Geoff Masel Aviation Law Prize 2024

Cover Sheet & Declaration

Name: **Ava Pearson**

University: **Bond University**

Course Name & Level: **Bachelors of Law and International Relations, 4th Year Undergraduate**
(Eg, Bachelor of Laws, 4th year Undergraduate Student, Masters Student)

Graduate Diploma of Legal Practice, 1st semester

Title: **The Legality of Cyber-Attacks on Satellites Under Articles III and IV of the Outer Space Treaty**

Word Count: **4,148**
(Must be 3,000-5,000; but not exceed 10,000 words)

Due Date: Friday 8th December 2023

By submitting this paper, I certify that:

- **This paper is my own original work;**
- **If I have incorporated the work of any other person, I have fully recognised and cited it;**
- **The word count specified is truthful and accurate; and**
- **I accept that ALAANZ Ltd has the right to publish my paper in the Association's journal, *Aviation Briefs***

Signed: APearson

Date: **8 December 2023**

The Legality of Cyber-Attacks on Satellites under Articles III and IV of the *Outer Space Treaty*

Addressing Treaty Interpretation, The OST, and the Use of Force

Ava Pearson

Table of Contents

I. Introduction

Outer space is recognised as one of the four global commons; a domain that extends beyond the concept of a State's exclusive jurisdiction and requires global governance for the benefit of mankind.[1] Following the launch of the first satellite in 1957, the presence of satellites in space has exponentially increased to approximately 6,900 active satellites in orbit.[2] Satellites are of significant strategic importance to a State as each can be utilised for various functions such as communication, navigation, environmental monitoring, disaster response, and national security.[3] The growing reliance on Satellites as critical infrastructure has exposed satellites to the increased threat of physical and cyber-attacks by States and non-State actors to gain strategic dominance. A recent example of this is Russia's cyber-attack on an American satellite one hour prior to the 2022 invasion of Ukraine.[4] The destructive malware cyber-attack erased all the data on the targeted satellite system and resulted in an immediate loss of communication for the Ukrainian army.[5] Cyber-attacks on satellites are becoming more frequent and escalating global security concerns;[6] therefore, it is crucial to address the legality of these attacks.

International law provides multiple frameworks for space law, such as the *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies* ('the *Outer Space Treaty')* and the *Agreement Governing the Activities of States on the Moon and Other Celestial Bodies* ('the *Moon Agreement*').[7] The majority of treaties relating to outer space were signed before major technological advancements, therefore, these treaties do not significantly delve into the cyber aspects of outer space. The lack of direct 'cyber operation dealings' in treaties is acknowledged in the *Tallinn Manual 2.0*.[8] Prior to the recent publication of the *Tallinn Manual 2.0*, there was limited discussion and consensus on the application of public international law to the cyber sphere. The *Tallinn Manual 2.0* is a manual on the international law applicable to cyber operations which was published by the NATO Cooperative Cyber Defence Centre of Excellence.[9] Although it is not a binding instrument in international law, it is a valuable resource as it

---

[1] Center for International Relations and Sustainable Development, *Outer Space as a Global Common* (Webpage) <https://www.cirsd.org/en/expert-analysis/outer-space-as-a-global-common#:~:text=As%20the%20exploration%20and%20utilization%20of%20outer%20space,they%20have%20a%20legal%20obligation%20to%20do%20so>.

[2] Statista, *Number of active satellites from 1957 to 2022* (Webpage, 2023) <https://www.statista.com/statistics/897719/number-of-active-satellites-by-year/#:~:text=In%202022%2C%20there%20were%20an%20estimated%20total%20of,active%20satellites%20from%201957%20to%202022%20Additional%20Information>.

[3] Theodora Ogden, 'Satellite Security in New Space' (2022) 2 *Air & Space* 4.

[4] MIT Technology Review, *Russia hacked an American satellite company one hour before the Ukraine invasion* (Webpage, 2022) < https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/>.

[5] Ibid.

[6] Microsoft Network, *Attacks and cyberattacks on satellites becoming more common, says EU's top diplomat* (Webpage) < https://www.msn.com/en-xl/news/other/attacks-and-cyberattacks-on-satellites-becoming-more-common-says-eus-top-diplomat/ar-AA16GcPH>.

[7] *Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and on Celestial Bodies,* opened for signature on the 27 January 1967, 610 UNTS (entered into force 10 October 1967) ('*Outer Space Treaty*'); *The Agreement Governing the Activities of States on the Moon and Other Celestial Bodies*, opened for signature on the 18 December 1979, 1363 UNTS 3 (entered into force 11 July 1984) ('*The Moon Agreement*').

[8] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2nd ed, 2017), 3 ('*Tallinn Manual 2.0*').

[9] *Tallinn Manual 2.0* (n 8).

contains the collective opinions of two International Groups of Experts (IGEs) in international law and what they believe to be a reflection of customary international law.

This paper aims to address the unique intersection of international law and space law, and its application to the cyber realm in order to assess the legality of cyber-attacks on a States' satellite. This paper will specifically focus on whether such attacks violate articles III and IV of the *OST* by drawing on international law, the *Tallinn Manual 2.0,* the *McGill Manual International Law Applicable to Military Uses of Outer Space: Volume I* ('*McGill Manual*') and other scholars in these areas.[10] This paper proposes that cyber-attacks conducted against a State's satellite, which are attributable to another State, may contravene the prohibition on the use of force under article 2(4) of the *UN Charter* and subsequently violate article III of the *OST*. However, cyber-attacks will not violate article IV of the *OST*, which prohibits the weaponization of outer space and launching weapons of mass destruction (WMD) in orbit, as cyber-attacks do not constitute a weapon.

Only the *OST* out of the five space treaties will be analysed as it is one of the main treaty related to satellites in orbit. Further, this paper will not address liability under the *Liability Convention*.[11] It is acknowledged that there are legal issues regarding attribution due to the anonymity of some cyber-attacks and attacks committed by non-state actors. However, for the purpose of this paper, discussion regarding the attribution of a cyber-attack to a State will be limited and it is presumed that the laws of State responsibility are satisfied.

This paper identifies the difficulties in relying on the *Tallinn Manual 2.0* as it is not a binding instrument under international law. There are limited treaties dealing directly with cyber operations and sparse *opinio juris* to establish customary international law.[12] Reliance on any rules from the *Tallinn Manual 2.0* is due to the understanding that it reflects customary international law and to that extent the rules are binding on States subject to potential persistent objectors.[13] Therefore, there should be deference with respect to its use in this paper. Finally, the term "cyber-attack" is defined in this paper to encompass an array of cyber-attacks which are malicious in nature such as jamming and distributed denial of service (DDoS) attacks.

II. Outer Space Treaty

Articles III and IV of the *OST*, the obligations each article imposes, and the respective application to satellites and cyber-attacks will be analysed within this section of the paper. Article IV states in part that:

> *"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… the moon and other celestial bodies shall be used by all States Parties to the Treaty exclusively for peaceful purposes."*

---

[10] Ram Jakhu and Steven Freeland, *McGill Manual on International Law Applicable to Military Uses of Outer Space* (Centre for Research in Air and Space Law, vol I, 2022) ('*McGill Manual*').
[11] *Convention on International Liability for Damage Caused by Space Objects*, opened for signature on the 29 March 1972, 961 UNTS 187 (entered into force on 1 September 1972).
[12] *Tallinn Manual 2.0* (n 8), 2.
[13] *Tallinn Manual 2.0* (n 8), 4.

Further, article III imposes the obligation for States Parties to the Treaty to act "in accordance with international law, including the Charter of the United Nations." [14] Accordingly, this requires States to comply with international law, customary international law, and general principles such as sovereignty, non-intervention, and the prohibition of the use of force.[15]

1. Obligation to use Space for 'Peaceful Purposes'

The preamble and article IV of the *OST* emphasises the importance of, and the obligation of, States to ensure that activities in space are for peaceful purposes;[16] this obligation is also imported via article III of the *OST*. Under the *Tallinn Manual 2.0*, cyber operations conducted in space must be for peaceful purposes and this rule is reflected in article IV of the *OST*. Due to the doctrine of *lex specialis,* the wording of the *OST* overrides the wording of this customary rule, hence, the interpretation of article IV will be the focus of this section. In accordance with articles 31 and 32 of the *Vienna Convention on the Law of Treaties* (*VCLT*), this paper argues that cyber-attacks on a State's satellite does not violate article IV of the *OST*.

A. Defining 'Peaceful Purpose' in Article IV

The term 'peaceful purpose' is not defined in the *OST*. There is scholarly debate as to what constitutes non-peaceful activities, but due to the ambiguity of the terminology in the treaty, there is no general consensus. Article 31 of the *VCLT* can be used to provide clarity in interpreting the wording "for peaceful purposes".[17] Article 31(1) of the *VCLT* provides that:

> *"a treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose".*[18]

Article IV of the *OST* is made in two parts. The first part prohibits States from placing "any objects carrying nuclear weapons or any other kinds of weapons of mass destruction" into Earth's orbit. Whereas the second part specifies that "the moon and other celestial bodies shall be used by all States Parties to the Treaty exclusively for peaceful purposes." Article IV explicitly distinguishes orbit from the moon and other celestial bodies, only requiring that nuclear weapons and Weapons of Mass Destruction (WMD) are not placed in orbit. This wording choice, in its ordinary meaning, indicates that States are not obligated to use orbit for "exclusively peaceful purposes". Therefore, cyber-attacks on Satellites in orbit will not violate article IV. This interpretation is supported through the intention and subsequent practice of the States Parties to the *OST*.

Article 31(2) and (3) of the *VCLT* provides that the interpretation of terms in a treaty should take into consideration its preamble, subsequent agreements between the parties, subsequent

---

[14] *Outer Space Treaty* (n 7), art III.
[15] Du Li, 'Cyber attacks on Space Activities: Revisiting the Responsibility Regime of Article VI of the Outer Space Treaty' (2023) 63 *Space Policy* 101522, 5.
[16] *Outer Space Treaty* (n 7), preamble, art IV.
[17] *Vienna Convention on the Law of Treaties*, signed on the 23 May 1969, 1155 UNTS 331 (entered into force 27 January 1980), art 31(1) ('*VCLT*').
[18] Ibid.

practice, and any relevant rules of international law.[19] Further, the *travaux preparatoires* of a treaty are the official records of treaty negotiation which can be used to clarify the intention of a treaty, as reflected in article 32 of the *VCLT*.[20]

Since the Space Race in the 1950s and 60s, the inherent military nature and military advantage space offers to States has been recognised. With the commercialisation of space and growing non-military benefits offered by space, such as broadcasting and environmental management, technology in space is considered to have a 'dual nature' of private and military purposes.[21] Therefore, the split between 'military' and 'non-military' and 'peaceful' and 'non-peaceful' is increasingly difficult to distinguish.

In the *travaux preparatoires* of the *OST,* the United States and the USSR rejected India's proposal of extending the application of "peaceful purposes" to all areas of space, including orbit, rather than just to the moon and celestial bodies.[22] This is partially because in the 1950s, the opinions of the United States and the United Socialist Soviet Republic (USSR) was that 'peaceful' meant 'non-military'.[23] Therefore, by extending the application of "exclusively peaceful purposes" to all of space, including in orbit, the 'dual nature' of satellites in orbits would inherently violate this obligation because the use of satellites would be a non-peaceful activity.

Therefore, taking into consideration the distinct wording and intention of the parties, article IV does not require activities in orbit to be for peaceful purposes. A cyber-attack on a satellite will not violate article IV unless the cyber-attack constitutes a nuclear weapon or WMD.

B. Are Cyber-Attacks 'Nuclear Weapons' or 'WMDs'?

The first part of article IV provides an undertaking that States will not place nuclear weapons or WMDs into orbit. Cyber-attacks are not nuclear weapons. However, there is currently a legal debate regarding whether cyber-attacks constitute weapons of mass destruction.[24]

Weapons of mass destruction have been defined by the United Nations Security Council to include:

> *"atomic explosive weapons, radio-active material weapons, lethal chemical and biological weapons, and any weapons developed in the future which have characteristics comparable in destructive effect to those of the atomic bomb or other weapons mentioned above."*[25]

---

[19] *VCLT* (n 17), art 31(2), (3)(a)-(c).
[20] *VCLT* (n 17), art 32.
[21] *Tallinn Manual 2.0* (n 8), 275.
[22] *Peaceful Purposes OST* (n 26), 14.
[23] Stephan Hobe, 'The Meaning of "Peaceful Purposes" In Article V of the Outer Space Treaty' (2015) 40 *Annals Air & Space* 9, 12 ('*Peaceful Purposes OST*').
[24] Tahir Azad and Muhammad Haider, 'Cyber Warfare as an Instrument of Hybrid Warfare: A Case Study of Pakistan' (2021) 36 *Research Journal of South Asian Studies* 383, 388; Jeffrey Carr, 'The misunderstood acronym: Why cyber weapons aren't WMD' (2013) 69 *Bulletin of the Atomic Scientists* 5, 32.
[25] *Armaments: regulation and reduction,* UNSCR Res 18, UN Doc S/268/Rev.1/Corr.1 (13 February 1947).

Each cyber-attack is different in nature; therefore, it is highly fact dependant on whether a cyber-attack could amount to the definition of a weapon of mass destruction. For example, had the 2010 Stuxnet cyber-attack on an Iranian nuclear powerplant resulted in the intentional spread of nuclear material, it could be argued to constitute a weapon of mass destruction.[26] Therefore, that specific cyber-attack, if conducted on a satellite, may violate article IV of the *OST*. However, as there has not been a cyber-attack that has amounted to such levels, it is unlikely that cyber-attacks on satellites will violate article IV of the *OST*.

It is the position of this paper that a cyber-attack cannot constitute a weapon of mass destruction. In accordance with article 31(1) of the *VCLT*, the word 'weapon' must be interpreted in its ordinary meaning in good faith and in light of its object and purpose. A cyber-attack is an act and not in itself a weapon. Certain policy issues arise as to whether cyber-code can constitute a weapon due to the nature and widespread use of malicious codes. There would difficulty discerning the threshold of what code constitutes a weapon and what does not. Hence, it is unlikely that cyber-attacks can constitute a weapon. Therefore, cyber-attacks on a satellite will not violate article IV as it does not require for activities in orbit to be for "exclusively peaceful purposes" and does not reach the threshold of being a WMD.

2. Customary Obligation: Cyber Operations to have 'Respect for Space Activities'

Rule 59 of the *Tallinn Manual 2.0* requires that States conducting cyber operations in space have respect for space activities. This rule is provided for in two parts. First, the obligation for States to respect the jurisdiction and control over a satellite of a registered State. Second, the obligation for States to avoid interference with peaceful space activities.[27] Where a satellite is purely used by one State, a cyber-attack will interfere with that State's jurisdiction and control over the satellite, hence breaching rule 59(a). Further, despite practical difficulties in rule 59(b)'s application, a cyber-attack will breach rule 59(b) due to the inherently malicious nature of a cyber-attack.

A. Rule 59(a) – Jurisdiction and Control

Under rule 59(a), a "State must respect the right of States of registry to exercise jurisdiction and control over space objects appearing on registries."[28] This rule is further reiterated in rule 114 of the *McGill Manual*.[29] This rule is founded in and established due to a combination of article II of the *Convention on Registration of Objects Launched into Outer Space* ('*Registration Convention*') and article VIII of the *OST*.[30] Under article II of the *Registration Convention*, States are obligated to register a space object by means of an appropriate registry

---

[26] Cf. Australian Broadcasting Company, *Stuxnet: The real life sci-fi story of 'the world's first digital weapon'* (Webpage, 2016) < https://www.abc.net.au/triplej/programs/hack/the-worlds-first-digital-weapon-stuxnet/7926298>.
[27] *Tallinn Manual 2.0* (n 8), r 59(a)-(b).
[28] *Tallinn Manual 2.0* (n 8), r 59(a).
[29] *McGill Manual* (n 10), r 114.
[30] *Convention on Registration of Objects Launched into Outer Space*, opened for signature on the 14 January 1975, 1023 UNTS 15 (entered into force on 15 September 1976), art II.

and shall inform the Secretary-General of the United Nations of such registry.[31] The requirement to register space objects works in conjunction with article VIII of the *OST* which holds that States will retain jurisdiction and control over space objects which are registered to that State.[32] States that retain jurisdiction and control over space objects also enjoy prescriptive and enforcement jurisdiction over that object.[33] Therefore, a cyber-attack which restricts or impedes the registered State from controlling its satellite purely used by that State is an interference with the jurisdiction and control afforded to the registered State. Therefore, under certain circumstances, a cyber-attack can be in contravention to rule 59(a) of the *Tallinn Manual 2.0*. This rule will be addressed more in conjunction with sovereignty further below.

B. Rule 59(b) – Avoid Interference with Peaceful Space Activities

Rule 59(b) reads that a State must conduct its cyber operations involving outer space with due regard for the need to avoid interference with peaceful space activities of other States.[34] This rule is based on the obligation for States to act with 'due regard to corresponding interests' under article IX of the *OST*. States must take into consideration whether acts in space could be "potentially harmful interference" with other States' peaceful use of outer space. The obligation under article IX to consult with other States before proceeding with a space activity does not have sufficient State practice to be regarded as custom.[35] This is despite the IGEs regarding it as custom.

It's the position of this paper that although States are obligated to consider the potentially harmful interference of its space activities, this rule neglects the reality of anarchy and military strategy in international relations. Within the outer space paradigm, the capabilities and interests of other States are not explicitly announced due to the significant military strategy space offers. Due to the strategic significance of concealing a State's military might in outer space, it is difficult for States to practice having due regard for potentially harmful interferences. Despite this, the inherently malicious nature of cyber-attacks is in direct opposition to the obligation for States to avoid interference with peaceful space activities and therefore contravenes rule 59(b).

3. Concluding thoughts on the *Outer Space Treaty* and the *Tallinn Manual 2.0* obligations

A State will not breach its obligations under the *OST* by launching a cyber-attack on a satellite because the *OST* does not obligate States to use orbit for exclusively peaceful purposes and cyber-attacks do not constitute a WMD. Additionally, if a State conducts a military-oriented cyber-attack on a satellite to obtain information (a non-interfering cyber-attack), then it lacks the malicious nature to violate the obligation to avoid interference with peaceful space activities. Unless the cyber-attack violates international law principles such the prohibition on the use of force, it will unlikely rise to the threshold to violate international law or the *OST*.

---

[31] Ibid.
[32] *Outer Space Treaty* (n 7), art VIII.
[33] *Tallinn Manual 2.0* (n 8), 278.
[34] *Tallinn Manual 2.0* (n 8), r 59(a), (b).
[35] *Tallinn Manual 2.0* (n 8), 278.

III. Use of Force

1. Scope of Use of Force

The prohibition against the use of force is a *jus cogens* norm established in customary international law and under article 2(4) of the *UN charter*.[36] The prohibition on the use of force traditionally relates to acts such as armed force, an armed attack, or is related to military force. This interpretation of 'force' is consistent with the preamble of the *UN Charter* where it identifies the Charter's goals of ensuring armed force is not used and with *Declaration of Friendly Relations* where it outlines use of force involving military force.[37] Rule 58(b) of the *Tallinn Manual 2.0* outlines that cyber operations in outer space are subject to international law limitations on the use of force. If a cyber-attack satisfies the threshold and constitutes an unlawful use of force, then it would violate both rule 58(b) of the *Tallinn Manual 2.0* and article III of the *OST*.

2. Scope of Use of Force in Cyber Context

Despite the prohibition on the use of force traditionally referring to military force, it is also applicable in the cyber context.[38] The damage caused from a State violating the prohibition on the use of force does not need to arise from the use of traditional kinetic weapons.[39] Article 2(4) of the *UN Charter* applies with respect to the use of biological and chemical weapons, which demonstrates that armed force does not need to be of a kinetic nature like traditional weapons.[40] This paper argues that the prohibition on the use of force also applies to the cyber context.[41] The majority of scholars and the IGEs in the *Tallinn Manual 2.0* use an "effects-based approach" to determine whether a cyber act constitutes armed force.[42] Rule 68 of the *Tallinn Manual 2.0* reads

> *"cyber operation that constitute a threat or use of force against the territorial integrity or political independence of any state, or that is an any other matter inconsistent with the purpose of the United Nations, is unlawful."*[43]

---

[36] *Military and Paramilitary Activities in and against Nicaragua Case (Nicaragua v United States of America)* (Jurisdiction and Admissibility) [1986] ICJ Rep 392, [73]; Charter of the United Nations ('*UN Charter*'), art 2(7); *Military and Paramilitary Activities in and against Nicaragua Case (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep 14 ('*Nicaragua*'), [187]-[190]; *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (Advisory Opinion) [2004] ICJ Rep 136, [87]; *UN Charter* (n 36), art 2(4).
[37] *UN Charter* (n 36), preamble; *The Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States,* GA Res 2625, UN Doc A/Res/25/2625 (24 October 1970).
[38] *Tallinn Manual 2.0* (n 8), r 68.
[39] Johann-Christoph Woltag, *Max Planck Encyclopedia of Public International Law* (August 2015), "Cyber Warfare", [8] ('*Max Planck Cyber Warfare*').
[40] *UN Charter* (n 36), art 2(4); *Max Planck Cyber Warfare* (n 39), [8].
[41] *Tallinn Manual* (n 8), r 68.
[42] *Max Planck Cyber Warfare* (n 39), [8]; Michael Schmitt and Brian O'Donnell, "Computer Network Attack and International Law" (2002) 76 *International Law Studies* 103, 103; *Tallinn Manual 2.0* (n 8), r 11.
[43] *Tallinn Manual 2.0* (n 8), r 68.

Despite the wording of the rule 68, it is not essential that acts are directed against a State's territorial integrity or political independence.[44] The crucial aspect of this rule is that State's conducting cyber operations ensure that the acts are consistent with the purpose of the United Nations.[45] Therefore, the nature of the attack and its effects must be considered to determine whether the act constitutes a use of force.[46] This approach to assessing the prohibition on the use of force is consistent with the decision in *Nicaragua* where the International Court of Justice took into consideration the "scale and effect" of an attack to determine if an act constitutes a use of force.[47]

To determine whether a cyber-attack constitutes a use of force, factors such as severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement, presumptive legality should be considered.[48] The most significant of these factors is the severity of the attack. These factors are used to determine whether an act is analogous to a traditional use of force. For use of force to arise there typically needs to be a physical manifestation of damage or injury from the cyber-attack.[49]

3. Sovereignty Thresholds in the Cyber Context

A violation on the prohibition on the use of force inherently requires a breach of a State's sovereignty. As recognised in the *Tallinn Manual 2.0,* the principle of sovereignty extends to cyberspace.[50] Similar to outer space, cyberspace is not subject to claims of sovereignty. Both the *Tallinn Manual 2.0* and the UN Group of Governmental Experts (UNGGE) have recognised that the principle of sovereignty extends to cyberspace and cyber operations.[51] As stated by the UNGGE,

> *"State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory."*[52]

Further, the UN Charter also applies in the cyber realm.[53] Therefore, a States' sovereignty extends to the cyber realm and must be respected accordingly.

---

[44] *Tallinn Manual 2.0* (n 8), 329.
[45] Ibid.
[46] *Tallinn Manual 2.0* (n 8), r 69.
[47] *Nicaragua* (n 36), [195].
[48] *Tallinn Manual 2.0* (n 8), 333-336.
[49] *Tallinn Manual 2.0* (n 8), 333.
[50] *Tallinn Manual 2.0* (n 8), r 1.
[51] *Tallinn Manual 2.0* (n 8), r 1; UNGA, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 24 June 2013, UN Doc A/68/98, [20]; UNGA, *Report of the Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174, 22 July 2015, [27], [28(b)].
[52] Ibid.
[53] Ibid.

4. Thresholds to Violate Article 2(4) in Cyber Space

A. Physical Damage

Any cyber-attack on a satellite that results in physical damage or injury in the territorial State will be a breach of sovereignty. Scholars agree that the manifestation of physical consequences by remote means on that territory constitutes a violation of sovereignty.[54]

i. Stuxnet: Physical Damage and Use of Force

The Stuxnet cyber-attack is an example where a cyber-attack could amount to a use of force under article 2(4) of the *UN Charter*. Although Stuxnet is not specific to satellite use, this cyber-attack is regarded as a 'game changer' due to its physical effects on Iran's critical infrastructure.[55] In 2010, a virus called Stuxnet was detected in the computer systems of Iran's nuclear power plant. It was designed to change the rotor speeds of the centrifuges that are used to enrich uranium. The change in rotor speed resulted in an irregular spin which caused damage to the centrifuges.[56] The attack was not specifically attributed to another State but it is generally speculated that it was conducted by American and Israeli intelligence agencies.[57]

If the cyber-attack satisfies the laws of State responsibility, Stuxnet is a key example of a cyber-attack violating the prohibition on the use of force. There is emerging consensus that Stuxnet constituted a use of force as it satisfies the severity, immediacy, directness, and invasiveness thresholds as outlined in the *Tallinn Manual 2.0*.[58] Stuxnet was a direct and invasive cyber-attack on a critical piece of infrastructure which resulted in physical damage.[59]

As demonstrated by Stuxnet, cyber-attacks can violate the prohibition of the use of force in article 2(4) of the *UN Charter*. Hence, a cyber-attack on a satellite that satisfies the threshold of the 'effects based' assessment outlined in the *Tallinn Manual 2.0* can violate the prohibition on the use of force and subsequently article III of the *OST*.

B. Loss of functionality

This section of the paper suggests that loss of functionality of a satellite by means of jamming or DDoS attacks is unlikely to reach the threshold needed to constitute a use of force, as demonstrated by an effects-based assessment and State practice. In 2007, Russia launched a DDoS cyber-attack against Estonia which halted the Estonian government, television and bank websites. Although the attack could not be attributed to a State, Estonia reported this cyber-

---

[54] *Tallinn Manual 2.0* (n 8), 20-21.
[55] Andrew Foltz, 'Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force"Debate' (2012) 67 *Joint Force Quarterly* 40, 4 ('*Stuxnet and Use of Force*').
[56] Josh Fruhlinger, *Stuxnet explained: The first known cyberweapon* (Web Page, 2022) <https://www.csoonline.com/article/3218104/stuxnet-explained-the-first-known-cyberweapon.html#:~:text=Stuxnet%20is%20a%20powerful%20computer,of%20the%20Iranian%20nuclear%20program>.
[57] *Stuxnet and Use of Force* (n 55), 5.
[58] Ibid.
[59] Ibid.

attack to NATO.[60] NATO concluded that a DDoS attack did not violate the prohibition on the use of force.[61] Following 2007, there have been numerous instances where the jamming of satellite transmissions has not amounted to a use of force such as the in the "Cuban disruption of Iranian Broadcasts in 2009; Iranian disruption of Eutelsat transmissions since 2009; the subject of formal protest to the ITU; Brazilian hackers' disruption of US Navy FLTSAT-8 in 2010; Jordanian jamming of Al-Jazeera transmissions in 2011; and China's blocking of BBC transmission in 2012."[62] Although these are only a few examples of State practice in relation to electromagnetic interference such as jamming or DDoS attacks, these instances demonstrate that State practice is reluctant to constitute stand-alone cyber operations by States as armed attacks or a use of force.[63] In many of the circumstances above, the cyber operation halted television broadcasting or temporarily hacked military transponders. When assessing the effects of these cyber-attacks, many of these scenarios lacked severity in consequences, military character, and were not invasive as many targeted TV stations. Further, these cyber-attacks were not causally connect any significant physical damage to the target State and therefore lack the required physical damage or injury needed to constitute a use of force. Referring back to the IGEs' conclusions surrounding sovereignty and use of force, cyber-attacks that cause physical damage are likely to be a use of force under article 2(4). Whereas, loss of functionality, such as jamming or DDoS, are less likely to be a use of force depending on the effects of the cyber-attack. As agreed by the IGEs, non-destructive cyber psychological operations intended solely to undermine confidence in a government does not constitute a use of force.

IV. Conclusion

This paper aimed to address whether cyber-attacks conducted by a State against another State's satellite breaches any obligations under articles III and IV of the *OST*. Article IV of the *OST* only prohibits the placement of nuclear weapons and WMDs into Earth's orbit. Since cyber-attacks and coding do not constitute a weapon or a WMD, the use of cyber-attacks on orbital Satellites does not violate article IV. Despite customary international law requiring that States use space for exclusively peaceful purposes, due to the doctrine of *lex specialis*, the *OST* 's interpretation must take precedent.

State practice has demonstrated so far that simple jamming and DDoS attacks will unlikely violate article 2(4) of the *UN Charter* where there is only a temporary loss of functionality of services and infrastructure provided for by satellites. However, as acknowledged, most of the State practice referred to was not severe in nature, was targeted towards television broadcasting companies, was only temporary and had no, or limited, physical damage. Therefore, this paper has proposed that loss of functionality can constitute a violation of article 2(4) where there is sufficient gravity of the effects of the cyber-attack and other elements referred to by the IGEs are considered. Further, as seen with the analysis of the Stuxnet virus, a cyber-attack that causes physical damage in the territory of the target State, or to the satellite, will likely constitute a use of force.

---

[60] Arie J. Schaap, 'Cyber Warfare Operations: Development and Use under International Law' (2009) 64(1) Air Force Law Review 121, 146 ('*Cyber Warfare Operations*').
[61] Ibid.
[62] Vincent L. DeFabo, 'Rethinking Cyberspace Operations: Widespread Electromagnetic Jamming by States Indicates Cyber Interference Is Not a Use of Force' (2021) 86(2) Journal of Air Law and Commerce 219, 252.
[63] Ibid.

Bibliography

Webpage

Australian Broadcasting Company, *Stuxnet: The real life sci-fi story of 'the world's first digital weapon'* (Webpage, 2016) < https://www.abc.net.au/triplej/programs/hack/the-worlds-first-digital-weapon-stuxnet/7926298>

Center for International Relations and Sustainable Development, *Outer Space as a Global Common* (Webpage) <https://www.cirsd.org/en/expert-analysis/outer-space-as-a-global-common#:~:text=As%20the%20exploration%20and%20utilization%20of%20outer%20space,they%20have%20a%20legal%20obligation%20to%20do%20so>

Microsoft Network, *Attacks and cyberattacks on satellites becoming more common, says EU's top diplomat* (Webpage) < https://www.msn.com/en-xl/news/other/attacks-and-cyberattacks-on-satellites-becoming-more-common-says-eus-top-diplomat/ar-AA16GcPH>

MIT Technology Review, *Russia hacked an American satellite company one hour before the Ukraine invasion* (Webpage, 2022) < https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/>

United Nations Office for Disarmament Affairs, *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies* (Webpage) <https://treaties.unoda.org/t/outer_space>

United Nations, *Agreement governing the Activities of States on the Moon and Other Celestial Bodies* (Webpage) <https://treaties.un.org/Pages/showDetails.aspx?objid=080000028003b946>

Thomas Roberts, *Popular Orbits 101* (Web Page, 2017)<https://aerospace.csis.org/aerospace101/earth-orbit-101/#:~:text=The%20majority%20of%20satellites%20orbiting,relative%20closeness%20to%20the%20Earth>.

Chatham House, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention* (Web Page, 2019), [43] <https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks/2-application-sovereignty-cyberspace>

Josh Fruhlinger, *Stuxnet explained: The first known cyberweapon* (Web Page, 2022) <https://www.csoonline.com/article/3218104/stuxnet-explained-the-first-known-cyberweapon.html#:~:text=Stuxnet%20is%20a%20powerful%20computer,of%20the%20Iranian%20nuclear%20program>

Article

Andrew Foltz, 'Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force"Debate' (2012) 67 *Joint Force Quarterly* 40

Du Li, 'Cyber attacks on Space Activities: Revisiting the Responsibility Regime of Article VI of the Outer Space Treaty' (2023) 63 *Space Policy* 101522

Jeffrey Carr, 'The misunderstood acronym: Why cyber weapons aren't WMD' (2013) 69 *Bulletin of the Atomic Scientists* 5

Stephan Hobe, 'The Meaning of "Peaceful Purposes" In Article V of the Outer Space Treaty' (2015) 40 *Annals Air & Space* 9

Tahir Azad and Muhammad Haider, 'Cyber Warfare as an Instrument of Hybrid Warfare: A Case Study of Pakistan' (2021) 36 *Research Journal of South Asian Studies* 383, 388
Theodora Ogden, 'Satellite Security in New Space' (2022) 2 *Air & Space* 4

Martin Svec, 'Outer Space, an Area Recognised as Res Communis Omnium: Limits of National Space Mining Law' (2022) 60 *Space Policy*

Michael Schmitt and Brian O'Donnell, "Computer Network Attack and International Law" (2002) 76 *International Law Studies* 103

Arie J. Schaap, 'Cyber Warfare Operations: Development and Use under International Law' (2009) 64(1) Air Force Law Review 121

Vincent L. DeFabo, 'Rethinking Cyberspace Operations: Widespread Electromagnetic Jamming by States Indicates Cyber Interference Is Not a Use of Force' (2021) 86(2) Journal of Air Law and Commerce 219

Priyanka R. Dev, 'Use of Force and Armed Attack Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response' (2015) 50(2-3) Texas International Law Journal 381

Book

Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2nd ed, 2017)

Ram Jakhu and Steven Freeland, *McGill Manual on International Law Applicable to Military Uses of Outer Space* (Centre for Research in Air and Space Law, vol I, 2022)

Joan Fitzpatrick, 'Sovereignty, Territoriality, and the Rule of Law' (2002) 25(3) *Hastings International and Comparative Law Review* 303

Dan Svantesson et al., *The Developing Concept ofSovereignty: Considerations for Defence Operations in Cyberspace and Outer Space* (Technology and Jurisdiction Research Team, 2021)

Treaties and International Instruments

Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space, opened for signature on the 22 April 1968, 672 UNTS 119 (entered into force on 3 December 1968)

Charter of the United Nations

Convention on International Liability for Damage Caused by Space Objects, opened for signature on the 29 March 1972, 961 UNTS 187 (entered into force on 1 September 1972).
Convention on Registration of Objects Launched into Outer Space, opened for signature on the 14 January 1975, 1023 UNTS 15 (entered into force on 15 September 1976)

Declaration of the Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space, UNGA Res XVIII, 1st Comm, 18th sess, Agenda Item 28(a), UN Doc A/RES/18/1962 (13 December 1963)

International Cooperation in the Peaceful Uses of Outer Space, UNGA Res 55/122, 4th Comm, 55th sess, Agenda Item 83, UN Doc A/Res/55/122 (27 February 2001)

Reducing space threats through norms, rules and principles of responsible behaviours, UNGA Res 75/36, 1st Comm, 75th sess, Agenda Item 101(a), UN Doc A/RES/75/36 (16 December 2020)

The Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, opened for signature on the 18 December 1979, 1363 UNTS 3 (entered into force 11 July 1984)

Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and on Celestial Bodies, opened for signature on the 27 January 1967, 610 UNTS (entered into force 10 October 1967)

Vienna Convention on the Law of Treaties, signed on the 23 May 1969, 1155 UNTS 331 (entered into force 27 January 1980), art 31(1)

The Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States, GA Res 2625, UN Doc A/Res/25/2625 (24 October 1970)

UNGA (2013), *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 24 June 2013, UN Doc A/68/98

UNGA (2015), *Report of the Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174, 22 July 2015

Encyclopaedia

Max Planck, *Max Planck Encyclopedia of Public International Law* (April 2011), "Sovereignty"

Philip Kunig, *Max Planck Encyclopedia of Public International Law* (April 2008), "Intervention, Prohibition on"

Johann-Christoph Woltag, *Max Planck Encyclopedia of Public International Law* (August 2015), "Cyber Warfare"

Cases

Corfu Channel Case (United Kingdom v. Albania) (Separate Opinion Judge Alvarez) [1949] ICJ Rep 4

North Sea Continental Shelf Cases (Federal Republic of Germany v. Denmark and Federal Republic of Germany v. The Netherlands) (Judgment), Dissenting Opinion of Judge Lachs [1969] ICJ Rep 3

Certain Activities carried out by Nicaragua in the Border Area (Costa Rica v Nicaragua), (Judgment) ICJ Rep 2015

Military and Paramilitary Activities in and against Nicaragua Case (Nicaragua v United States of America) (Merits) [1986] ICJ Rep 14

Military and Paramilitary Activities in and against Nicaragua Case (Nicaragua v United States of America) (Jurisdiction and Admissibility) [1986] ICJ Rep 392

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (Advisory Opinion) [2004] ICJ Rep 136