Junctions and thresholds in space and cyber security contexts

08 October 2024 Laetitia Cesari Researcher - University of Luxembourg

The recent UN Convention Against Cybercrime highlights the need for specific protections tailored to outer space

Far from being a legal vacuum, outer space is governed by an international legal framework, including the Outer Space Treaty (OST)[1] , designed to provide a framework for the peaceful exploration and use of outer space. Drafted in the 1960s, the OST is often regarded as an international security treaty, although it is not explicitly formulated as such. A key instrument for cooperation between States, it establishes a number of fundamental principles aimed at promoting peaceful uses and exploration of outer space. However, the OST neither refers to a specific technology nor mentions

counterspace capabilities or malicious cyber activities against space infrastructure on Earth or in outer space. Alongside this framework, States have recently drafted a Convention against Cybercrime at the UN level[2], marking a significant step forward in the international fight against cyber threats.

The OST provisions have been essential in guiding the negotiations on the Prevention of an Arms Race in Outer Space (PAROS) agenda item at the Conference on Disarmament, which aims to extend and strengthen confidence- and security-building measures applicable to space activities. Although the OST does not completely ban military activities in outer space, it sets out some limits on States with regard to prohibited weapons systems. For example, the deployment of satellites for military reconnaissance or communication purposes is tolerated, leaving room for States to interpret what constitutes a peaceful use of outer space. Conversely, pursuant to Article IV, States shall not place nuclear weapons or other weapons of mass destruction in Earth orbit, on the Moon or any other celestial body[3]. In recent discussions, experts recognised that threats to or involving space systems could involve both kinetic and non-kinetic means, resulting in a gradient of reversible or irreversible effects along four vectors: Earth-to-space, space-to-Earth, space-to-space and Earth-to- Earth[4].

While there are no internationally accepted criteria yet for determining whether a non-kinetic counterspace capability is equivalent to an armed attack[5] dialogue could be open on hostile cyber operations. Roscini adopts an “effects-based approach” to presume that the notion of “force” has an evolving meaning[6]. Tepper considers that the scale and effects of some capabilities are so damaging that they come close to being classified as “use of force”[7]. Adversely, for Smith, the impact of non-kinetic capabilities does not have the characteristics in particular lethality, that would make them a weapon[8]. However, because of the economic and psychological effect that can be caused by the interruption of certain space services, the use of counterspace capabilities can have serious consequences for civilian populations and critical or essential infrastructures (health, energy, water, transport)[9]. According to some experts, “to focus only on the bloodless

potential of space and cyberspace capabilities would seem to miss the point, because their other potential effects are still quite frightening"[10]. This was the case with the interruption of services provided by the KA-SAT satellite to its European customers[11]. Even if there is no threshold precisely defined by States, malicious cyber activities targeting space infrastructures can, in certain cases, constitute a use of force and violate international law.

Evaluating the effect, scale, and scope of non-kinetic counterspace capability may therefore prove useful in assessing their admissibility under international rules. As cyber hostile activities are expected to be an increasingly important threat[12], especially against space infrastructures, lawmakers must prepare for this reality and anticipate consequences and collateral damages, particularly given the potentially widespread and disruptive impacts.

Clear understanding of what is and is not permissible at the international level is important, especially in the context of cyber protection of space infrastructures. Although the recent United Nations Convention against Cybercrime provides guidance for the general use and protection of cyberspace[13], it may be necessary to work on the specificities of outer space to ensure clear and coherent protection and mitigate potential threats.

---

[1] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies Adopted by the General Assembly in its resolution 2222 (XXI) of 19 December 1966, entry into force on 10 October 1967.

[2] Draft United Nations convention against cybercrime Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes, Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, United Nations A/AC.291/L.15, 7 August 2024.

[3] Outer Space Treaty, Article IV.

[4] Report of the Group of Governmental Experts on further practical measures for the prevention of an arms race in outer space, August 2024.

[5] Use of Force in Cyberspace, Congressional Research Service, In Focus, 14 December 2023.

[6] Marco Roscini, Cyber Operations and the Use of Force in International Law, Oxford University Press 2014, page 53.

[7] Eytan Tepper, The Laws of Space Warfare: A Tale of Non-Binding International Agreements, Maryland Law Review, Volume 83, Issue 2, Article 4, 2024, page 495; Harold Hongju Koh, Remarks: Twenty-First-Century International Lawmaking, Georgetown Law Journal, Volume 101, 2012, page 725.

[8] Shane Smith, Cyber Threats and Weapons of Mass Destruction, Proceedings, Center for the Study of Weapons of Mass Destruction, National Defense University, June 2021, page 3.

[9] Nivedita Raju, Space security governance: steps to limit the human costs of military operations in outer space, 22 August 2023, ICRC Humanitarian Law and Policy.

[10] Duncan Blake and Joseph S. Imburgia, “Bloodless Weapons”? The need to conduct legal reviews of certain capabilities and the implications of defining them as “weapons”, Air Force Law Review (Issue 66), Winter 2010.
[11]Laetitia Cesari, Commercial Space Operators on the Digital Battlefield, CIGI Essay Series, Cybersecurity and Outer Space, 29 January 2023.
[12] Tepper, The Laws of Space Warfare: A Tale of Non-Binding International Agreements, page 493.
[13] Draft United Nations convention against cybercrime Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes.