.

Conclusion

Humankind has set eyes on returning to the Moon by the end of the present decade. This time, the goal is to establish a sustained and sustainable presence that can enable and support the expansion of our species throughout the solar system. In the course of this process, lunar resource activities will play a key role in lowering the cost of lunar exploration while also promoting the strategic utilization of the Moon. Notwithstanding these clear benefits, the regulation of lunar resource activities is still affected by a significant degree of uncertainty. Due to the current regulatory impasse in UNCOPUOS, it is likely that the early stages of lunar mining will be governed by the general principles of the OST, as complemented by a series of ad-hoc bilateral arrangements among the relevant operators. Within this context, this article showed the main legal implications of the fundamental rules of international space law for the regulation and conduct of lunar resource activities. As a result of this analysis, the article argued that the ambiguity and broadness of the OST principles inevitably brings a serious potential for disagreement and conflict among lunar actors, especially on the topic of lunar resources utilization. In the short term, this potential could be lowered thanks to the combined application of Articles IX and XI OST. The public and proactive release of information on the nature, location and duration of lunar activities will enable actors to pay due regard and undertake appropriate international consultations to avoid potentially harmful interferences. While certainly useful, information sharing and ad-hoc coordination can stabilize the system only for a while. Therefore, it is imperative to begin working now for the development of a flexible international framework that can serve as reference point for the incremental regulation of all lunar activities as the province of all humankind.

***

Source: www.nato.int

Strategic and Legal Implications of Emerging Dual-Use ASAT Systems[1]

by Linda Slapakova,
Theodora Vassilika Ogden and
James Black[2]

Introduction

When the North Atlantic Treaty Organization (NATO) formally recognised space as an operational domain in 2019, this was in acknowledgement of the increasing importance of space in military operations and the growing threat of escalation in this arena.[3] Military operations and NATO's defence and

[1] **DISCLAIMER**: The views expressed in this article are solely those of the authors and may not necessarily represent the views of NATO, Allied Command Operations, or Allied Command Transformation, or of their affiliated organizations, nor those of RAND Europe and the wider RAND Corporation.

[2] The authors are part of the Defence, Security and Infrastructure research group at RAND Europe, part of the RAND Corporation, a not-for-profit research institute that works extensively for NATO institutions, allies, and partners. Linda is an Analyst and has recently completed studies of emerging space technologies for the UK Space Agency and Defence Science and Technology Laboratory. Theodora is a Research Assistant and former Legal Intern at NATO HQ SACT; she is currently conducting research supporting the UK Defence Space Strategy. Alongside coordinating RAND Europe's defence strategy and policy work stream, James is European Lead for the RAND Space Enterprise Initiative (RSEI), a global hub for RAND's ongoing research on space policy, operations, capabilities and technologies. For more information: https://www.rand.org/capabilities/space-enterprise-initiative.html

[3] Alexandra Stickings, 'Space as an Operational Domain: What Next for NATO?' (*RUSI*

deterrence posture more broadly have become increasingly dependent on space. Secure access to and exploitation of different orbits provide key services such as satellite communications (SATCOM), positioning, navigation and timing (PNT), and Earth observation (EO) for intelligence, surveillance and reconnaissance (ISR) purposes. Satellites, data links and ground stations all form essential enablers of the Alliance's networked command and control (C2) systems and information architecture, supporting joint operations on land, in the air, at sea and in cyberspace and the electromagnetic environment.

Beyond defence, services such as SATCOM, PNT and EO are increasingly provided or used by an expanding array of government, civilian and commercial actors. In this way, space has become essential to modern global society, the digital economy, and critical national infrastructure.[4] Satellite services now play central roles in everything from credit card payments to managing supply chains and monitoring climate change. Growing demand, coupled with rapid innovation and falling costs of launch, is contributing to space becoming increasingly "congested, contested and competitive", with a rising number of actors establishing a presence in orbit.[5]

While satellites and other space technologies are of increasing importance for the global economy, their "dual-use" nature means they can often be used for both non-military and military purposes, such as anti-satellite (ASAT) attacks. In principle, the risk of armed attacks on civilian infrastructure could appear to preclude most ASAT attacks under the Law of Armed Conflict (LOAC).[6] In practice, however, many states are not only deploying overtly military ASAT capabilities (both kinetic and non-kinetic) but also pursuing civil programmes to develop and field new technologies with overlapping uses. Any such systems, for example those intended for on-orbit repair, refuelling or debris management (e.g. through forced de-orbiting), are inherently dual-use.[7] This dual-use conundrum may significantly impact space safety and security,

---

Newsbrief, 2020) https://rusi.org/publication/rusi-newsbrief/space-operational-domain-what-next-nato accessed 3 May 2021

[4] James Black, Linda Slapakova, Kevin Martin, 'Future Uses of Space out to 2050' RAND Corporation (forthcoming)

[5] Gregory L Schulte, 'A New Strategy for New Challenges in Space' (*Remarks to the National Space Symposium,* 2011)

[6] See the following section of this article on legal implications.

[7] Jakub Prazak, 'Dual-use conundrum: Towards the weaponisation of outer space?'(*Acta Astronautica*, 2020) https://www.sciencedirect.com/science/article/abs/pii/S0094576520307943?via%3Dihub accessed 3 May 2021

strategic stability, and wider defence and protection of civilians on Earth; thereby presenting a number of challenges from an international legal perspective, including arms control, non-proliferation and the promotion of responsible space behaviour.[8]

This article addresses the dual-use conundrum of space technology, examining where the threshold lies for ASATs. We first consider the issue from a technological standpoint, briefly examining which current or emerging technologies may constitute ASATs, how they can be (mis/)used in offensive operations, and how innovation could exacerbate the dual-use challenge in the future. Secondly, we discuss the international legal implications of the development and deployment of dual-use ASAT capabilities, including in relation to the Outer Space Treaty and its principle of space use "exclusively for peaceful purposes". Lastly, we discuss the potential implications for NATO and its evolving approach in this new operational domain.

Characterising Threats and Key Technologies

The space environment has undergone a major transformation in recent years, with commercialisation, digitalisation, miniaturisation and falling launch costs all driving an increasing use of Earth orbit for both military and civil applications.[9] Before laying out the legal and strategic challenges associated with dual-use technologies, the following sections describe key drivers of innovation in the space domain, the nature of these innovations – particularly in relation to on-orbit servicing and other close proximity missions – and their potential (mis)use for ASAT purposes.

ASAT Threats in a Changing Space Environment

As of May 2021, there are more than 3,000 operational satellites currently in orbit,[10] along with an estimated 29,000 objects, including debris, larger than 10cm and approximately 670,000 larger than 1cm.[11] This growing mass of clutter

[8] Bruce McClintock, Katie Feistel, Douglas C. Ligor, Kathryn O'Connor, 'Responsible Space Behaviour for the New Space Era' (*RAND Corporation*, 2021) Responsible Space Behavior for the New Space Era: Preserving the Province of Humanity (rand.org) accessed 20 April 2021

[9] OECD, 'Space sustainability: The economics of space debris in perspective' (2020) https://www.oecd-ilibrary.org/docserver/a339de43-en.pdf?expires=1618920091&id=id&accname=ocid56013842&checksum=2AFCA8325D7D6742EB34AFD7231CA36C accessed 20 April 2021

[10] USC Satellite Database (2021) https://www.ucsusa.org/resources/satellite-database accessed 5 May 2021

[11] ESA 'How many space debris objects are currently in orbit?' (undated) http://www.esa.int/Safety_Security/Clean_Space/How_many_space_debris_objects_are_curr

is the result of several years of unprecedented growth, provoked by the advent of re-usable launch vehicles (e.g. SpaceX's Falcon 9 or Blue Origin's New Shepard) and the ambition of various commercial actors (e.g. SpaceX, OneWeb, Amazon) to deploy mega-constellations of small satellites in low Earth orbit (LEO).[12] This "NewSpace" movement represents a major departure from the previous paradigm of space use, which had centred around military and government agencies, and had often focused on operating small constellations of large "traditional" satellites in other orbits such as MEO or GEO.[13]

Given the design challenges produced by the harsh environment of space and a drive to minimise weight (and thereby launch costs), many satellites are inherently "soft" targets that might easily be damaged through either kinetic or non-kinetic means.[14] Physics and orbital dynamics also make the paths of satellites relatively easy to predict and track (though not necessarily straightforward to intercept).[15] However, with increasing dependence on satellite-enabled services in defence as well as other parts of the global economy, a range of developments have also increased the risk of incidental or non-incidental damage. Together, the inherent vulnerability of satellites and the increasing dependence of militaries and societies on the services they provide have raised fears that they may be attractive targets in any future conflict.

---

ently_in_orbit accessed 20 April 2021

[12] Lloyds & London Economics, 'NewSpace: Bringing the new frontier closer to home' (*Emerging Risks Report, Lloyds & London Economics*, 2019) https://www.lloyds.com/news-and-risk-insight/risk-reports/library/understanding-risk/newspace-bringing-the-new-frontier-closer-to-home accessed 3 May 2021

[13] For example, the U.S.'s Global Positioning System (GPS) requires 24 satellites, plus any spares for redundancy and resilience, which are distributed across six orbital planes in medium Earth orbit (MEO). Other EO and meteorological satellites are in geostationary or geosynchronous equatorial orbits (GEO), appearing to hover above a fixed point on the Earth's surface.

[14] Kinetic means are understood as those that can cause physical damage to a space asset through physical contact, such as direct strike or detonation of a warhead in a close vicinity of an asset. In contrast, non-kinetic means are understood as causing damage without any physical contact, such as through cyberattacks or electromagnetic measures. Source: Todd Harrison, Kaitlyn Johnson, Makena Young, 'Defense against the dark arts in space' (*CSIS Aerospace Security Project*, 2021) https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210225_Harrison_Defense_Space.pdf?N2KWelzCz3hE3AaUUptSGMprDtBlBSQG accessed 3 May 2021

[15] Rebecca Reesman & James R. Wilson, 'The physics of space war: How orbital dynamics constrain space-to-space engagements' (*Centre for Space Policy and Strategy,* 2020) https://aerospace.org/sites/default/files/2020-10/Reesman_PhysicsWarSpace_20201001.pdf accessed 3 May 2021

ASAT capabilities leverage a wide range of technologies to deliver kinetic or non-kinetic effect, either in space itself (i.e. space-to-space) or from Earth. While direct space-to-space engagements between two satellites, such as phasing manoeuvres, remain technically and operationally challenging, there are a range of manoeuvres that can cause danger or disruption. Co-orbital ASATs can be used by placing a satellite into orbit and manoeuvring it to deliver direct or indirect action against another satellite. Theorised attack methods then include everything from basic surveillance and ramming through to the use of chemical sprays, nets, mines, pellets, harpoons, robotic arms and other intricate measures. It is important to note that most such concepts are yet to be operationalised.[16]

Tests by the United States, Russia, China and India have shown that ASAT attacks can be carried out through the launch of ASAT missiles on an intercept course from Earth, either from a fixed base or from mobile air and maritime platforms. Short of such overt measures, non-kinetic ASATs also make use of cyber and electromagnetic means to engage targets, for example via hacking, spoofing, jamming or dazzling. Additionally, disrupting or damaging satellites can be carried out through attacks on vulnerable ground stations, launch sites and supply chains – for example sabotage, subversion or attack – recognising that operational satellites are only one element of a larger "system of systems".

In some cases, the intent of hostile kinetic or non-kinetic actions against satellites may simply be to force them into evasive manoeuvring. This, in addition to using up finite stores of fuel and propellant, might ensure the gaze of an ISR satellite is moved off a strategically important location on Earth at a vital moment. In other instances, attacks may be intended to degrade the performance of a target satellite's payload temporarily and reversibly (for example, as a means of coercion or to create uncertainty and confusion in a crisis), or to destroy the target permanently. In all cases, any spill over of a terrestrial conflict into space could not only have major consequences for military operations in other domains (e.g. affecting communication or navigation systems), but also potentially threaten – perhaps unintentionally – space-based systems that form critical components of nuclear C2 and early warning.[17]

While military ASAT capabilities have thus historically represented

[16] 'Defense against the dark arts in space' (n 14)
[17] 'Future Uses of Space out to 2050' (n 4)

significant threats to space security, a wider transformation of the space environment has produced new vulnerabilities and risk factors. This includes poor domain and situational awareness (especially for any NATO Allies besides the United States, which operates a worldwide system of optical and radar sensors for space situational awareness, the Space Surveillance Network).[18] The number of objects launched to orbit each year has grown significantly in recent years, and current projections predict a doubling or tripling of the number of operational satellites in the next five years.[19] As technical and financial barriers-to-entry decrease, the space economy has even come to feature "amateur" satellite launches by students and hobbyists launching small satellites, on top of the ambitious plans of governments and commercial actors entering a crowded market.

This increasingly "congested, contested and competitive" environment has seen certain orbits, notably LEO, being much more intensively used. This exacerbates existing challenges associated with space security and sustainability. Even a minor collision or "conjunction" can cause significant damage or veer a satellite off course. Any resultant debris may, in turn, because a cascade of other collisions, each generating more debris and increasing the risk that entire orbits might be rendered unsafe (the so-called Kessler syndrome).[20] This means that any system capable of causing physical damage of a space object could also be used to deliberately threaten or disrupt satellites for military purposes.

Advances in non-military space technologies

Alongside changes in the political and commercial landscape, advances in science and technology also continue to drive change in the "state-of-the-art" for both kinetic and non-kinetic ASAT capabilities. This creates new threat vectors and vulnerabilities as well as enabling new mitigation strategies.[21]

---

[18] The U.S. SSN does involve input from, and information sharing with, key allies and partners, including beyond NATO (e.g. Australia). The UK, for example, hosts sensors at RAF Fylingdales and on Ascension Island and Diego Garcia, while Denmark contributes to the network's global coverage through its hosting of the U.S. military's operations at Thule Air Base in Greenland.

[19] 'Space sustainability: The economics of space debris in perspective' (n 10)

[20] 'Future Uses of Space out to 2050' (n 4)

[21] Australian Government Department of Defence, Science and Technology 'Space Technologies: Insight Paper' (2020) https://www.dst.defence.gov.au/sites/default/files/events/documents/EDTAS%20Space%20Te

Given the significant potential impact of in-space collisions – both in terms of the direct costs of any damage and the wider disruption to space-enabled services – both private and public sector actors have explored various ways and means of protecting space-based assets. This includes physical hardening of satellites or improvements in cybersecurity and defences against electronic attack, as well as investing in modelling and conjunction analysis or enhancing space situational awareness.[22] Broader efforts have also aimed at strengthening the resilience of space services, such that even if a satellite were to be damaged, on purpose or otherwise, the impact on downstream markets would be minimised. These efforts include building larger constellations of small low-cost satellites or investing in initiatives to manage debris and repair or recycle damaged or decommissioned satellites.[23] This translates to a growing requirement for capabilities for satellite refuelling, repairing, repositioning, removal and assembly on orbit and enabling technologies for rendezvous and proximity operations (RPO), in-space docking, assembly and manufacturing, and active debris removal (ADR).[24]

Satellites designed for RPO have received increasing attention due to the similarity of their technological features to those that might be found in co-orbital ASAT weapons.[25] These features include high levels of manoeuvrability, enabling satellites designed for RPO to make significant orbital adjustments to reach a specific target; advanced on-board sensor suites, guiding rendezvous and proximity engagements at very close distances; and inspection, docking and manipulation capabilities. While development of such capabilities is typically driven (at least ostensibly) by a desire to perform various civil and commercial missions, existing analysis notes that they could be leveraged for military purposes. Relevant missions could include collecting high-resolution imagery of other satellites, intercepting their transmissions, or disabling a satellite

chnologies%20-%20Insights%20Paper.pdf accessed 20 April 2021

[22] 'Responsible Space Behaviour for the New Space Era' (n 6)

[23] Alexander Soucek, 'On-Orbit Satellite Servicing/Close Proximity Operations: Legal Aspects' (*European Space Agency*, 2018) https://indico.esa.int/event/234/contributions/4134/attachments/3111/3820/2018CSID_ASoucek_LegalAspectsOfCPO.pdf accessed 20 April 2021

[24] Borowitz, Mariel, Lawrence Rubin, Brian Steward 'National Security Implications of Emerging Satellite Technologies' (2020) 64(4) Orbis https://www.sciencedirect.com/science/article/abs/pii/S0030438720300429 accessed 20 April 2021

[25] Ibid. Bohumil Dobos & Jakub Prazak, 'To Clear or to Eliminate? Active Debris Removal Systems as Anti-satellite Weapons' (2019) 217 (47) Space Policy https://doi.org/10.1016/j.spacepol.2019.01.007 accessed 3 May 2021

through manipulation or attack.[26]

Developing technologies for ADR – defined as "active deorbiting of pieces of debris to decrease the possibilities of collisions" – has also been considered a key step to mitigate the increasing congestion of the space domain.[27] As the amount of space debris increases, new ADR technologies have been developed in the commercial and civil space sectors. These range from kinetic ADR systems (e.g. robotic semi-autonomous debris capture mechanisms) to non-kinetic, laser-based ADR systems. Though currently still at the technology demonstration stage, on-orbit servicing may also be achieved in the near future with the integration of advanced robotics and sensor suites with specialised spacecraft and software for semi-autonomous servicing operations.[28] While kinetic ADR systems have a higher technology readiness level, they also pose a higher risk of collision and require complex rendezvous manoeuvring as part of the debris removal process.[29] Additionally, their development has sparked concerns as to the potential for misuse of ADR systems for ASAT engagements

A range of civil and commercial actors are investing in the development, testing and planned deployment of RPO, ADR and other technologies, speaking to the increasing relevance of such systems to the space economy. The United States has, for example, recently announced its plans for a post-2025 National Security Launch Architecture (NSLA) which seeks to engage the commercial on-orbit servicing market to develop on-orbit transfer and manoeuvring capabilities.[30] The European Space Agency (ESA) has meanwhile commissioned the world's first debris removal mission, ClearSpace-1, which is to take place in 2025.[31] ESA is also supporting ongoing tests on harpoons, nets, robotic arms and other technologies for capturing debris or decommissioned

---

[26] 'National Security Implications of Emerging Satellite Technologies' (n 24)
[27] 'To Clear or to Eliminate? Active Debris Removal Systems as Anti-satellite Weapons' (n 25)
[28] Mahashreveta Choudhary, 'On-orbit satellite servicing: Process, Benefits and Challenges' (2019) https://www.geospatialworld.net/article/on-orbit-satellite-servicing-process-benefits-and-challenges-2/ accessed 20 April 2021
[29] 'To Clear or to Eliminate? Active Debris Removal Systems as Anti-satellite Weapons' (n 25)
[30] These, among other factors, could reportedly also help secure US national security satellites against ASAT attacks. Source: Theresa Hitchens, 'Next-Gen SMC Launch Study Targets Satellite Maneuver' (*Breaking Defense*, 2019) https://breakingdefense.com/2019/10/next-gen-smc-launch-study-targets-satellite-maneuver/ accessed 20 April 2021
[31] ESA, 'ESA commissions world's first space debris removal', (*The European Space Agency*, 2019) https://www.esa.int/Safety_Security/Clean_Space/ESA_commissions_world_s_first_space_debris_removal accessed 3 May 2021

satellites and either de-orbiting them or transferring them to safe "graveyard orbits".[32] Russia and China have both reportedly carried out RPO missions, and their scientists are investigating the utility of ground-based lasers as a non-kinetic form of ADR.[33]

Many dual-use ASAT capabilities can be designed as military systems with primary non-ASAT designs (as for example, co-orbital satellites for use in space situational awareness activities).[34] Similarly, commercial and civil on-orbit repair and refuelling programmes could conceivably provide systems with a potential secondary ASAT application. As such, while the increasing interest in on-orbit servicing, assembly and manufacturing represent significant advances towards strengthening space security and sustainability, this also provides a growing challenge as technologies for approaching, capturing and manipulating space objects to advance PRO and ADR mature.[35]

As discussed in the next section, the dual-use conundrum produces complex impacts on space security and questions for international law, while exacerbating broader uncertainties regarding the potential for future weaponisation of space. Notably, the dual-use nature of RPO and ADR capabilities might be exploited to conduct ambiguous and deniable counter space operations in the "grey zone" below the threshold of armed conflict.[36] This could enable hostile actors to threaten satellites and probe NATO's defences and political resolve in this new operational domain, while trying to avoid triggering a full Article 5 response from the Alliance.

Understanding Potential Legal Implications of Dual-Use ASAT Capabilities

The dual-use conundrum poses a challenge to establishing the status of a space asset under international law and strengthening the international legal framework for safe and sustainable use of space overall. Strictly speaking, a

---

[32] ESA, 'Mitigating space debris generation' (*The European Space Agency*, 2021) https://www.esa.int/Safety_Security/Space_Debris/Mitigating_space_debris_generation accessed 3 May 2021

[33] Matt Williams, 'China has a plan to clean up space junk with lasers' (*PHYS.ORG*, 2018) https://phys.org/news/2018-01-china-space-junk-lasers.html accessed 3 May 2021

[34] Theresa Hitchens, 'Russia Builds New Co-Orbital Satellite: SWF, CSIS Say' (*Breaking Defense*, 2019) https://breakingdefense.com/2019/04/russia-builds-new-co-orbital-satellite-swf-csis-say/ accessed 20 April 2021

[35] ESA, 'Writing the Rules on Close-Proximity Orbital Operations' (2019) https://blogs.esa.int/cleanspace/2019/07/08/writing-the-rules-on-close-proximity-orbital-operations/ accessed 20 April 2021

[36] Ibid.

space weapon is defined as any system *designed* to attack targets.[37] However, a potential dual-use system, such as an orbital debris removal system, could be used in a different way than initially intended. It is therefore hard to define space weapons or ASATs, particularly when taking into consideration the dual-use nature of systems.

The difficulty of defining potentially harmful space-based systems under international law has driven interest in behaviour-based governance mechanisms to foster space security and sustainability. Building trust and agreeing basic norms of behaviour were central goals of the European Union (EU)'s abortive attempt to promote an international code of conduct in 2008.[38] They are similarly important in the UK-sponsored United Nations (UN) Resolution on responsible behaviours in outer space at the Plenary Meeting of the United Nations General Assembly in December 2020, which focuses on defining hostile behaviours rather than capabilities. Entitled "Reducing Space Threats Through Norms, Rules and Principles of Responsible Behaviours", the resolution pursues "norms, rules and principles of responsible behaviours" and "the reduction of the risks of misunderstanding and miscalculations with respect to outer space."[39] Maintaining this emphasis in mind, it is worth examining how the use of both dual-use systems and purposefully designed ASAT technologies may interact with international law, by firstly examining the Outer Space Treaty (OST), as well as the Law of Armed Conflict (LOAC) and Customary International Law (CIL).

Outer Space Treaty 1967 and ASATs

Contrary to occasional claims that space is an unregulated "Wild West", the OST sets out the basic framework for international space law upon which a host of other agreements build. It notably emphasises that the exploration and use of space is to be carried out for the benefit and interests of all countries and "all [hu]mankind", maintaining space free from claims of sovereignty and

---

[37] Todd Harrison, Kaitlyn Johnson, Thomas Roberts, 'Space Threat Assessment 2018' (*CSIS*, 2018) https://aerospace.csis.org/wp-content/uploads/2018/04/Harrison_SpaceThreatAssessment_FULL_WEB.pdf accessed 20 April 2021

[38] Council of the European Union, 'Council conclusions and draft Code of Conduct for outer space activities' (2008) https://data.consilium.europa.eu/doc/document/ST-17175-2008-INIT/en/pdf accessed 20 April 2021

[39] UN General Assembly, 'Reducing Space Threats Through Norms, Rules and Principles of Responsible Behaviours' (UN General Assembly, 2020) https://digitallibrary.un.org/record/3895440?ln=en accessed 20 April 2021

protecting its environment from damage and contamination.[40] Above all, it prescribes that space is to be used for peaceful purposes, banning the "establishment of military bases, installations and fortifications, the testing of any type of weapons and the conduct of military manoeuvres on celestial bodies."[41]

It is worth noting that the notion of "peaceful purposes" is not explicitly defined in the OST, with the United States viewing the term to mean "non-aggressive" and others as "non-military".[42] The U.S. interpretation of the principle of the use of space for peaceful purposes, enshrined in the 2020 National Space Policy, permits national security activities in space, including those relating to the right of self-defence.[43] Beyond its reference to structures, weapons and military exercises on celestial bodies, Article IV of the OST only prohibits the placement "in orbit around the Earth [of] any objects carrying nuclear weapons or any other kinds of weapons of mass destruction, install[ation of] such weapons on celestial bodies, or station[ing of] such weapons in outer space in any other manner".[44] As such, conventional ASAT weapons may not be explicitly prohibited from placement in orbit or stockpiling on Earth (e.g. for launch from land, maritime or air platforms).

Similarly, this provision does not prevent nuclear weapons transiting through space, such as intercontinental ballistic missiles.[45] While the OST's reference to "weapons of mass destruction" (WMD) typically evokes nuclear, biological, and chemical weapons, some argue that the term could be interpreted more widely to include ASAT weapons.[46] For instance, the Vienna Convention on the Law of Treaties emphasises the "ordinary meaning" of terms,

---

[40] 'Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (OST) UN RES 2222 (XXI)' (*Treaties & Principles*,1966) https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html accessed 20 April 2021

[41] Ibid.

[42] Almudena Azcárate Ortega, 'Placement of Weapons in Outer Space: The Dichotomy Between Word and Deed' (*Lawfare*, 2018) https://www.lawfareblog.com/placement-weapons-outer-space-dichotomy-between-word-and-deed accessed 20 April 2021

[43] Ibid.

[44] UN RES 2222 (XXI) (n 40)

[45] David Koplow, 'ASAT-isfaction: Customary International Law and the Regulation of Anti-Satellite Weapons' (*Georgetown Law*, 2009) https://scholarship.law.georgetown.edu/facpub/453/ accessed 20 April 2021

[46] Jeffrey Murphy, 'The Cold Vacuum of Arms Control in Outer Space: Can Existing Law Make Some Anti-Satellite Weapons Illegal?' (2019) 68(1) Cleveland State Law Review, https://engagedscholarship.csuohio.edu/clevstlrev/vol68/iss1/9/ accessed 20 April 2021

which would allow for an interpretation of WMD which looks beyond the means of the destruction (nuclear, biological etc.), instead focusing on the scale of the destruction ("mass").[47] It is worth noting that the scale of destruction caused by a single ASAT engagement can be significant; current estimates suggest that destroying a single large satellite could potentially double the current amount of large debris in low earth orbit.[48] Conversely, any attack is unlikely to generate large-scale loss of life, at least directly, given the small number of astronauts in orbit at any one time (e.g. living in the International Space Station or undertaking crewed spaceflight missions). However, disruption of satellite services could indirectly contribute to loss of life on Earth, potentially in unanticipated ways and locations, due to cascading failures of space-dependent systems, networks and infrastructure.

By generating debris, the use of ASATs may constitute a further violation of the OST. In 2007 China tested an ASAT weapon, destroying an old Chinese weather satellite and generating a sizeable cloud of satellite and missile fragments. Japan's former Prime Minister Shinzo Abe claimed the test violated the OST, as the treaty prohibits signatory states from purposefully generating debris in space.[49] Article I of the OST establishes space as "free for exploration and use by all States" to include "free access to all areas of celestial bodies,"[50] with debris resulting from the kinetic use of ASATs potentially restricting such free access to space.[51] Removing or damaging a satellite, kinetically or otherwise, may also violate the right to free exploration. Article VII of the OST goes on to establish that launching states are liable for "any damage caused by space objects or component parts",[52] which would include debris generated by ASATs.[53] While the development and deployment of ASATs may not currently be directly prohibited under international law, their use to deny space capabilities or access to others, or generate debris, may violate the OST. As such, the misuse of dual-use (including civilian) systems as ASATs could also be

[47] Ibid.
[48] Union of Concerned Scientists, 'Debris in Brief: Space Debris from Anti-Satellite Weapons' (2007) https://www.ucsusa.org/resources/space-debris-anti-satellite-weapons accessed 20 April 2021
[49] NTI, 'Japan's Space Law Revision: the Next Step Toward Re-Militarization?' (2008) https://www.nti.org/analysis/articles/japans-space-law-revision/ accessed 20 April 2021
[50] UN RES 2222 (XXI) (n 40)
[51] 'The Cold Vacuum of Arms Control in Outer Space: Can Existing Law Make Some Anti-Satellite Weapons Illegal?' (n 46)
[52] UN RES 2222 (XXI) (n 40)
[53] 'The Cold Vacuum of Arms Control in Outer Space: Can Existing Law Make Some Anti-Satellite Weapons Illegal?' (n 46)

prohibited under the OST.

LOAC and Customary International Law

International law justifies the use of force under special circumstances, provided that it is in exercise of the right to individual or collective self-defence as recognised by Article 51 of the UN Charter, or when authorised by a decision of the UN Security Council as critical for international peace and security, as per Article 42 of the Charter.[54] It is notable that no provision of the Charter or aspect of customary law imposes "any upper limit above the surface of the Earth on the legitimate exercise of the right of self-defence", meaning that space is not necessarily precluded from these laws despite the lack of sovereign territory or claims in that domain.[55]

LOAC sets out fundamental principles restricting the use of force: military necessity, distinction, and proportionality. Regarding an attack on space assets, as some satellites are dual-use, a kinetic or non-kinetic attack on them may negatively affect non-belligerents, raising challenges regarding the principles of distinction and proportionality. The space ecosystem is becoming more complex as militaries increasingly make use of commercial satellites; similarly, a single satellite might be used to host payloads for multiple nations and agencies, or to sell imagery or bandwidth to different customers on each pass of the Earth.

Furthermore, LOAC, Article 35 of Additional Protocol I establishes fundamental rules regarding the methods and means of warfare. Paragraph 3 of the Article states: "[I]t is prohibited to employ methods or means of warfare which are intended or may be expected to cause widespread, long-term and severe damage to the natural environment." The use of ASATs, including dual-use systems, could cause long-term damage, which could be prohibited under this provision, considering the widespread, potentially centuries-long and severe effects caused by space debris that could result from a kinetic attack on a satellite in certain orbits.[56]

---

[54] Promit Chatterjee, 'Legality of Anti-Satellites Under the Space Law Regime' (2014) 12(1) Astropolotics https://www.tandfonline.com/doi/full/10.1080/14777622.2014.891558?scroll=top&needAccess=true accessed 20 April 2021

[55] Fawcett, cited Maogoto, Jackson Nyamuya and Steven Freeland 'Space Weaponisation and the United Nations Charter Regime on Force: A Thick Legal Fog or a Receding Mist?' (2007) https://core.ac.uk/download/pdf/216908215.pdf accessed 20 April 2021

[56] Jackson Maogoto, Steven Freeland, 'The Final Frontier: The Laws Of Armed' (*SSRN*, 2008)

While the LOAC only applies to armed conflict, customary international law (CIL) applies more widely, including to testing.[57] CIL is considered less "definite" than treaty law, although it takes into account the full range of a country's "words as well as deeds, silences as well as inactions, and oral as well as written statements".[58] Previous ASAT test activity, notably by China in 2007 and the United States in 2008, has drawn criticism from other countries, but no assertions that such testing is illegal under CIL.[59] Instead of calls to "refresh" CIL to suppress ASAT activity, focus has remained on campaigning for the drafting of new treaties.[60] Hence, for now, besides the OST, the most important principles via which to assess the use of ASATs and increasing role of new dual-use systems remain military necessity, distinction, and proportionality.

Implications for NATO

Though it was only formally recognised in 2019, space is fast emerging as an important operational domain for NATO – one that is not only central to the Alliance's security and operations today, but also a major part of ongoing initiatives to modernise and transform joint operations for the future. This reflects the vital role of space-based ISR, PNT and SATCOM in helping realise the ambitions of HQ SACT and individual NATO Allies to embrace emerging concepts of "Multi-Domain" or "Joint All Domain Operations", field more networked forces and achieve information advantage in the face of growing counter space, cyber and electronic threats.[61] It is therefore important that NATO continues to "enhance its space domain awareness and understanding of the space environment, including potential risks and threats".[62]

Robust space domain awareness – supported by horizon scanning to understand possible emerging trends in technology, capability, or hostile intent – remains an essential prerequisite for any strategy for mitigating kinetic and non-kinetic threats in space. Given the key role of space situational awareness in facilitating safe and sustainable space operations, and mitigating potential

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1079376 accessed 20 April 2021

[57] 'ASAT-isfaction: Customary International Law and the Regulation of Anti-Satellite Weapons' (n 45)

[58] Ibid.

[59] Ibid.

[60] Ibid.

[61] James Black, Alice Lynch, 'Cyber Threats to NATO from a Multi-Domain Perspective' (*NATO CCDCOE*, 2021) https://ccdcoe.org/uploads/2020/12/7-Cyber_Threats_NATO_Multidomain_Perspective_ebook.pdf accessed 3 May 2021

[62] NATO, 'NATO's approach to Space' (2021) https://www.nato.int/cps/en/natohq/topics_175419.htm#:~:text=Space%20underpins%20NATO's%20ability%20to,companies%20based%20on%20their%20territory accessed 20 April 2021

threats caused by dual-use ASATs, NATO members could more actively facilitate robust detection and tracking as well as coordination and communication among space actors. This is particularly as the development of military ASAT capabilities (e.g. by Russia, China, and other adversaries or competitors) continues to be a serious concern for NATO Allies and partners. There is also a need for improved awareness of dual-use RPO and ADR systems and the potential for misuse of such systems in the "grey zone" below the threshold of armed conflict. Tracking advances in military ASATs alone is unlikely to sufficiently advance the Alliance's understanding of such future threats. The dual-use nature of many RPO and ADR technologies therefore indicates the need for broader market intelligence and monitoring of technological advances across the commercial, civil and military sectors.

The potential abuse of dual-use ASAT technologies is not only an issue for space security but also concerns wider space safety and sustainability. A recent RAND submission to the UN in relation to the current UK-led resolution on "Responsible Behaviours" notes that, given the greater barriers to achieving consensus concerning matters of space security, discussions on space safety should be prioritised to facilitate progress in strengthening international governance and the current rule of law framework for uses of space.[63] As such, it should be noted that international governance and law relating to the dual-use conundrum may evolve outside the immediate and more narrowly defined limits of space security, in the context of wider discussions on space safety and sustainability.

NATO members may seek to contribute to this dialogue towards shaping norms and rules in international space law, working together to ensure a coherent approach based on shared interests and values. This should also include engaging with industry, academic and civil society perspectives – something which the Alliance already does through various fora and mechanisms, but which is especially important in space given the complex, multi-stakeholder and dual-use nature of the domain. There may be beneficial lessons from how NATO has contributed to the evolving debate over norms of behaviour and international legal aspects of cyberspace, another "new" domain only formally recognised by the Alliance in 2016. At the same time, it is important to recognise and pursue the safety (and therefore security) benefits that maturing RPO and ADR technologies may bring to NATO members if they are used for peaceful purposes.

[63] 'Responsible Space Behaviour for the New Space Era' (n 6)

NATO's evolving approach to space will remain in accordance with international law, but the same cannot necessarily be said about the Alliance's potential adversaries. Some of the ambiguities in the OST do not establish clear and universally understood parameters for ASATs specifically designed for military use, let alone the more ambiguous case of civilian systems with potential dual uses. It is hence important to pursue an understanding of international space law that emphasises and prescribes hostile behaviours rather than capabilities. As more state and non-state actors establish a presence in space, the Alliance and its members will need to remain aware of global developments and advocate for the peaceful use of space, while also taking steps to enhance resilience, safeguard critical assets and deter hostile action.

The principles of military necessity, distinction and proportionality are likely to remain as important as ever, considering the devastating potential impacts of an attack on satellites. This is true not only for NATO's joint or multi-domain operations, but also for wider economies, society and civilian infrastructure, as well as the space environment. It is important that continued attention is given to preserving this fragile space environment, which is essential towards the continued exploration and use of space for the benefit and interests of all of humankind, including the international peace and security that is at the core of the Alliance's terrestrial mission.

***

Source: www.nato.int

'Heavens Open' - The Need for Increased Data from Space and Creating a Duty to Share that Data[1]

by Christopher J. Newman[2] and Matthew G. Zellner[3]

Introduction

Of all of the wicked problems that bedevil human operations in space, the management of space objects within the Earth's orbital environment is proving to be one of the most challenging. Space is a multi-national and multi-sectored common area, where scientific investigators and commercial actors work alongside sensitive military activities. The ubiquity of space applications in

[1] **DISCLAIMER**: The views expressed in this article are solely those of the authors and may not necessarily represent the views of NATO, Allied Command Operations, Allied Command Transformation, or of their affiliated organizations, or the U.S. Department of Defense and its components, or Northumbria University.

[2] Professor of Space Law and Policy, Northumbria University, Newcastle, United Kingdom.

[3] Major, U.S. Air Force; Chief of Space, Operations, and International Law at Combined Force Space Component Command and Space Operations Command-West, Vandenberg Air Force Base, California. Major Zellner used only information available to the public in the researching and presentation of this work.

society, coupled with the dependency of a whole range of essential earth-based systems, means that national governments are expending considerable resources figuring out how best to defend the space hardware underpinning these critical systems[4]. Indeed, space has become a 'strategic centre of gravity'[5] with individual nations and collective alliances looking to ensure that they can enjoy the continued benefits that space brings whilst having protection from threats to their space-based infrastructure.

This growing dependence on space, coupled with the increased awareness of the vulnerability of space hardware, has been heightened by the dramatic upsurge in the number of active satellites, particularly in Low Earth Orbit (LEO)[6]. All of this has led to an increased focus on the space surveillance and tracking capabilities to monitor both the passage of traffic in the Earth orbital environment and to better understand and identify behaviour in space operations that can escalate tensions between countries[7].

This discussion will advocate not only for openness and transparency in the handling and dissemination of this data about space, but also that there should be an obligation to provide such openness and transparency. Such an approach is both vital to ensure a complete picture of busy orbital paths and is strategically desirable. In addition to the Space Situational Awareness (SSA) sharing agreement programme that is already in place[8] and the provisions of space-track.org, States need to provide as much information about the orbital environment as possible, and this will include increasing investment in space surveillance and tracking (SST) capacity.

Increasing the amount and availability of data will allow the United States and its allies to demonstrate openness and collaboration. It will also be possible to use this freely available information to shine a light on behaviours that cause

---

[4] See Robert S. Wilson et al, *The Value of Space*, (Aerospace Corporation, May 2020), available at: https://aerospace.org/paper/valueofspace [Accessed 18 April 2021].
[5] Patrick K. Gleeson, 'Perspectives on Space Operations' (2007) 5 Astropolitics 2 145-172.
[6] Low Earth Orbit (LEO) is 'normally at an altitude of less than 1000km but it could be as low as 160km' ESA, 'Low Earth Orbit'. Available at: https://www.esa.int/ESA_Multimedia/Images/2020/03/Low_Earth_orbit#:~:text=A%20low%20Earth%20orbit%20(LEO,very%20far%20above%20Earth's%20surface [Accessed 18 April 2021].
[7] See for example, Regina Peldszus and Pascal Faucher, 'European Space Surveillance and Tracking Support Framework' in Kai-Uwe Schrogl, Peter L. Hays, Jana Robinson, Denis Moura, Christina Giannopapa (Eds.) *Handbook of Space Security Springer* (Springer 2020), 883-904.
[8] United Space Strategic Command (USSTRATCOM) has over 100 SSA data sharing arrangements in place with 20 nations, ESA and commercial actors see, for example: https://www.stratcom.mil/Media/News/News-Article-View/Article/1825882/100th-space-sharing-agreement-signed-romania-space-agency-joins/ [Accessed 18 April 2021].

international tension and threaten the stability of the space environment. It is not within the purview of this discussion to advocate specific solutions - that is a much more extensive discussion[9]. Nor will it seek to engage in a technical critique of existing provision for monitoring the Earth's orbit. It is the core principle and the fundamental legality underpinning the sharing of information that will be assessed.

This article will outline some of the definitional issues that can obfuscate discussions on tracking space objects. The inquiry will then examine the extant legal position as to the requirements for sharing information about space objects. Following on from this will be a critique of the current strategic position regarding the opaque aspects of data and information sharing. The work will conclude by advancing the creation of an overarching regime underpinned by data sharing that provides for transparency of activity, greater provenance in the quality of data and ways in which such a regime can embed security and positive behaviour at its heart.

Understanding Space Situational Awareness

Throughout this discussion, several discrete functions regarding the monitoring of the orbit of the Earth will be examined. A fundamental starting point is the term Space Situational Awareness (SSA) itself, the umbrella term for the pursuit of a complete understanding of the orbital environment. SSA aims to characterize the space environment and activities in space[10]. In order to conduct the monitoring of the orbital environment and the behaviour of the various actors, a range of dedicated SST sensors (e.g., radar, optical, laser ranging) acquire data on objects (e.g., active and non-active satellites, debris, fragmentations, re-entries), which are then processed as part of a catalogue.[11] Satellites operate in different orbits, and those orbits have other observational requirements; this means that data collection from a variety of sensors is required[12].

In essence, however, the first and most fundamental aspect of SSA is acquiring as much data as possible, from the different orbital planes, and from

[9] Peldszus and Faucher, (n4)
[10] Brian Weedon, 'Space Situational Awareness Fact Sheet', (2017) Secure World Foundation available online at: https://swfound.org/media/205874/swf_ssa_fact_sheet.pdf [Accessed 18 April 2021]
[11] Regina Peldszus, 'Foresight methods for multilateral collaboration in space situational awareness (SSA) policy & operations' (2018) 5 Journal of Space Safety Engineering, 115-120, 115
[12] Ibid

as many sources as possible. As stated above, it is not the purpose of this discussion to critique the current technical arrangements for surveilling the orbital environment. It would, however, be remiss not to point out that the dramatic increase in the number of space objects being placed in orbit needs to be accompanied by an equally dramatic rise in SST capacity if the data-sharing provisions advocated herein are to enjoy their full potential.

The acquisition of data from space is, however, only part of the process. For the data to be of use, the tracking and sensing information mentioned above needs to be analysed and combined with information about the naturally occurring space environment - such as ambient space weather conditions to produce warnings and collision avoidance advice[13]. At present, the United States is recognised as having a hegemonic position regarding both the physical hardware and the dedicated resources for operating SSA. While the US's notion of domain situational awareness can be traced back to World War II airspace,[14] and the "first formalized effort to catalogue satellites" occurred in the late 1950's,[15] the modern genesis of today's construct was the establishment in 1979 of the United States Space Defense Operations Centre to "command and control the space surveillance network."[16] It was founded amidst the recognized needs to facilitate space surveillance, protect space systems used for battle management, communications and intelligence, and prevent hostile uses of space by adversaries.[17]

While the United States' focus on space surveillance understandably waned after the fall of the Soviet Union and spiked in the aftermath of China's 2007 destructive anti-satellite missile test[18], the notion of external sharing of SSA data can be traced to the 2004 National Defense Authorization Act, which authorized the Department of Defence's creation of a "pilot program for the provision of satellite tracking support to entities outside the United States

[13] Peldszus (n11) 115
[14] Laurence Nardon, 'Space Situational Awareness and International Policy', (Ifri 2007) 1, available at: https://www.ifri.org/sites/default/files/atoms/files/docu14ssanardon.pdf [Accessed 18 April 2021].
[15] Felix R Hoots, Paul W. Schumacher Jr.; Robert A. Glover 'History of Analytical Orbit Modeling in the U. S. Space Surveillance System' (2004) Journal of Guidance Control, and Dynamics, 174
[16] Mark A. Baird, 'Maintaining Space Situational Awareness and Taking It to the Next Level', (2013) Air and Space Power Journal, 55
[17] Ibid 55
[18] Ibid 56

Government.[19] This was codified into an evolving statute,[20] and laid the groundwork for today's robust SSA sharing program.

A few years later, the program received additional impetus by then-President Barack Obama's 2010 National Space Policy[21]. In the stated interest of preserving the space environment and encouraging the responsible use of space, it directed the development and maintenance of SSA using commercial, civil, and national security sources, the pursuit of debris mitigation and removal measures, and collaboration;

"… [with] industry and foreign nations to *maintain and improve space object databases; pursue common international data standards and data integrity measures; and provide services and disseminate orbital tracking information to commercial and international entities, including predictions of space object conjunction.*"[22]

These objectives have been restated in later policy documents, including 2018's Space Policy Directive-3[23] and 2020's National Space Policy.[24] Currently, the United States through its Department of Defense has more than 100 SSA Sharing Agreements with foreign governments, universities, and commercial satellite operators, whereby Agreement holders receive specialized "space information such as conjunction assessment, launches, deorbits, and re-entry assistance."[25] The stated purpose of the program is to "foster openness, predictability of space operations, and transparency in space activities."[26] The Department of Defense tracks more than 23,000 objects on-orbit and disseminates the information through the public facing Space-track.org website.[27] Agreement holders share and receive additional detailed information, while any member of the public can create a free account and

---

[19] 2004 NDAA, Public Law 108-136, 108th Congress, Section 913
[20] 10 USC 2274, Space situational awareness services and information: provision to non-United States Government entities
[21] See National Space Policy of the United States of America promulgated on 28 June 2010 available at: https://history.nasa.gov/national_space_policy_6-28-10.pdf [Accessed 18 April 2021] 1
[22] ibid 7-8.
[23] Space Policy Directive-3 (2018) Section 4 available online at https://trumpwhitehouse.archives.gov/presidential-actions/space-policy-directive-3-national-space-traffic-management-policy/ [Accessed 18 April 2021].
[24] National Space Policy Federal Register, section 3(a) (xi).
[25] See above (n 5)
[26] Ibid
[27] See https://www.space-track.org/documentation#faq [Accessed 18 April 2021] for further information

obtain satellite catalogue, positional, decay, and re-entry data.[28]

The information on space-track.org is freely accessible. Participation and data sharing in the program is, however, on a voluntary basis. There are no international treaties or other agreements which mandate the provision of information. Similarly, there is no legal duty to provide additional information. The delivery of information through this voluntary mechanism is rooted in pragmatism and an attempt to provide a basic level of service. The significant increase in active satellites, particularly smaller satellites acting under shared control in large constellations, means that the current provisions for both gathering and sharing SSA information may well be shown up as inadequate. This discussion will now go on to examine whether there is any legal duty that could be relied upon to mandate an increase in SST capacity and the subsequent sharing of any information gained as a result.

The current legal framework: No duty to share data?

In order to establish the extent of the duty on nations to share information, it is first necessary to explore the legal framework that governs international activity in outer space. The primary instrument of international law which regulates national activity in outer space is The Treaty on Principles Governing the Activities of States in the Exploration Use of Outer Space, including the Moon and Other Celestial Bodies, known colloquially as the Outer Space Treaty (OST)[29]. This is a universal treaty opened for signature in 1967. As with other international treaties[30], the OST does not provide the granular detail or 'rules of the road' for actions in space. Instead, it contains several foundational principles which shape how Nation-States should conduct space activity. The OST grants certain freedoms relating to these activities, which it then regulates by specific limitations.[31] Throughout the Treaty are woven aspirational notions that led the countries to create such a binding instrument. These concerns are clearly articulated in the preamble to the Treaty and highlight the need for space activity to be for peaceful purposes and benefit all nations.

---

[28] https://www.space-track.org/documentation#/odr [Accessed 18 April 2021].
[29] Treaty on Principles Governing the Activities of States in the Exploration Use of Outer Space, including the Moon and Other Celestial Bodies, London, Moscow and Washington, opened for signature 27 January 1967, entered into force 10 October 1967; 6 ILM 386 (1967); 18 UST 2410; TIAS 6347; 610 UNTS 205; 1968 UKTS 10, Cmnd 3519.
[30] For detailed description of the negotiating history see Stephan Hobe, Bernhard Schmidt-Tedd, & Kai-Uwe Schrogl (Eds.), *Cologne commentary on space law* (Vol. I). Cologne, Germany: (Carl Heymanns Verlag 2009)
[31] Stephan Hobe, 'Article I', ibid 27

The OST does not have any specific mention of a duty upon States to track their space objects, much less to share information about this tracking. This is, perhaps, not surprising, as the Treaty was a product of the Cold War race to the Moon and drafted at a time when there were only two nations, the USA and USSR, launching a few objects into space.[32] The resulting Treaty that emerged was as much a security treaty as anything else,[33] with the prohibition of placement of nuclear weapons in space under Article IV attracting most of the headlines at the time.[34] Nonetheless, to ensure the two superpowers did not look to restrict access of other countries, Article I of the Treaty provides that all States are granted the right to engage in scientific investigation in space and use or explore space.

To reinforce unhindered access to space for all States, Article II of the OST confirmed that territorial sovereignty principles do not apply in space, and any appropriation of any area of outer space is expressly prohibited[35]. The OST recognizes that the regime of sovereign control and tracking that underpins airspace is not appropriate for regulating outer space. Instead - as with other common areas such as Antarctica - it provides that no State can exercise sovereign rights in such a domain.[36] In signing the Treaty, national governments accept international responsibility for the activity of their nationals or other non-governmental entities within their jurisdiction.[37] States that launch a space object, procure a launch or allow their territory or facilities to be used for launching a space object, are, "*internationally liable for damage to another State or to its natural or juridical persons by such object or its component parts on the Earth, in air space or outer space.*"[38]

---

[32] See Joanne Gabrynowicz, 'Space Law: Its Cold War Origins and Challenges in the era of Globalization' (2004) 37 *Suffolk U L Rev* 1041

[33] P.J. Blount 'Renovating Space: The Future of International Space Law' 40 Denv. J. Int'l L. & Pol'y 515 2011-2012

[34] Article IV of the Treaty did not completely remove nuclear weapons from the sphere of space activity. The provisions of Article IV (part 1) prohibit the *stationing* of nuclear weapons and weapons of mass destruction (WMD) 'anywhere in extra-terrestrial space'. The Treaty does not, however, prohibit the transit through outer space for intercontinental ballistic missiles. See Cheng (n 27) 246

[35] Article II of the OST provides that 'Outer space, including the Moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means.' For a broader explanation of the concept of *Res Communis* see James Crawford, Iain Brownlie, *Brownlie's Principles of Public International Law* (Oxford University Press 2012), 203.

[36] Hobe (above n 31) 27

[37] Outer Space Treaty 1967, Article VI.

[38] Outer Space Treaty 1967, Article VII. The provisions in Art. VII were expanded by The

Even before the drafting of the OST, the international community had recognised the importance of keeping a log of objects in orbit and beyond.[39] Article VIII of the Treaty codified this registration regime and provides that a State 'on whose registry an object launched into outer space' shall retain 'jurisdiction and control over such object'[40]. The requirement of registration was two-fold. It was to collect information on what space objects were being placed in orbit and to provide, in a sovereignty-free area, 'a chain of attribution between the launching state, the space object, international responsibility and jurisdiction and control'.[41] Article VIII and the subsequent Registration Convention[42], are provisions that create a historical record of objects placed in orbit. Still, it would seem that nowhere in the Treaty is there a duty on States to track their objects after launch, much less for States to share that data with other users of the space environment.

An implied duty to share data: OST Redux

The OST does not contain an explicit duty to track space objects. Nonetheless, usage, exploration and scientific investigation of space under Article I needs to be undertaken following the limitations and obligations outlined in the rest of the Treaty. Perhaps most crucially, Article III of the OST provides that State Parties to the Treaty,

> *'shall 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*

Convention on International Liability for Damage caused by Space Objects, 29 March 1972; 961 UNTS 187; 1974 UKTS 16, Cmnd. 5551; 24 UST 2389, otherwise known as The Liability Convention.

[39] The UNGA Resolution 1721B (XVI) on 'International co-operation in the Peaceful Uses of Outer Space' was adopted by the General Assembly on 20 December 1961 and provided for the creation of an international voluntary registry of space objects.

[40] Outer Space Treaty 1967, Article VIII

[41] Bernhard Schmidt-Tedd and Stephan Mick, 'Article VIII' in Hobe (n30) 147

[42] Convention on the Registration of Objects Launched into Outer Space, opened for signature 14 January 1975, entered into force 15 September 1976; 14 ILM 43 (1975); 28 UST 695; TIAS 8480; 1023 UNTS 15, 1978 UKTS 70, Cmnd 7271. For further information about this please see Frans G. von der Dunk, "The Registration Convention: Background and Historical Context", (2003) 32 Space, Cyber, and Telecommunications Law Program Faculty Publications available at: https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1031&context=spacelaw [Accessed on April 18 2021]

international cooperation and understanding'[43].

Indeed, it has been observed that 'references to cooperation, consultation and due regard for the interests of other States recur throughout the Treaty (Article I, para 3, X, XI)'.[44] The very ethos underpinning the OST is, therefore, one of cooperation between States.

Article IX of the OST is perhaps the closest expression of this need for cooperation and one which, at first blush, suggests legal support for an 'Open Skies' approach to the sharing of SST data. The first sentence of Article IX provides that '*in the exploration and use of outer space… States shall be guided by the principle of cooperation and mutual assistance and shall conduct all their activities in outer space, including the Moon and other celestial bodies, with due regard to the corresponding interests of all other States Parties to the Treaty*'.[45] This requirement permeates all of the space activities for which a State is internationally responsible under the OST[46]. The provision of registration is dealt with separately under Article VIII. A registry merely provides a document of what has been sent up; it does not provide details of where objects are currently.

To satisfy the due regard provision of Art IX, States that have international responsibility for national activities (under Article VI) must be able to locate their space objects and provide freely available information on those objects' locations. It is not explicit in the Treaty, but it would seem a logical result of the principles within the OST. The principle of 'due regard' is well recognised in international law[47], first appearing in the Chicago Convention of 1944. It is a specific qualification upon the unfettered freedom of States to use and explore space. Indeed, the requirement of due regard should mean that States have done everything possible to prevent a harmful act from occurring[48]. Operators looking to make informed decisions about a spacecraft need to have as much information about the space environment as possible. It is not unreasonable to expect States to provide all the information they have collected about that

[43] Outer Space Treaty 1967, Article III
[44] Francis Lyall and Paul B. Larsen, *Space law: A treatise* (2nd edn, Routledge, 2018) 53
[45] Outer Space Treaty 1967, Article IX.
[46] Lyall and Larsen (n 37) 267
[47] Sergio Marchisio 'Article IX' in in Stephan Hobe, Bernhard Schmidt-Tedd, & Kai-Uwe Schrogl (Eds.), *Cologne commentary on space law* (Vol. I). Cologne, Germany: (Carl Heymanns Verlag 2009) 175
[48] Ibid 176

environment to prevent a harmful act, such as a collision.

Strategic imperatives for increased data sharing

States utilize outer space as an enabler for a range of government functions, including those relating to national security. Military satellites enable "navigation, communications, weather, and technology development missions, in addition to intelligence gathering."[49] Exact statistics are impossible to garner but estimates indicate roughly one third of the 3,372 operational satellites on orbit serve governmental functions, whether civilian or military.[50] Even if States provide complete transparency on a large percentage of those satellites, that still leaves hundreds lacking key public-facing data. This is unsurprising, considering the aforementioned dearth of legal regimes obligating data sharing and the obvious strategic benefit derived from withholding functional and orbital details from adversaries. The latter underscores an enduring moral hazard hearkening back to Thucydides' exposition on the delicate balance of the crucial attainment of power with adherence to international order and norms of justice.[51]

According to the UN Office of Outer Space Affairs, "over 88% of all satellites, probes, landers, crewed spacecraft and space station flight elements launched into Earth orbit or beyond have been registered."[52] These filings in accordance with the Registration Convention comprise "launching state, date and location of launch, basic orbital parameters and general function of the space object."[53] There are two crucial limitations on this data. First is the sheer time taken for States to file details of launches within the registry? The Convention nebulously allows States to furnish this *post facto* information 'as soon as practicable', with updates requested 'from time to time'.[54] While this was likely drafted to accommodate comparatively lacking communications and monitoring technology of the 1970s, it has since been exploited by some States to delay reporting by several years.[55] In fact, approximately 140 space

---

[49] See above (n1).
[50] How many satellites are operating in space? | World Economic Forum (weforum.org); *see also* Satellite Database | Union of Concerned Scientists (ucsusa.org)
[51] For details of how this could apply to space see Joan Johnson-Freese, *Space Warfare in the 21st Century* (Routledge 2016) 56
[52] https://www.unoosa.org/oosa/en/spaceobjectregister/index.html
[53] ESPI, *Towards a European Approach to Space Traffic Management*. (2020) ESPI Report 71, 56 [online] European Space Policy Institute. Available at: <https://espi.or.at/publications/espi-public-reports/category/2-public-espi-reports> [Accessed 18 April 2021].
[54] UN Registration Convention, Article IV, sections 1-2.
[55] Ram S. Jakhu, Bhupendra Jasani, and Jonathan C. McDowell, "Critical issues related to

objects have been registered 'after a 10 year or longer delay'.[56]

Second, the information does not provide any scrutiny of how the State of Registry has classified the object's function. This is perhaps 'the most abused aspect of the Convention, as military and intelligence satellites are rarely acknowledged as such'.[57] Military payloads specifically "are inadequately reported or, more often than not, they are not reported at all'.[58] These omissions certainly contribute to the 12% of objects not registered, leaving hundreds of space objects without even elementary reporting of information. The combination of State motivations to obscure operational information and the gaps in governance have unsurprisingly led to the concealment of vast arrays of national security satellites currently in Earth orbit.

At first blush, restricting information about highly classified assets in space would seem to be appealing to both preserve classified assets and the capability of those assets. Yet, when considered holistically, such hoarding of information by States is counterintuitive. Veiling orbital data may benefit covert government and military operations in the short term but it significantly increases the risk to spaceflight safety *for all* in the long term. This, in turn, means that any temporary advantages are offset by an increase in tension and a loss of moral authority. The manifest problem with concealing orbital data is the reduction in ability to predict, and thus avoid, potentially catastrophic collisions. The combination of an ever-increasing orbital population and lack of data sharing regarding position and characteristics of space objects in orbit is lurching the international community towards an eventual outcome which poses an existential threat to human space activity[59]. The sky may not be falling, but every time a State conceals data in the interest of national security, it incrementally adds to the unpredictability of space operations, can be viewed as being antagonistic and renders space less useful as a domain of operations.

Operational support for data sharing

Naturally, these considerations have led to attempts on an international level to try and produce some sort of framework. These initiatives have yet to

registration of space objects and transparency of space activities" [2018] 143 Acta Astronautica, 406-420, 409

[56] Ibid

[57] Ibid 411

[58] Ibid

[59] Christopher J. Newman and Mark Williamson, "Space sustainability: reframing the debate" [2018] 46 Space Pol. 30-37, 31

produce any tangible results. Indeed, having fully accessible data is only part of the solution. The application of the data received from SSA, in the form of some sort of space traffic management (STM) regime, is the natural corollary of extended data sharing. While "not defined under international space law, discussion of STM appeared first in the 1980s"[60] and continues to be discussed. Indeed, so pressing has the need been for managing orbital traffic that several aforementioned Presidential and Congressional actions have been taken over the years, directing the US to take the lead on STM. Nonetheless, the stark truth remains: without sufficient SST data, any STM regime will struggle to be effective.

Alongside the rise of STM, the rapid increase in space-capable actors and realization of the potential for misunderstanding in space activities has led States and international organizations to begin parallel efforts aimed at identifying desirable behaviour in space operations.[61] In 2013, the UN established a Group of Governmental Experts (GGE) whose final report underscored the need for "transparency and confidence-building measures in outer space activities," a measure that can only be achieved by increasing SST capacity.[62] Within their report, the GGE attempted to codify desired State obligations whilst accepting the reality that States will engage in covert operations, recommending "States may exchange general information on their…space activities and provide risk reduction notifications for foreseeable hazardous situations."[63]

While correctly underscoring certain similarities between openness in space activities and arms control management, the 2013 GGE and similar informal efforts[64] do little more than reaffirm that data sharing and transparency increase the safety of outer space. In November 2020, the UN General Assembly (UNGA) First Committee approved the UK-led resolution 'Reducing threats through Norms, Rules and Principles of Responsible Behaviours'[65]. The

[60] Ntorina Antoni, Christina Giannopapa and Kai-Uwe Schrogl, "Legal and Policy Perspectives on Civil-Military cooperation for the establishment of Space Traffic Management" [2020] 53 Space Policy, 2
[61] Ibid 2-4.
[62] Group of Governmental Experts on Transparency and Confidence Building Measures in Outer Space Activities, UN GAOR, 68th Sess UN Doc A/68/189* (July 29 2013) Available at: https://www.un.org/ga/search/view_doc.asp?symbol=A/68/189 [Accessed 18 April 2021]
[63] Ibid 15.
[64] Antoni (n 48) 2-4.
[65] UN General Assembly Resolution 75/36, Reducing space threats through norms, rules and principles of responsible behaviours A/RES/75/36 (7 December 2020) available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/354/39/PDF/N2035439.pdf?OpenElement [Accessed on

UNGA resolution (A/RES/75/36) aims to 'broker an international consensus on responsible behaviour in space'. This includes helping to improve transparency and confidence building measures in respect of space activity. Whilst there have been previous attempts at this, most notably the European Code of Conduct on Outer Space Activities[66], these attempts were subject to considerable resistance. Some States viewed them as either an attempt to impose 'backdoor' arms control treaties, unnecessarily limiting space activity or, as ageing European powers seeking to unilaterally impose behaviour in a top-down fashion without consultation[67]. While the session scheduled for September 2021 may not produce any concrete frameworks, it will be instructive to see the extent to which States are willing to engage in producing binding obligations.

Conclusion

There are both strategic and environmental reasons why space tracking data *should* be shared. It is suggested that these override any potential strategic advantages of covertness in either operations or capability. The extant space law, in the form of the Outer Space Treaty, whilst not having explicitly mandated data openness, was clearly intended to promote international collaboration and cooperation. The sharing of data and the enhancement of individual national SST capability must surely come within the ambit of such cooperation. Crucially, the issue is one of safety in space operations. If any form of STM is to be introduced, it needs to be based on as complete a set of data as is available. With state actors using increasingly sophisticated satellite manoeuvres to gather intelligence, and commercial operators engaging in rendezvous and proximity operations, enhancing the flow of information about space is going to become essential.

It is not within the purview of this discussion to advocate *how* such data should be shared, but ideally the arrangement would be a formalised network between States, based on an internationally agreed mechanism. In the

April 18 2021]

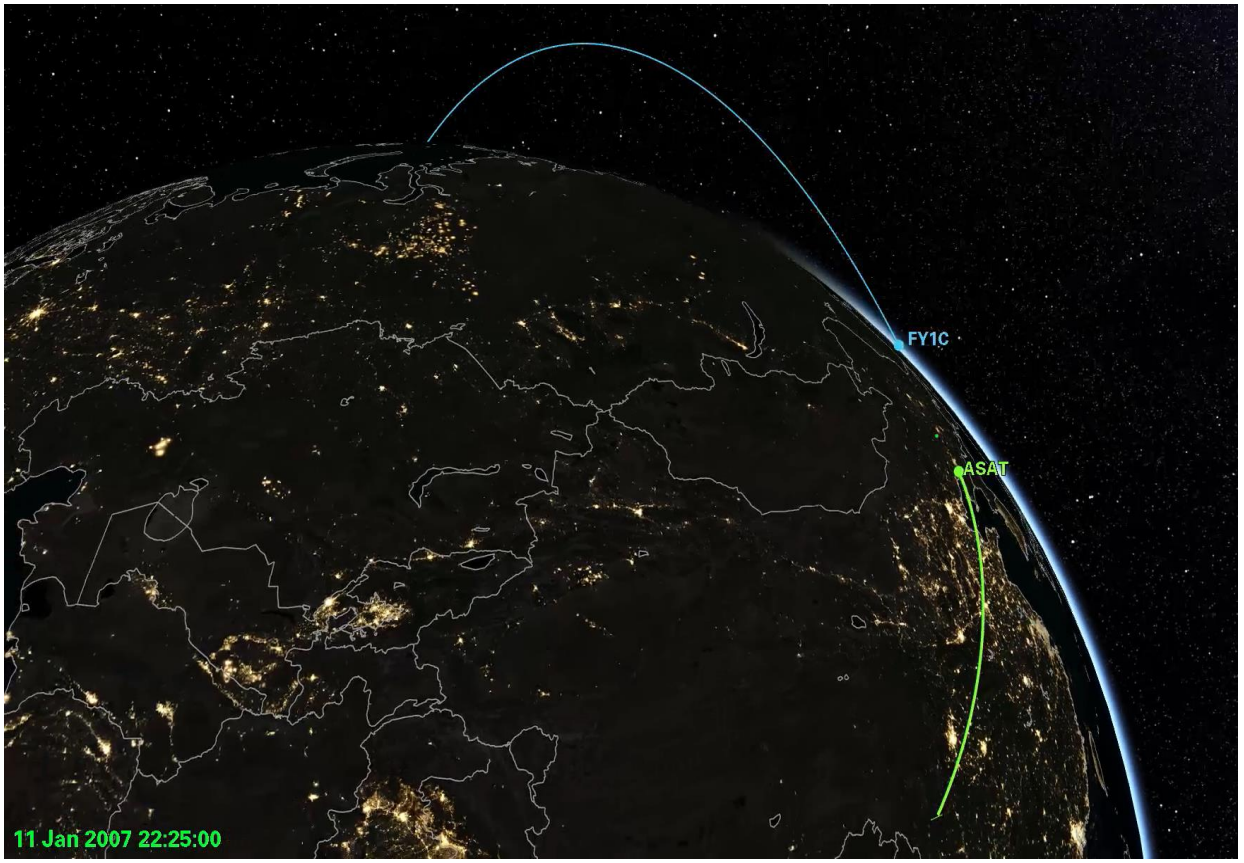
[66] Council of the European Union, Version March 31, 2014, Draft International Code of Conduct for Outer Space Activities, available at: https://eeas.europa.eu/archives/docs/non-proliferation-and-disarmament/pdf/space_code_conduct_draft_vers_31-march-2014_en.pdf [Accessed on April 18 2021]

[67] Jack M. Beard, "Soft Law's Failure on the Horizon: The International Code of Conduct for Outer Space Activities" (2016) 87 Space, Cyber, and Telecommunications Law Program Faculty Publications available at: http://digitalcommons.unl.edu/spacelaw/87 [Accessed on April 18 2021]

absence of a codified behavioural schema, the more that States voluntarily share orbital data, the greater the likelihood of public and political pressure being placed on those that do not. If enough nations participated, then departures from this baseline could be highlighted and international pressure brought to bear.[68] It is possible several States already have or are developing their own space object tracking mechanisms, in which all their object data is or will be openly shared. However, to begin the gradual process towards binding rules, States must first embrace the core principle of transparency in space tracking, allowing openness and safety to outweigh the individual benefits of strategic concealment.

***

[68] For example, in July 2020 the UK joined with the USA in protesting against what was seen as alarming veiled Russian space activities. See https://www.bbc.com/news/world-europe-53518238



Source: COMSPOC Corporation

Debris-creating Anti-satellite Weapons and Their Indiscriminate Effects[1]

by Christopher D. Johnson[2]

Introduction

Satellites make attractive targets. Undefended, they silently orbit the Earth in coldness and darkness, steadfastly performing their duty. At the same time, they often serve as critical components of a State's military infrastructure,

[1] **DISCLAIMER**: The views expressed in this article are solely those of the author and may not necessarily represent the views of NATO, Allied Command Operations, Allied Command Transformation, or of their affiliated organizations, or of the author's employers.

[2] Christopher D. Johnson is the Space Law Advisor at the Secure World Foundation and an Adjunct Professor of Law at Georgetown University Law Centre.

The author wishes to thank David Koplow, Jonathan McDowell, Dan Oltrogge, Daniel Porras, Victoria Samson, Brian Weeden, and Jessica West for their helpful comments. All remaining errors are entirely my own.

The author thanks Dan Oltrogge, COMSPOC Corp., Dr Aaron Boley, UBC Physics and Astronomy, and Todd Harrison, CSIS for permission to use their images and graphics.

in continual service to planners and decision-makers here on Earth. Regarding the purported easier decision-making surrounding the targeting of satellites, it is often remarked that "satellites don't have mothers." Consequently, the reasoning goes, satellites make more attractive targets than terrestrial military objectives – especially when non-combatants and civilian objects are near those terrestrial options. Additionally, if an adversary in an armed conflict is particularly reliant on their space infrastructure, their spacecraft might be the "Achilles' heel" that military minds are looking for, and thus even more inviting.

However, the intentional destruction of on-orbit spacecraft travelling at high speeds in Earth orbit is likely to create debris fields that are both long-lived (persisting over long time-spans), vast in physical dimension, continually changing, creating miniscule pieces impossible to track, and flying through orbits used by a multiplicity of other users of the space domain. In choosing the option to strike a satellite, military commanders risk creating debris fields that threaten to damage others in the space domain, including actors not participating in the conflict.

Due to the size and long life of debris fields, can their intentional creation ever conform to international humanitarian law's strictures on attacks in armed conflict, including the prohibition on indiscriminate attacks?

This article will explore whether the intentional creation of space debris through targeting of an adversary's satellites in the course of an international armed conflict may violate various relevant and applicable norms. Additionally, and crucially, other regimes of international law (including international space law and international environmental law) inform any analysis of the legality of targeting spacecraft, and of the foreseeable mass debris creation it brings.

Discussions and scholarship regarding the legality of anti-satellite attacks is not new.[3] However, this article updates the discussion with relevant facts surrounding historical and recent debris-creating events, including a richer view of the current space domain and uses of outer space. These additions update the legal analysis in a way that re-characterizes and reinforces past scholarship.

[3] David Koplow, 'ASAT-isfaction: Customary International Law and the Regulation of Anti-Satellite Weapons' [2009] 30 Michigan J Intl L 4, 1187; David Koplow, 'An Inference about Interference: A Surprising Application of Existing International Law to Inhibit Anti-Satellite Weapons' [2014] 35 Pennsylvania J Intl L 3; William Boothby, 'Space Weapons and the Law' [2017] 93 Intl L Studies 179; Cassandra Steer and Matthew Hersch (eds), *War and Peace In Outer Space* (OUP 2021).

Overview of Sources of Laws Applicable to Anti-satellite Attacks

A host of relevant international rules regulate the creation of debris in outer space. These rules are found in the special regimes of international space law, international environmental law, and international humanitarian law (IHL). Some of these rules may primarily apply during peacetime (which includes times of rising tension), while other rules regulate the behaviour of States in the course of an international armed conflict. However, each of these regimes includes rules whose substance may be broad in scope, imprecise in language, open to subjective interpretation and application, or exist only as non-binding "soft law". Nevertheless, the broad aims and intentions of these regimes should be acknowledged, and good faith efforts should be made to adhere to them.

International Space Law

As the activity in question would occur in outer space, the special regime of international space law is one valid and applicable set of rules. The United Nations treaties on outer space developed in the 1960s and 1970s at the United Nations Committee on the Peaceful Uses of Outer Space include four core treaties governing the activities of States in the exploration and use of outer space. They are the 1967 Outer Space Treaty,[4] the 1968 Astronaut Rescue and Return Agreement,[5] the 1972 Liability Convention,[6] and the 1975 Registration Convention.[7] The Outer Space Treaty has a number of provisions broadly relevant to space debris creation and surrounding issues. The next few subsections discuss these provisions in thematic (rather than sequential) order.

Outer Space Treaty (OST) Article IX requires observance of a cooperation principle

The first sentence of Article IX of the Outer Space Treaty requires observance of a dual-natured principle of cooperation and mutual assistance, whereby States Parties to the treaty "shall be guided by the principle of cooperation and mutual assistance" in their exploration and use of outer

[4] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies (adopted 19 December 1966, entered into force 10 October 1967) 610 UNTS 205.
[5] Agreement on the Rescue of Astronauts and the Return of Objects Launched in Outer Space, (adopted 19 December 1967, entered into force 3 December 1968) 672 UNTS 119.
[6] Convention on International Liability for Damage Caused by Space Objects (adopted 29 November 1971, entered into force 1 September 1972) 961 UNTS 187.
[7] Convention on Registration of Objects Launched into Outer Space (adopted 12 November 1974, entered into force 16 September 1976)1023 UNTS 15.

space. This provision may not seem directly relevant, but it reflects the exploratory and uncertain nature of space exploration and use, and therefore the necessity for space-faring States to cooperate with each other. When linked with other provisions of space law, this principle of cooperation and mutual assistance creates a broad framework of respect for the rights, freedoms, and ambitions of others in space.[8]

OST Article IX requires observance of a due regard principle

The first sentence of Article IX of the Outer Space Treaty then enshrines a principle of due regard, whereby States must conduct their activities in outer space "with due regard to the corresponding interest of all other States Parties to the Treaty."[9] As with the principle of cooperation and mutual assistance, paying due regard to the corresponding interests of other States underlines the notion that the actions of one State in outer space may affect other States. While due regard as used here is undefined, this treaty clause also reflects the idea that activity in space does not fall into a hierarchy – where some activities outrank others activities – but rather, that all legitimate activities are given recognition, consideration, and regard.[10]

OST Article IX requires avoiding harmful contamination

In the context of its first sentence, the second sentence of Article IX then requires that States pursuing studies and conducting exploration of outer space do so in a manner "so as to avoid their harmful contamination" and, "where necessary, shall adopt appropriate measures for this purpose." It is a drawback that the treaty does not define what exactly "harmful contamination" is, but the inclusion of the word "harmful" before "contamination" points toward the notion that there is a difference between mere contamination, and contamination which is "harmful". Article IX is an early example of an international understanding of space as an environment requiring safeguards.

Since the dawn of the space age, debris creation has occurred in the normal course of operations, that of launching a space object, orbit raising, insertion into its final orbit, and during operational and post-operational

[8] PJ Blount, 'Peaceful Purposes for the Benefit of All Mankind – The Ethical Foundations of Space Security' in Cassandra Steer and Matthew Hersch (eds), *War and Peace on Outer Space* (OUP 2021).

[9] Outer Space Treaty, Article IX.

[10] Jinyuan Su, 'The Legal Challenges of Arms Control in Space' in Cassandra Steer and Matthew Hersch (eds), *War and Peace in Outer Space* (OUP 2021) 196, noting that "this obligation essentially deals with the degree of interference that one may reasonably cause to others and that others are expected to tolerate."

lifespan. Used upper stages of rockets separate from satellites during orbital insertion, and both large and small pieces of hardware fall back to Earth, as well as remain on orbit at the end of life. Traditionally, on-orbit explosions of fuel tanks was a potential and foreseeable occurrence. All these activities were seen as expected, necessary, and therefore allowable behaviour, and therefore not within the conception of "harmful" contamination of space.

Nevertheless, even small debris created in the normal course of operations are very harmful should they strike other spacecraft. Indeed, since the late 1980s, space debris concerns have risen in salience and urgency, and international efforts (while lagging) have attempted to keep pace with the proliferation of space debris. In harmony with the first sentence of Article IX, further obligations (discussed below) to avoid harmful contamination reflect the shared nature of the space domain, its fragility, the need for stewardship, and obligations owed to others users and to the space domain itself.

OST Article IV prohibits certain weapons

Turning to security matters, Article IV of the Outer Space Treaty reflects the reality that the Outer Space Treaty is fundamentally a security treaty, and was intended to defuse potential rivalries and conflicts in the space domain. Article IV significantly (but not completely) de-weaponises outer space. It places a negative obligation on States in the form of a prohibition on their activities.

> "States Parties to the Treaty undertake not to place in orbit around the Earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction, install such weapons on celestial bodies, or station such weapons in outer space in any other manner."[11]

The implications of this negative obligation is that: 1) conventional weapons are hereby *not* prohibited,[12] and 2) though otherwise prohibited from space, weapons of mass destruction are not prohibited from *transiting* through space. Both of these gaps (or *lacunae*) in Article IV were created intentionally by the negotiators of the treaty. Additionally, Article IV does not address space debris, or weapons or actions that create space debris.

[11] Outer Space Treaty, Article IV.
[12] Michel Bourbonnière and Ricky Lee, 'Legality of the Deployment of Conventional Weapons in Earth Orbit: Balancing Space Law and the Law of Armed Conflict' (2008) 18 EJIL 873.

OST Article VII creates international liability rules

A comprehensive discussion of space debris creation, and likely resulting effects, must include the international responsibility and liability provisions contained in Article VI and VII of the Outer Space Treaty. Article VI creates the attribution rule in international space law, whereby States are internationally responsible for their national space activities. As a corollary to such international responsibility, Article VII then creates a liability rule particular to physical damage caused by space objects.

States which fit the definition of a Launching State of a space object can be found internationally liable for those space objects when damage occurs. A Launching State is a State which launches or procures the launch of a space object, from whose territory or facility launches a space object.[13] Launching States are internationally liable for damage caused by their launched space objects to other States Parties to the treaty, or to their natural or juridical persons suffering damage. The 1972 Liability Convention subsequently elaborates the categories of liability, including absolute liability for damage suffered on the Earth or to aircraft in flight, and a fault-based liability regime for damage suffered in outer space between multiple States.

This liability regime was created to reflect the reality that space activities are risky, and that physical damage is foreseeable. Consequently, causing damage is not illegal *per se* or "against" the law (*contra legem*). Rather, the rule stipulates that when damage occurs, a liability duty (the legal requirement to pay compensation) arises. The drafters of the Outer Space Treaty and the Liability Convention created a system of responsibility & liability obligations for peacetime activities in space, where damage results in foreseeable, legal, and unintentional manners. This conception is different from the context discussed in the majority of this article, where damage to another State's space object is created in an intentional, volitional manner.

As a thought experiment, could a State destroy another State's satellites intentionally, and then avail itself of space law's responsibility & liability rules? Under these rules, compensation for the physical damage is the legal consequence, rather than the characterization of those acts as an aggressive act or use of force under IHL. The answer is no, as the space law liability regime was meant to address damage resulting from otherwise lawful activity (although the treaties do not make this point explicit). For damage created

[13] Liability Convention (n 5).

intentionally, as in the case of conflict between States, other applicable international rules, such as IHL, would seem to predominate in the characterization under the law. The intentions behind the creation of the space debris is the critical element in deciding whether to apply space law or IHL.

Other norms addressing space debris

Other sources of rules relevant to space debris form the normative background of this discussion, although they often take the form of non-binding "soft law" sources. These include the 2002 IADC Space Debris Guidelines, the 2007 COPUOS Space Debris Mitigation Guidelines, and the 2019 COPUOS Long-term Sustainability Guidelines.[14] These various sources of law apply generally to peaceful uses of outer space, but are important to raise here as they all reflect the widespread and commonly-accepted understanding that the space domain is fragile, commonly shared, susceptible to despoliation by human-created objects, and that a growing global consensus has taken and continues to take efforts to preserve the space domain.

OST Article III situates space law within international law

Helpfully, Article III of the Outer Space Treaty creates an intentional and explicit link between the special regime of space law and the rest of international law. The article stipulates that space activities shall be carried on "in accordance with international law, including the Charter of the United Nations, in the interest of maintaining peace and security and promoting international cooperation and understanding." The mention of the UN Charter, as well as peace, security, international cooperation and understanding, further reinforce the sensitive security context of space activities, as well as the notions of outer space as a shared domain with interacting rights and obligations between actors, the necessity of due regard for the interests of other actors in the space realm and a respect for the space environment itself.

Conclusion of space law discussion

While not explicit in the text of Article III, it is widely understood that the UN space treaties regulate State activity (and non-State actors whose actions

[14] Inter-Agency Space Debris Coordination Committee, 'Space Debris Mitigation Guidelines Revision 2' (2020); United Nations Office for Outer Space Affairs, Space Debris Mitigation Guidelines of the Committee on the Peaceful Uses of Outer Space (United Nations 2010); United Nations Office for Outer Space Affairs, Guidelines for the Long-Term Sustainability of Outer Space Activities of the Committee on the Peaceful Uses of Outer Space (United Nations 2021).

are attributed to States) during peacetime.[15] This notion is bolstered by the fact that these treaties were developed in the United Nations Committee on the *Peaceful* Uses of Outer Space (emphasis mine); their repeated encouragement of peaceful scientific investigations and international cooperation; and the repeated phraseology of space exploration for peaceful purposes.[16]

In the context of armed conflict between States, the rules from the Outer Space Treaty and its progeny would not seem to take a primary role. Rather, conflict in space is governed by rules governing conflict.[17] According to experts, scholars, and the Oslo Manual on Select Topics of the Law of Armed Conflict, the principles of the law of armed conflict are *lex specialis* during armed conflict, and should a normative incompatibility or conflict arise between the application of the rules of this regime and those of space law, the law of armed conflict would prevail over the more generalized law of outer space.[18]

International Environmental Law and Space Debris Creation

International environmental law also applies to outer space. Central tenets such as the Precautionary Principle, the Polluter Pays Principle, etc., apply to human activities in the space domain, as do ideas of sustainable development. Environmental tenets stress that outer space requires protection, careful stewardship, collaboration, and common management norms. Particular to military operations, the 1979 Environmental Modification treaty also norms the normative context of the present article, since it explicitly links environmental concerns with military activities and warfighting.[19]

---

[15] Cassandra Steer and Dale, 'International Humanitarian Law and Its Application in Outer Space' in Cassandra Steer and Matthew Hersch (eds), *War and Peace on Outer Space* (OUP 2021) .

[16] Blount (n 7).

[17] Steer and Stevens (n 14).

[18] Yoram Dinstein and AW Dahl, *Oslo Manual on Select Topics of the Law of Armed Conflict: Rules and Commentary* (2020) 5.

[19] Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques (ENMOD) (adopted 18 May 1977, entered into force 5 October 1978) 1108 UNTS 115. Article 1.1 "Each State Party to this Convention undertakes not to engage in military or any other hostile use of environmental modification techniques having widespread, long-lasting or severe effects as the means of destruction, damage or injury to any other State Party." This prohibition suggests a corresponding argument against debris-creating ASATs additional to this article's argument founded on an indiscriminate effects analysis.

A more thorough discussion of the application of environmental law's application to the space environment is beyond the scope of this article, but this regime's application to outer space further bolsters the notion that the space domain is a fragile one and subject to despoliation and pollution.[20]

Stakeholders have to work to maintain a usable space environment. In this sense, a usable space domain is a global public good that requires positive actions to establish and maintain.[21] Its maintenance requires collective efforts, but is also susceptible to "tragedy of the commons" and free rider problems, as well as unilateral acts which could spoil the shared environment. In space, one bad actor or incident can have consequences for all other users, and severely diminish the space environment as a usable environment.

International Humanitarian Law

Armed conflict in outer space is governed under the same principles of armed conflict elsewhere. Namely, military operations must observe the principles of military necessity and considerations of humanity, and the sub-principles, or operational principles, of distinction, proportionally, and precaution in attacks.[22] The rules of international humanitarian law (IHL) may be found in treaty law and in customary international law. These principles will be discussed first. Next is a discussion of the requirements for States to assess new weapons and weapons systems to determine whether they can be used in conformity with IHL.

Principles of weapons law generally applicable

A core customary principle of international humanitarian law is that States are not unrestricted in the ways of injuring or damaging the enemy,[23] and that international law can and does specify what those restrictions are. International law prohibits the use of weapons and methods of warfare that cause superfluous injury or unnecessary suffering. Additionally, and more

---

[20] *See generally* Jinyuan Su (n 9) 191-195, discussing the Rio Declaration, the Stockholm Declaration, analogies from the UN Convention on the Law of the Sea, and various principles extant in ICJ jurisprudence.

[21] *See generally* Edith Brown Weiss, 'Establishing Norms in a Kaleidoscopic World: General Course on Public International Law' (2018) 396 *Recueil des Cours de l'Académie de Droit International* 37.

[22] Steer and Stevens (n 14).

[23] Also reflected in Article 36 of the Protocol Additional to the Geneva Convention of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflict (adopted 8 June 1977, entered into force 7 December 1979) 1125 UNTS 3.

relevant to the focus of this article, is the prohibition of the use of weapons that are of an indiscriminate nature.

The prohibition on weapons of an indiscriminate nature is a component of the general IHL principle of distinction, requiring States involved in an international armed conflict to distinguish between combatants and civilians, and between military objectives and civilian objects. In the course of military operations during an international armed conflict, only the targeting of enemy combatants and military objectives is permissible.

AP1 prohibits indiscriminate weapons

Article 51(4) of Additional Protocol 1 (AP1) of the Geneva Conventions defines and prohibits indiscriminate attacks, as:

a) those which are not directed at a specific military objective;
b) those which employ a method or means of combat which cannot be directed at a specific military target; or
c) those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol;

and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction.[24]

Paragraphs b) and c) of the above article contains the indiscriminate weapons principle. This principle prohibits weapons that cannot be directed at a specific military objective, or *whose effects cannot be limited to military objectives*.

Weapons review

States are required by international law to analyse new weapons and to determine whether the use of that weapon would, in some or all circumstances, violate the applicable rules of international law. This obligation to assess weapons and weapons systems is considered an implied obligation necessary to fulfil Common Article 1 of the 1949 Geneva Conventions requiring States to respect and ensure respect for the Conventions. Consequently, the assessment of weapons is a due diligence obligation necessary to comply with the primary obligations included in the Geneva Conventions and other weapons treaties.[25]

Boothby discusses how the requirement to review applies to new weapons, including space weapons. He points out that the International

[24] Boothby (n 2) at 204.
[25] Ibid.

Committee of the Red Cross holds that "the requirement that the legality of all new weapons, means and methods of warfare be systematically assessed is arguably one that applies to *all* States, regardless of whether or not they are a party to Additional Protocol 1."[26] Additionally, for States that are party to AP1, they must determine whether the employment of new weapons, means, and methods of warfare, in some or all circumstances, would be prohibited by international law, including during the study, development, acquisition, or adoption phase of such new weapons, means, or methods.[27] In performing this analysis, both customary principles and rules of international law as well as treaty rules are to be applied to legal review.

Boothby stresses that there is no rule of international law regarding the format or method of weapons reviews, and he then synthesizes a set of questions for the review of new weapons, including space weapons:

- "Is the weapon system of a nature to cause superfluous injury or unnecessary suffering?
- Is the weapon system indiscriminate by nature?
- For States that are party to AP1, is the weapon intended, or may it be expected, to cause widespread, long-term and severe damage to the natural environment?
- For States that are not party to AP1, is the use of the weapon going to be consistent with the State's obligation to have due regard to the natural environment?
- For States that are party to Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques (ENMOD), would the use of the weapon involve environmental modification techniques of the sort and involving the consequences prohibited by the ENMOD Convention?
- Are there *ad hoc* weapons law rules that apply to the weapon?"[28]

Conclusion of IHL Discussion

The previous sections should have highlighted that fundamental principles of IHL apply to weapons, including their effects and how they are

[26] Ibid. Also note that the USA is not a party to AP1.
[27] Ibid.
[28] Ibid 206. *See also* Gilles Giacca, 'Legal Reviews and New Weapons: Process and Procedures' in Baldwin de Vits (ed), *Weapons and the International Rule of Law* (International Institute of Humanitarian Law 2017); International Committee of the Red Cross, A Guide for the Legal Review of New Weapons, Means, and Methods of Warfare Measures to Implement Article 35 of Additional Protocol I of 1977 (2005) < https://www.icrc.org/en/doc/assets/files/other/icrc_002_0902.pdf > accessed 4 October 2021.

used. While space technology is new, the principles of IHL that apply to conflict elsewhere continue to apply to space. These rules include the necessity of weapons reviews, as well as the prohibition on weapons whose effects fail to discriminate between lawful targets such as enemy combatants and unlawful targets such as civilians, or fail to discriminate between lawful objects such as military objectives and unlawful targets such as civilian objects.

Anti-satellite Weapons (ASATs)

Weapons to attack spacecraft on orbit take a variety of forms. These include kinetic weapons, non-kinetic physical weapons, and electronic & cyber weapons.[29] Kinetic ASAT weapons are the primary focus of this article. Examples of kinetic anti-satellite weapons include direct ascent anti-satellite (ASAT) weapons and co-orbital anti-satellite weapons, both of which destroy their target through the force generated by a high speed impact.[30]

Direct ascent ASATS are not placed in orbit themselves, but are ground, air-, or sea-launched missiles with interceptors that are used to kinetically destroy satellites through force of impact."[31] In turn, co-orbital ASATs are already in orbit, and manoeuvre to the target satellite to attack it by various means, including those destructive and non-destructive.[32] Both direct ascent ASATs and co-orbital ASATS involve the weapon physically striking the target satellite at high speed, and therefore have the potential to create large and long-lived debris fields as a result.[33]

Non-kinetic ASATs include lasers or high-powered microwave technology to disable or destroy satellites. These weapons may cause physical damage to satellites, but would not make physical contact with the target satellite. Some directed energy ASATs, such as a high-energy laser, might cause sensitive parts of a satellite to explode (e.g. via overheating a fuel tank),

---

[29] Brian Weeden and Victoria Samson, 'Global Counter space Capabilities: An Open Source Assessment' (2021) Secure World Foundation, xxxi < www.swfound.org/counterspace > Accessed 1 October 2021; Todd Harrison and others, 'Space Threat Assessment 2021' (2021) Centre for Strategic & International Studies < www.csis.org/analysis/space-threat-assessment-2021 > accessed 1 October 2021.

[30] Kinetic does not mean destructive, it means destruction by ramming at high speed (in contrast to traditional bombs which destroy their target by exploding and generating heat and concussion).

[31] Weeden and Samson XXXI (n 28).

[32] Ibid.

[33] It is beyond the scope of this article, but are there differences in the debris clouds created by a kinetic direct-ascent ASAT versus a kinetic co-orbital ASAT, either because of speed of impact, or attack vector?

thereby also creating orbital debris, although often less than the amount created by a kinetic attack.

Similar to non-kinetic ASATs, electronic and cyber means and methods to disable or destroy satellites exist but do not involve physically striking the target satellite. Both non-kinetic ASATs and those of the electronic and cyber variety still could temporarily or permanently disable the target satellite, thereby turning it into a non-functioning space object, and therefore debris (albeit a single large piece).

Brief history of direct ascent ASAT tests and demonstrations.

A detailed history of kinetic direct-ascent ASATs is beyond the limits of this article, but this section details historical direct ascent ASATs tests which created debris in an effort to illustrate the debris fields such weapons create. A brief history of the development of direct ascent ASATs begins with early efforts by American and Russian militaries to develop and test these weapons in the context of the Cold War, and in contemplation of both anti-ballistic missile and anti-satellite capabilities.

The USA sought ASAT capabilities starting in the late 1950s and pursued them until the late 1980s.[34] In May 1963, a modified *Zeus B* missile successfully intercepted an *Agena D* rocket stage in orbit, a key early success.[35] The first American destructive intercept of a satellite occurred on September 13, 1985, with the striking of the *Solwind P78-1* satellite at 555 km altitude with an air-launched missile from a modified F-15A fighter. The missile utilised an infrared homing seeking guidance system, three rocket stages involving two types of solid rocket propellant, and an interceptor with 63 small rocket motors for fine trajectory and attitude control.[36] The system developed for this test was halted in 1988. This test created 285 pieces of trackable orbital debris.[37] This debris cloud was very long lived, but eventually completely deorbited.[38] The final piece of tracked debris from this test re-entered the Earth's atmosphere on May

[34] Kaila Pfrang and Brian Weeden, 'U.S. Direct Ascent Anti-Satellite Testing' (2021) Secure World Foundation Factsheet, 2–3 < https://swfound.org/media/207180/swf_us_da-asat_fact_sheet_apr2021.pdf >. Accessed 1 October 2021.
[35] Weeden and Samson (n 28).
[36] Ibid 2.
[37] Ibid 3.
[38] Marissa Martin and Brian Weeden, 'History of Anti-Satellite Tests in Space' (Secure World Foundation, 2021) <https://docs.google.com/spreadsheets/d/1e5GtZEzdo6xk41i2_ei3c8jRZDjvP4Xwz3BVsUHwi48/edit?usp=sharing > accessed 1 October 2021.

9, 2004. Consequently, the lifespan of debris from this test of a kinetic direct ascent ASAT at this altitude was 18.7 years.

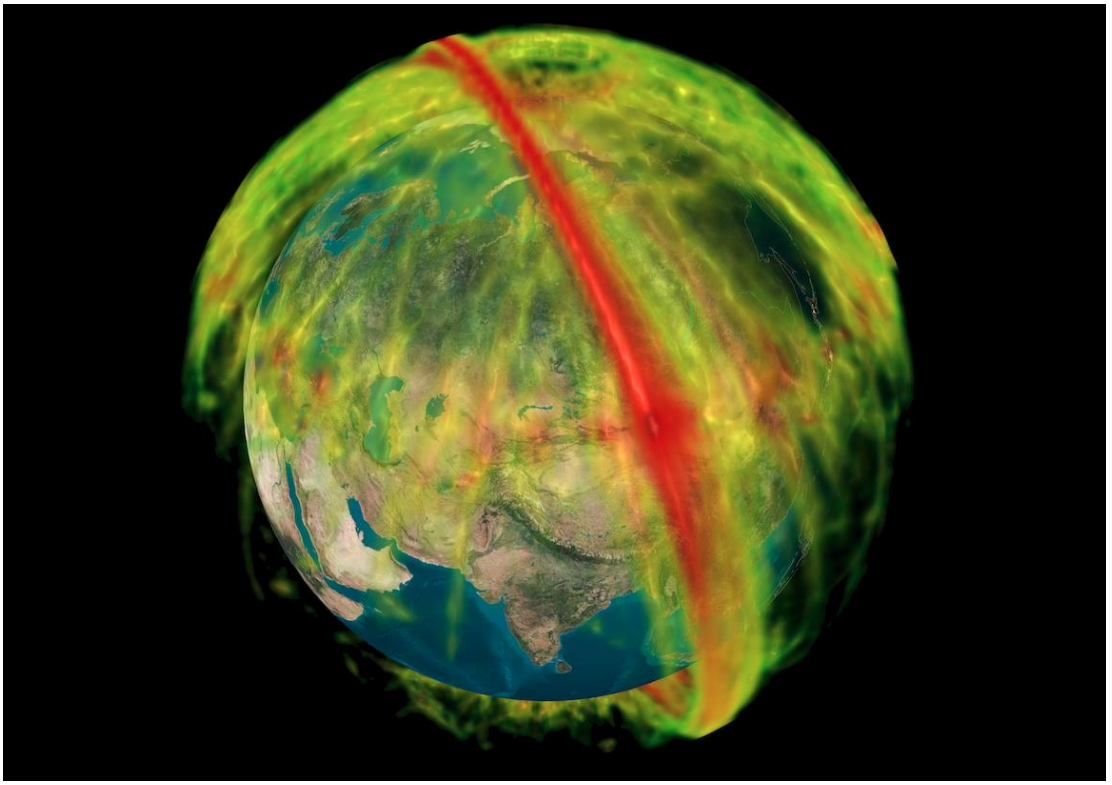
The next (and latest) known American test of an ASAT was on Feb 20, 2008, with the striking of the *USA 193* satellite with an SM-3 Block 1A interceptor missile launched from the USS Lake Erie as part of Operation *Burnt Frost*. The intercept and destruction of *USA 193* was at an altitude 240 km.[39] Three SM-3 missiles had a "one-time software modification" to enable them to intercept the satellites, and this method likely represents a potentially large and flexible DA-ASAT capability that could be used in a future conflict."[40] Some sources report that the targeting vector of this ASAT strike was from above, and was intended to strike the satellite downward and towards the Earth, with the assumption that this would also project the debris field downwards, and minimise the debris field's impact to other space assets.[41] Additionally, the satellite was headed towards re-entry but was still in a predictable orbit, and the time of its lowest orbital altitude (perigee) before it started to tumble into re-entry was also apparently chosen as the best time to strike it.[42] Despite these steps, the test created 174 pieces of trackable orbital debris.[43] Due to the lower altitude of this test, the debris cloud generated was not as long-lived as that from the 1985 test, but the final piece of orbital debris from this test re-entered the Earth's atmosphere on October 28, 2009.[44] Consequently, the lifespan of debris from this test was 1.7 years.[45]

Today the United States does not have an acknowledged kinetic-kill ASAT weapon system. The only acknowledged offensive counter space system is the Counter-Communications System (CCS) that uses electronic warfare technologies. While the United States likely retains significant technical expertise to develop a kinetic-kill ASAT system should it choose, current US military leadership is quite emphatic that debris-creating ASATs are irresponsible and untenable, however.[46]

---

[39] SWF U.S. Direct-Ascent ASAT Factsheet (n 33) at 2-3.
[40] Ibid 2.
[41] Michel Bourbonnière, "Law, Technology and the Conduct of Hostilities in Space" in Wolf Heintschel von Heinegg and Gian Luca Beruti (eds), *International Humanitarian Law and New Weapons Technologies* (IIHL 2012) 163.
[42] Ibid.
[43] SWF U.S. Direct-Ascent ASAT Factsheet (n 33).
[44] SWF History of Anti-Satellite Tests in Space (n 37).
[45] Ibid.
[46] Jeff Foust, 'Space Force to Consider Space Sustainability in Any Future Conflict' Space News (17 September 2021).

There is a complex history of Russia's development of direct ascent ASAT capabilities, but no known example of a successful intercept and destruction of targets on orbit.[47] Russia does appear to be developing a new DA-ASAT capability through a program called *Nudol*, but while it has been tested more than ten times, none of those have been against a space object. However, their co-orbital ASAT development, described in the next section, has been tested dozens of times between 1963 and 1982, and led to the creation of hundreds of pieces of orbital debris.



The anti-satellite missile test conducted by China on 11 January 2007 produced the largest recorded creation of space debris, with at least 3,513 trackable pieces (golf ball sized or larger) and an estimated 150,000 debris particles. This image shows the average distribution of trackable objects orbiting the Earth three months after this incident. Source: COMSPOC Corporation

China has a history of at least 10 known or suspected direct ascent ASATs tests, with one destroying a satellite.[48] That completed test was on January 11,

[47] Renata Knittel Kommel, Marissa Martin and Brian Weeden, 'Russian Direct Ascent Anti-Satellite Testing' (2021) Secure World Foundation Factsheet < https://swfound.org/media/207181/swf_russian_da-asat_fact_sheet_apr2021.pdf > Accessed 1 October 2021.

[48] Brian Weeden, 'Chinese Direct Ascent Anti-Satellite Testing' (2021) Secure World Foundation Factsheet < www.swfound.org/media/207183/swf_chinese_da-asat_fact_sheet_apr2021.pdf > accessed 1 October 2021.

2007, with the striking of a *FengYun 1C* weather satellite at an altitude of 865 km with an SC-19 missile launched from the Xichang launch centre. This event created thousands of pieces of orbital debris, of which (as of September 2021) 3,531 have been catalogued.[49]

This debris field is extremely long-lived due to the altitude of the interception. 667 catalogued pieces of this debris field have re-entered since 2007.[50] Therefore, 2,864 catalogued pieces of debris remain on-orbit.[51] Consequently, the lifespan of debris from this test is 14.7 years and counting. Additionally, the 3,531+ pieces of orbital debris created by the test in 2007 increased the number of tracked space objects by 31.5%, and the number of tracked space debris by 34.3%.[52] Since this 2007 test, China has continued to test direct ascent ASAT capabilities, but has not struck any target satellites (the targets have all been ballistic objects as they have been ostensibly part of their missile defence test program).[53]

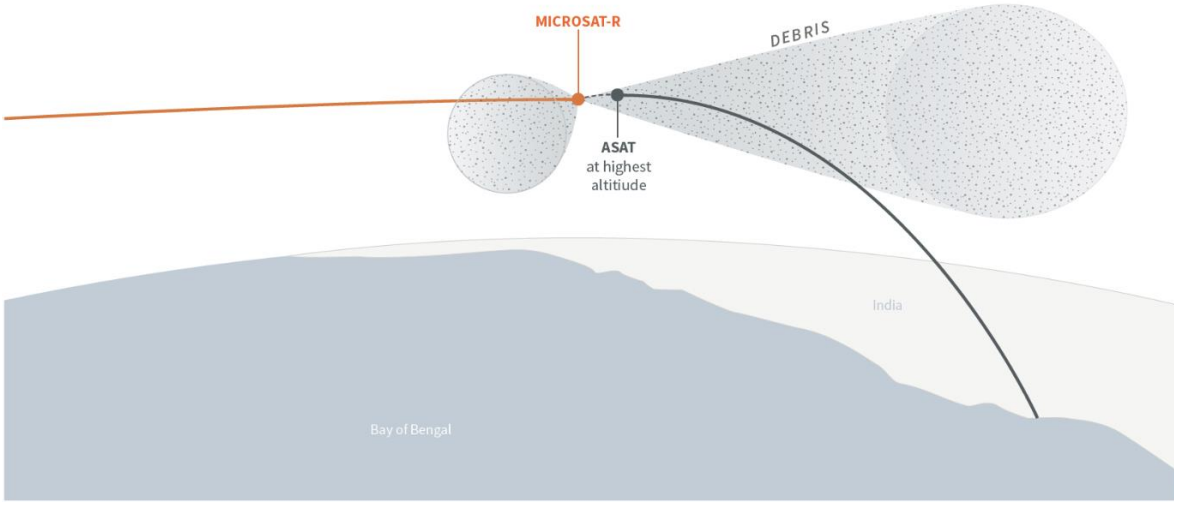
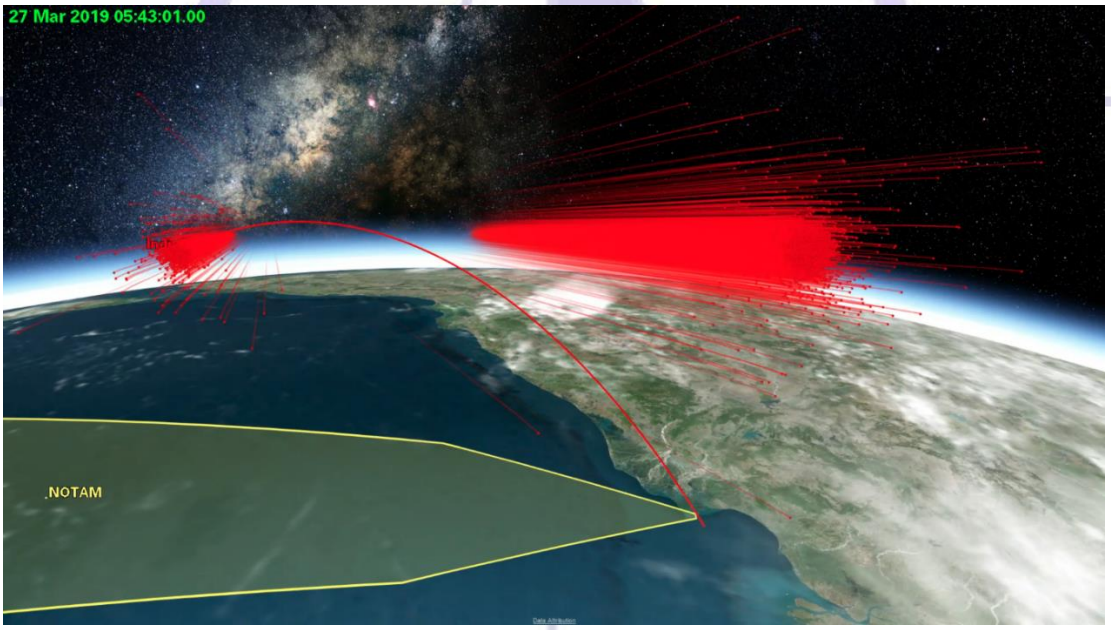


Diagram of the 2018 Indian Direct Ascent ASAT demonstration. Note the slight downward trajectory of the interceptor, and two resulting debris fields. Source: CSIS Aerospace Security Project / Emily Tiemeyer.

[49] Email from Jonathan McDowell to author, discussing McDowell's analysis of the Space-Track catalogue and archival TLE data (15 September 2021).
[50] Ibid.
[51] Ibid.
[52] Ibid. Before this test, there were 11,181 trackable objects, of which 874 (+/- 10%) were operational satellites, and 10,307 (+/-10%) were space debris. Adding 3,531 new pieces of trackable debris increases this total by ≈31.5% (total tracked objects), or ≈34.3% (total tracked debris).
[53] SWF Chinese Direct Ascent Anti-Satellite Factsheet (n 47) at 3.

India is the latest country to successfully demonstrate a direct ascent ASAT weapon. On March 27, 2019, a *Microsat-R* satellite was destroyed with a PDV-MK II interceptor.[54]

The intercept was at 300 km altitude.[55] This test created 129 pieces of trackable orbital debris.[56] Early analysis of the debris by AGI revealed 57 initial trackable objects, 46 of which had apogees above the orbit of the ISS, 13 having perigees above 1,000km, and the highest piece of debris with an apogee of 2,248 km.[57] Eventually, 128 catalogued pieces of this debris field have re-entered since 2019. As of writing (September 2021), there remains 1 catalogued piece of debris still on-orbit. Consequently, the lifespan of debris from this test is 2.5 years and counting.



AGI's simulation of the Indian ASAT demonstration moments after impact. The red upward line is the trajectory of the interceptor, while the red fields are resulting debris fields.
Source: COMSPOC Corporation, https://youtu.be/KYRHmEF1Azo

[54] Ankit Panda, 'Indian Prime Minister Announces Successful Anti-Satellite Weapon Test in National Address' *The Diplomat* (27 March 2019) <https://thediplomat.com/2019/03/indian-prime-minister-announces-successful-anti-satellite-weapon-test-in-national-address/ >; Marissa Martin, Kaila Pfrang and Brian Weeden, 'Indian Direct Ascent Anti-Satellite Testing' (2021) Secure World Foundation Factsheet < www.swfound.org/media/207182/swf_indian_da-asat_fact_sheet_apr2021.pdf> accessed 1 October 2021.

[55] Ibid.

[56] Ibid.

[57] Daniel Oltrogge, TS Kelso, and Timothy Carrico, 'Characterizing the India ASAT Debris Evolution Using Diverse, Complementary Tools' (2020) 171 Advances in the Astronautical Sciences 4283, 4285 < http://celestrak.com/publications/AAS/19-889/AAS-19-889-pp.pdf > accessed 3 October 2021.

Co-orbital ASAT developments

In addition to direct ascent ASATs, co-orbital ASAT weapons also risk the creation of long-lasting and large debris clouds. Co-orbital ASAT weapons operate by first placing the satellite interceptor into orbit, and this interceptor then manoeuvres to alter its orbit into a trajectory to bring it close to the target. Co-orbital ASATs are designed to be able intercept targets quickly after being placed into orbit, or to linger for an extended period of time before their final attack upon a targeted satellite.

Like direct ascent ASATS, co-orbital ASATs physically damage or destroy their target. However, while direct ascent ASATs kinetically strike, co-orbit ASATs can kinetically strike but might also release fragments which strike the target, use a robotic arm to destroy or damage the target, or use directed energy or other electronic means to damage or destroy their target. Thus, not all co-orbital ASATs methods threaten to create space debris.

Both the United States and Russia have developed and tested technologies for close approaches of target satellites in Low Earth Orbit (LEO) and at Geosynchronous orbit (GEO). It should be stressed that there are peaceful applications of ranging and proximity operations technologies, such as satellite servicing (repair, refuelling, orbit-raising) and end-of-life debris remediation.

A notable co-orbital ASATs program is Russian, with development of co-orbital attack systems beginning in the early 1960s.[58] The *Istrebital Sputnikov* ("satellite fighter", or IS) system is one that launches to orbit, manoeuvres to approach close to the target satellite, and explodes, releasing shrapnel with an effective range of 50m.[59] The IS system was tested in space multiple times from its first test in 1968 until its last test in 1982, against test targets between 230 and 1,600km in altitude, and resulted in the creation of nearly 900 pieces of orbital debris larger than 10cm.[60] As an example, one test of the system in 1968 created 252 pieces of orbital debris, 79 pieces of which are still on orbit today

[58] Marissa Martin, Kaila Pfrang and Brian Weeden, 'Russian Co-Orbital Anti-Satellite Testing' (2021) Secure World Foundation Factsheet < www.swfound.org/media/207185/swf_russian_co-orbital_asat_fact_sheet_apr2021.pdf> accessed 1 October 2021.
[59] Ibid.
[60] Ibid.

– over 52 years later.[61] Seven subsequent tests of the system from 1970 until 1982 have similarly long-lived debris clouds still in Earth orbit.[62]

A similar Russia system, the *Naryad-V*, was tested in the early 1990s and has also created long-lived debris. One such test of the *Naryad-V* in 1994 resulted in 27 pieces of trackable debris, only 3 pieces of which have re-entered, while 24 pieces of debris from this co-orbital test in the 1990s remain in space. (McDowell notes that this 1994 test is not clear, and questions whether this was a test of an interceptor or whether a *Briz-M* rocket stage unexpectedly exploded in orbit.)[63]

Finally, Russia is currently developing robotic co-orbital ranging and proximity operations under the *Burevestnik* program. Although this program has not created significant debris fields in space compared to the previous programs, at least one test in 2019 resulted in debris reaching apogees as high as 1,400km, and resulting in 27 trackable pieces of debris.[64] This had led to suspicion that Burevestnik could be a new co-orbital ASAT program.

In 1986, the US military tested the Delta 180 Payload Adapter System as a missile defence experiment (not part of a specific co-orbital ASAT testing program).[65] Two space objects, the interceptor (the Payload Assist System, or PAS) and its target, were launched on the same rocket on September 5, 1986 from Cape Canaveral Air Force Station.[66] The target and interceptor were then placed into a circular orbit at 220km altitude, and the PAS interceptor was moved to a separation distance of 200km from the target. At a set time, both the target and interceptor ignited their rockets on a collision course with each other, and collided at a combined speed of nearly 3km per second.[67] The collision was at 220 km altitude, but the impact sent debris much higher. Some 16 pieces of debris went into orbits whose apogees were as high as 2,300km.[68]

---

[61] SWF History of Anti-Satellite Tests in Space (n 37).
[62] Ibid.
[63] Email from Jonathan McDowell to author (15 September 2021).
[64] Martin, Pfrang and Weeden (n 53).
[65] Marissa Martin, Kaila Pfrang and Brian Weeden, 'U.S. Co-Orbital Anti-Satellite Testing' (2021) Secure World Foundation Factsheet < www.swfound.org/media/207184/swf_us_co-orbital_fact_sheet_asat_apr2021.pdf> accessed 1 October 2021.
[66] Ibid.
[67] Ibid.
[68] Ibid.

Two months after the test, there were still 3 debris objects on orbit; the final piece of debris re-entered on April 14, 1987 after 220 days on orbit as debris.[69]

Current Space Debris from Historical ASAT Tests

Most space debris is created through normal space launch and operations, historically conducted with little regard for the growing space debris problem. Nevertheless, the amount of debris created as a result of developing and testing ASATs weapons is sobering.

Combining debris from both direct ascent ASATs and co-orbital ASAT activity results, Weeden and Pfrang in March 2021 found these weapons tests and demonstrations created 5,036 pieces of trackable debris.[70] Of those 5,036 pieces of debris, 3,260 pieces remain in orbit. Consequently, 64.7% of all debris created from ASATs tests, even those tests going back to the 1960s, is still in outer space.[71] McDowell gives slightly different numbers, with 5,081 pieces of space debris resulting from ASAT tests, of which 3,159 (62.2%) remain on orbit as of September, 2021. These numbers are approximations, as the true number of debris is likely much higher because only debris larger than around 10cm in diameter is trackable.

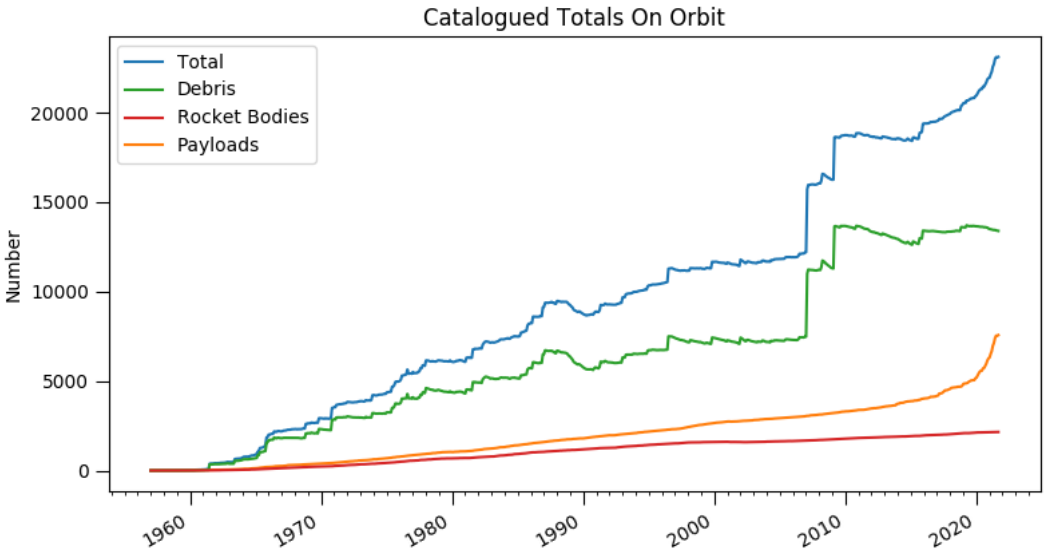
Pollution of the space domain

Anthropogenic space debris is an issue with worrying implications for the future sustainability of outer space. The population of objects is continually growing, but as of September 2021, McDowell states there are 23,102 catalogued objects in orbit, only 4,566 of which are functioning spacecraft.[72] The rest is debris. In other words, only 19.7% of catalogued space objects are operational spacecraft, while 80.2% of catalogued space objects are space debris.

Additionally, while objects smaller than 10cm cannot be accurately tracked, current estimates expect there to be approximately 36,500 objects greater than 10 cm, around 1,000,000 objects between 1 cm to 10 cm, and approximately 330 million objects sized between 1 mm to 1 cm in Earth orbit.[73]

---

[69] Ibid, and email from Jonathan McDowell to author (15 September 2021).
[70] SWF History of Anti-Satellite Tests in Space (n 37).
[71] Ibid.
[72] Email from Jonathan McDowell to author (15 September 2021).
[73] European Space Agency, Space Debris by the Numbers' (European Space Agency, 2021) https://www.esa.int/Safety_Security/Space_Debris/Space_debris_by_the_numbers > accessed 28 September 2021.



Historical growth of trackable objects on orbit. The 2007 and 2009 spikes are the Chinese ASAT test and the Iridium 33-Kosmos 2251 collision, respectively. The recent, rapid rise of the orange curve represents "newspace" objects. Source: Aaron Boley & Michael Byers[74]

The historical growth of the space debris population is also important to take into account. Space debris issues became more urgent in the 1990s. And while non-binding norms limiting space debris creation were created in the early 2000s, the growth of space debris has continued unabated. This recent and sharp growth in space debris is important to note for its own sake, and it also goes toward an understanding that notions about the acceptability of creating space debris have changed over time – with only a very recent emergence that space debris creation is not a sustainable practice, and should not be done.

Space is increasingly seen as congested, especially in lower orbits. The number of conjunction warnings generated by the US military have increased dramatically since conjunction issues first arose, and this level and complexity of space domain awareness, space traffic management, and conjunction warnings from both operational and non-functioning space debris show that space debris is a serious issue and that space debris cannot be wantonly created. Indeed, a number of notorious incidents have occurred where

[74] Aaron Boley and Michael Byers, 'Satellite Mega-constellations Create Risks in Low Earth Orbit, the Atmosphere and on Earth' (2021) 11 Sci Rep 10642 < https://doi.org/10.1038/s41598-021-89909-7> accessed 2 Oct 2021. The author would like to thank Dr Aaron Boley, UBC Physics and Astronomy, for the permission to use this image.

potential conjunctions have caused concern, as well as actual satellite-on-satellite collisions.

Critical Elements of Debris-Creating ASAT Tests

The current space debris problem, the magnitude of conjunction messages and warnings that are issued on a daily basis, and the growing awareness and anxiety of space debris provide greater context in discussing the intentional creation of space debris with ASATs.

The ASAT tests and demonstrations detailed above have at least two critical elements that inform a discussion about their legality. One is the time element of the debris being created, while the other is the size of the debris cloud created. Annexed to these elements, and related to both time and size, is their dynamic, evolving nature. Therefore this introduces a critical element of uncertain risk: even a small piece of debris, smaller than can even be tracked, can be damaging and even fatal to the functioning of the spacecraft that it collides with. And yet, these long-lived, vast, and dynamic debris fields confound our efforts to truly know where many individual pieces of debris actually are beyond a mere degree of likelihood.

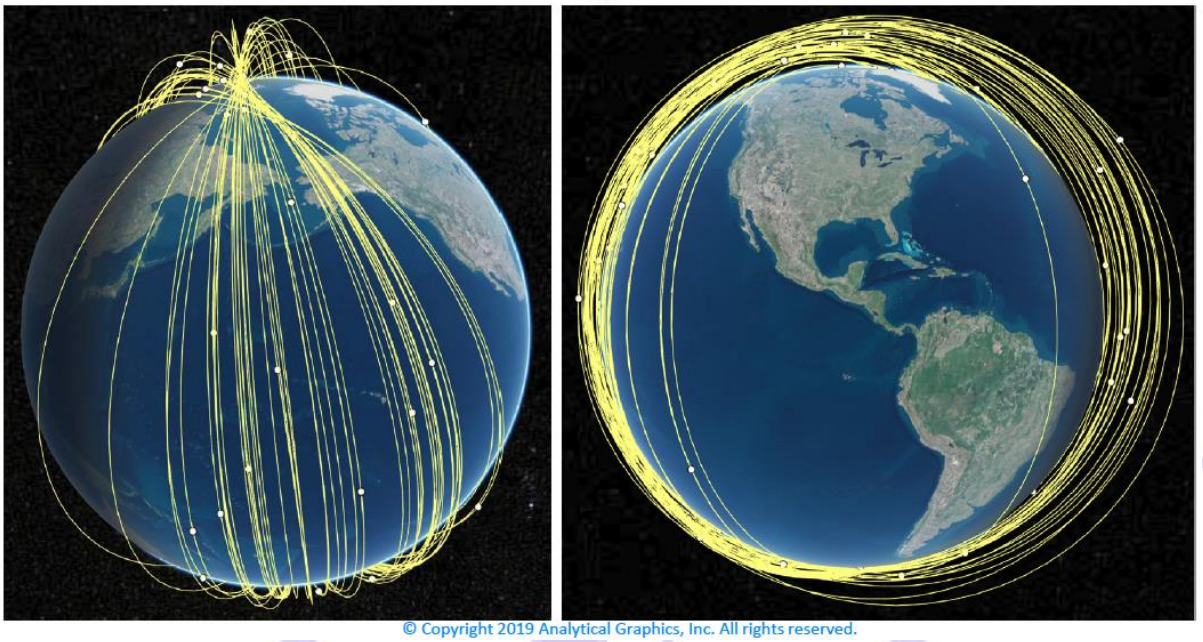
Debris clouds can be long-lived

While terrestrial explosions on the Earth surface or in the atmosphere create debris which settles to the ground within seconds or minutes, a debris-generating event in outer space lasts much longer. As we have seen, debris fields created decades ago persist as long-lived reflections of the collision that created them, as clouds of metal and other materials travelling around the Earth at orbital speeds. These debris fields are not static in space, as each individual piece of orbital debris has its orbit altered over time due to natural perturbations. If the incident was at a low enough altitude, some objects from a debris-creating incident re-enter within days, while other objects can remain in space for months or years. Generally, the higher the altitude of the intercept, the longer the resulting debris will remain in orbit, but as we have seen even some low altitude ASAT tests can throw debris more than a thousand kilometres higher. The long-lived nature of debris-created by weapons is highly important to the discussion of their legality.

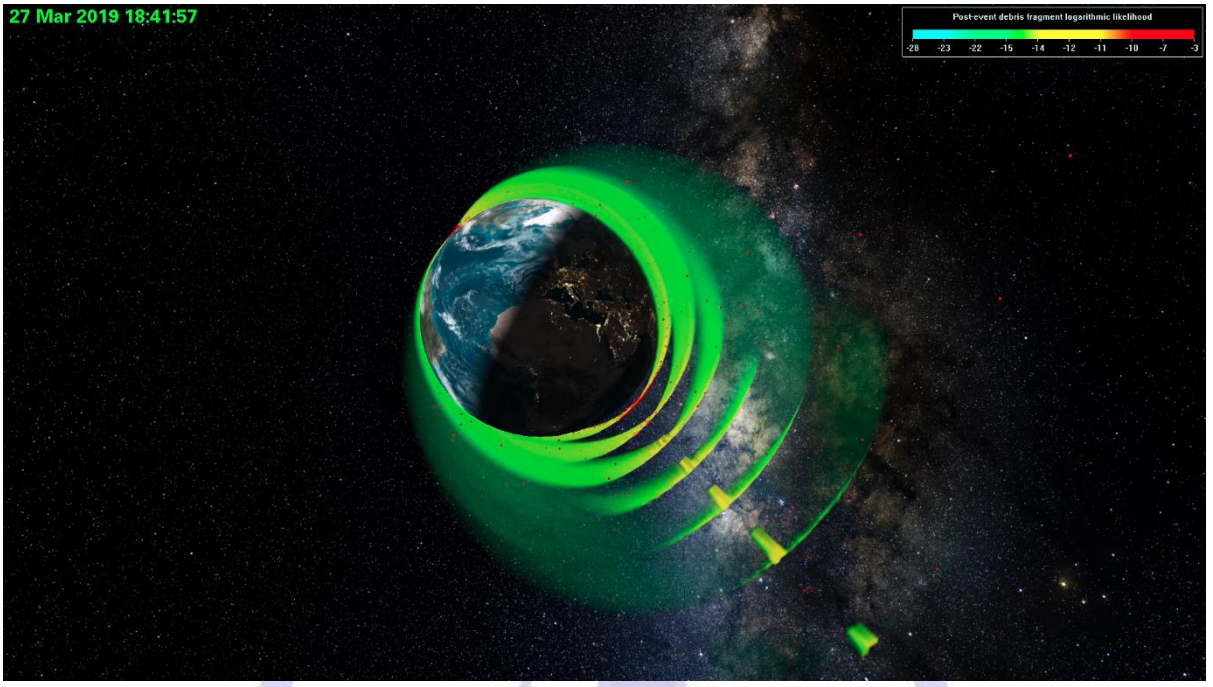
Debris clouds are both large in size, dynamic, and difficult to predict

The other critical element of the historical ASAT tests outlined above is their size and scope. A model of the 2007 Chinese ASAT test, as it sweeps around

the Earth, shows that this debris field is vast in size as it stretches out and cascades. Likewise, the 2019 Indian ASAT involved two initial debris fields that continued to spread out in orbit over time, impacting a much bigger area than the original collision, before eventually being pulled back to Earth by gravity and atmospheric drag. Also, because of the Earth's oblateness, when the debris cloud passes over the Equator and its stronger gravitational pull, the debris cloud will spread laterally into a shell. However, because of the wide variety of variables, predicting how a debris field will change and evolve over time is a matter of probability rather than certainty.



Orbit-normal and in-plane views of 53 pieces of Mission Shakti debris on 14 August 2019. Image on left shows the spreading of orbital planes of debris, image on right shows the distribution of orbital heights of debris. Source: COMSPOC Corporation



AGI's modelling of the Indian ASAT demonstration's fragments propagating in bands of debris over time. Source: COMSPOC Corporation, https://youtu.be/KYRHmEF1Azo

Debris clouds threaten a variety of other users of the space domain

Importantly, there are thousands of other satellites – both governmental and non-governmental – in LEO, the region most likely to see kinetic ASAT tests and their use during armed conflict. Governmental satellites in LEO include both civil and military spacecraft. These facts show how LEO is populated by a variety of actors and assets.

AGI's modelling of the debris cloud for the Indian ASAT showed that the debris field created in that incident threatened a multiplicity of private commercial satellites owned by companies including Planet, Spire, QB50, etc.,[75]

Additionally, there are humans in LEO aboard the International Space Station (ISS), a continuous human presence in space since November, 2000. The ISS orbits at an average altitude of 400 km. The ISS can support a standard crew of 7 individuals, although during crew changeover as many as 13 people are aboard. As of September 2021, 244 astronauts from 19 ISS partner countries have spent time at the ISS. LEO is also populated with crewed Chinese and

[75] Oltrogge, Kelso, and Carrico (n 53). Additionally, the ISS was also ranked further down on AGI's list (at #58) of potentially threatened spacecraft, but the authors noted that it would be higher up the list if their modelling tools took into account the size of the ISS, rather than just its orbit.

crewed commercial space stations likely to be operating in space in the near future.

Because of the uncertain nature of all of the influences on our understanding of the debris cloud, including everything from uncertainty in the modelling & tracking, to atmospheric drag and gravity, to space weather, it is essentially impossible to know for certain where fragments from an on orbit explosion will be in the future, and only probabilities can be given for where debris is and is going to be. Consequently, debris clouds are not just vast in size, they are difficult to model and predict. And yet, it is not a cloud of debris that is the sole danger – as just a single piece of debris is dangerous, and can damage and even destroy other operational spacecraft. In such a scenario, it was not the cloud of debris that was most worrying, it was the single piece that was the real danger. As such, even one piece of unnecessary space debris is too many.

The Legality of Debris-Creating Anti-satellite Attacks

Having shown that kinetically attacking and/or destroying satellites results in large explosions of debris which are challenging to predict, large in size, changing in size and shape, are long-lived, and which threaten multiple uninvolved actors in the space domain, a consideration of their legality under IHL can be well informed with the most updated information and picture of the space domain and the actors there. This consideration should include the requirements of IHL that attacks be proportionate, and observe the prohibition against indiscriminate attacks.

Some after-impact modelling of debris field evolution is possible

Debris fields inevitably change altitude from the altitude of the initial impact, even when the impact vector is at the same altitude or from above. Perturbations in the upper atmosphere, space weather, and gravity all push, pull, and stretch the resulting explosion. These physical forces cannot be known and accounted for beforehand, nor can they be mitigated or changed.

Writing in 2011, Bourbonnière asserted that, because the US ASAT test was on a downward (Earth-ward) attack vector, and the target at perigee of its orbit, the "US interception actually proved that you can use an ASAT weapon in a way that does not cause harmful space debris"[76]

[76] Bourbonnière (n 38) at 163.

Even if this were true, reducing the time the debris field remains in space to threaten other space objects speaks only to the time element of resulting debris fields. This alleged precaution does not go towards the requirement of discrimination. We still would not know where the debris field will be heading, nor whom that debris field would be threatening. Accurately modelling the explosion and the resulting debris field before impact are currently impossible, and will probably remain so. It is true that one can predict, using advanced computers, the evolution of debris fields and their shape after impact – but this still includes uncertainties, especially as details of the fragmentation affect the debris cloud in unpredictable ways. Additionally, one cannot predict the detailed position of these individual debris objects and whether they will collide with other spacecraft. Consequently, debris fragments remain unpredictable, and each piece of debris can only be predicted with a degree of uncertainty.

Dan Oltrogge, the Director of Integrated Operations and Research at COMSPOC, when asked whether "before a kinetic impact or other debris-creating event, there is any way to predict or foresee the size, shape, dimensions, or even any particular orbits or trajectories of debris" gave the following answer:

> "Computationally intensive hypervelocity impact fragmentation and propagation models are required to get a high-fidelity understanding of post-fragmentation debris cloud evolution, but unfortunately, the many inputs and initial conditions required by models are typically unavailable. Thankfully, there are more empirical, statistics-based models that, when properly constrained to adhere to physics conservation laws, are quite effective at generating highly representative distributions of fragment size, mass, and velocity magnitude and direction. Coupling those with a cloud evolution model works quite well, as has been demonstrated in post-event forensics for both the Chinese and Indian ASAT tests."[77]

This quote shows that some forecasting as to how a debris field will evolve is possible when given sufficiently accurate inputs. Such might be the case when the actor performing the kinetic intercept is also the owner/operator of the target, can precisely steer their own spacecraft into the desired impact, and possesses the engineering schematics of the target and use them for their

[77] Email from Dan Oltrogge to author (2 October 2021).

propagation model. These facts change if the target was an opposing actor; and therefore, their propagation models would likely be less accurate.

Moreover, even using statistics-based models to generate representative distributions of fragments, and coupling them with cloud evolution models, this method gives an accurate representation of what the debris field is predicted to be – rather than actual statements of where pieces of debris actually are.

Nevertheless, while advanced computers provide some probability-based predictions, these predictive models clearly highlight the other worrisome characteristics of debris fields – that they spread out, change in size and shape, persist over time, and, when combined with knowledge of other spacecraft orbits, clearly show that other spacecraft will likely be threatened.

Indiscriminate effects of debris creation in space

Turning once again to Article 51(4) of AP1, it is sub-paragraphs b) and c) which give the test for indiscriminate weapons. These are weapons which "b) employ a method or means of combat which cannot be directed at a specific military objective" or "c) employ a method or means of combat the effects of which cannot be limited as required by the Protocol, and which, consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction."

Boothby restates this as it pertains to space weapons, saying that a space weapon is unlawful "if, when used in its normal or designed circumstances, it cannot be directed at a specific military objective, and, if as a result, its nature is to strike lawful targets, such as military objectives, and protected persons and objects without distinction."[78]

To give an example, supposing a targeted satellite were a permissible military objective, and was attacked using existing kinetic ASAT technology – even in a manner so as to minimize space debris creation through downward attack vectors and striking the target at its perigee closest to the Earth's atmosphere so as to direct debris downward – the certain result is that immediately after impact, two distinct debris fields result.

Some of the debris from the impact (mostly target debris) will be headed in the same direction it was before impact. Some of the debris (largely comprising interceptor debris) will be headed in the same direction the

[78] Boothby (n 2) at 187.

impactor was before intercept. As the interceptor was not orbital, likely this debris will also not be orbital. However, each fragment from the impact, both from the interceptor and from the target will have some change in velocity applied to it as a result of the collision. Much will depend on the specific dynamics of the event, and the structural integrity and makeup of the target. Some pieces of debris, largely from the interceptor, as well as target pieces whose velocity was changed, will re-enter the atmosphere immediately, while other pieces (likely target pieces with large velocity changes) will be thrown into much higher orbits. Many pieces will fall somewhere in-between these extremes. Regardless, it will be an essentially random distribution of velocities applied to pieces of debris.

Over several revolutions around the Earth, these debris fields would spread out in various dimensions, being stretched out lengthwise along their orbit even as they spread upwards and downwards in altitude and their orbits spread out around the Earth (see image of Mission Shakti debris, above). More debris will be trackable the more time progresses and the debris spreads out. The distinct field will eventually look more like bands of debris as they encircle the Earth, and are further affected by gravitational perturbations, solar winds, space weather and atmospheric friction also pushing, pulling and stretching the debris fields. Some debris will descend quickly to Earth, others will decay much more slowly. Days, months, and possibly years will pass. Some debris will be trackable, while other pieces will be too small to track. Meanwhile, other spacecraft are more and more likely to pass through this projected debris cloud. If above roughly 500 km altitude and in circular orbits, the debris will persist for decades. At lower altitudes (if even at perigee) the debris may re-enter sooner. However, both lower and higher altitudes are populated with other spacecraft and debris, and conjunctions and collisions will increase in probability.

Boothby stresses how impermissible damage may result from the long-lived nature of debris clouds, writing

> "An outer space weapon that is designed to kill a satellite by a kinetic impact in medium to high orbit would inevitably create a cloud of debris. That debris can be expected to remain in orbit for a protracted period, if not indefinitely. The individual fragments would be likely to cause damage to any space vehicles, whether civilian or military, and whether they belong to the adverse party to the armed conflict or to a neutral, that happen to pass through the affected area. Any State considering

> the use of such a method of anti-satellite operation would need to give most careful consideration to the indiscriminate weapons rule and to the proportionality rule as reflected in Article 51(5) (b) of AP1. Indeed, from a strictly weapons law perspective, it is arguable that such a method of warfare, by virtue of its inherently indiscriminate expected effects, may breach Article 51(4)(c) of AP1 if, for example, the method is employed in parts of outer space where the likelihood of interference with other protected space vehicles is high."[79]

While targeting may get better, there is no way to control the other forces which affect a debris field. When targeting a satellite, once the ASAT is launched, no one can really know where the resulting debris cloud may go, how it will change, grow, transform in size and shape, persist over time, and what spacecraft will fly through it in the future. These are the various reasons such an attack is indiscriminate according to the rules of AP1.[80] It is therefore plain that the effects of such weapons breach the law of armed conflict. Therefore, it is clear that a State should not undertake this method of warfare.

Further Questions and Conclusion

This article has sought to update the debate on the effects of ASAT weapons by showing how the resulting debris fields are more uncertain and more serious than may have previously been understood, as well as discussing how there are more (and more diverse actors) using the same orbits and altitudes as potentially permissible targets.

Additionally, the amount of space debris already in space, and the dynamic and uncertain nature of the space domain, all lean against an argument that the effects of ASAT attacks can ever be discriminate. While it may have appeared the case in decades past, when there were both fewer operational spacecraft, and much fewer debris, it is not the case now. Because

---

[79] Boothby (n 2) at 188, and footnote.

[80] Guidance on the definition of an indiscriminate attack can be found from the ICRC, who interpret a definition "based on the logical argument that means or methods of warfare whose effects cannot be limited as required by international humanitarian law should be prohibited. But this reasoning begs the question as to what those limitations are. Practice in this respect points to weapons whose effects are uncontrollable in time and space and are likely to strike military objectives and civilians or civilian objects without distinction. The US Air Force Pamphlet gives the example of biological weapons. Even though biological weapons might be directed against military objectives, their very nature means that **after being launched their effects escape from the control of the launcher and may strike both combatants and civilians** and necessarily create a risk of excessive civilian casualties" (emphasis mine) ICRC IHL Database, *Rule 12. Definition of Indiscriminate Attacks*, < https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule12 > accessed 4 October 2021.

of advances in both Space Situational Awareness (SSA), with radar and modelling, we know what debris fields from ASATs attacks look like, how they evolve over time as they orbit the Earth, how they spread, deform and grow as they transit the Earth. We also know that other users of the space domain will almost certainly cross the orbits of those debris fields.

Can debris-generating ASATs be used in a discriminating fashion? It would appear that they cannot. With each test of ASATs so far, the interceptor and the target were controlled by the same entity, yet even in those circumstances – when the controllers could steer the attack and shape the collision as they wanted – these tests still resulted in large, changing, uncontrolled, and long-lived debris clouds that rose in altitude and spread and stretched around the globe.

When and/or if an kinetic ASAT were directed at an enemy's spacecraft, their awareness of the target spacecraft will be less than it would be if it were their own spacecraft, and strikes will likely be less precise and predictable. Consequently, it will be even harder to know beforehand the effects of attacking an enemy's spacecraft, and the threat of indiscriminate effects will only increase.

This article has not discussed the proportionality question, nor the question of duties to protect the environment during the course of an armed conflict. Those issues merit serious attention, but the indiscriminate effects question has provided ample fodder for analysis. Further discussions on the legality of debris-creating ASATs is welcome, as well as action to bring actors to comply with the strictures of international law.

***

...of NOTE

The NATO Legal Gazette can be found at the official ACT web page:
http://www.act.nato.int/publications

and at LAWFAS

Disclaimer:

The NATO Legal Gazette is produced and published by Headquarters Supreme Allied Commander Transformation (HQ SACT). The NATO Legal Gazette is not a formal NATO document and does not represent the official opinions or positions of NATO or individual nations unless specifically stated. The NATO Legal Gazette is an information and knowledge management initiative, focused on improving the understanding of complex issues and facilitating information sharing. HQ SACT does not endorse or guarantee the accuracy of its content.

0449-21 NATO PRINTING & GRAPHICS

Point of Contact: Galateia Gialitaki, galateia.gialitaki@shape.nato.int