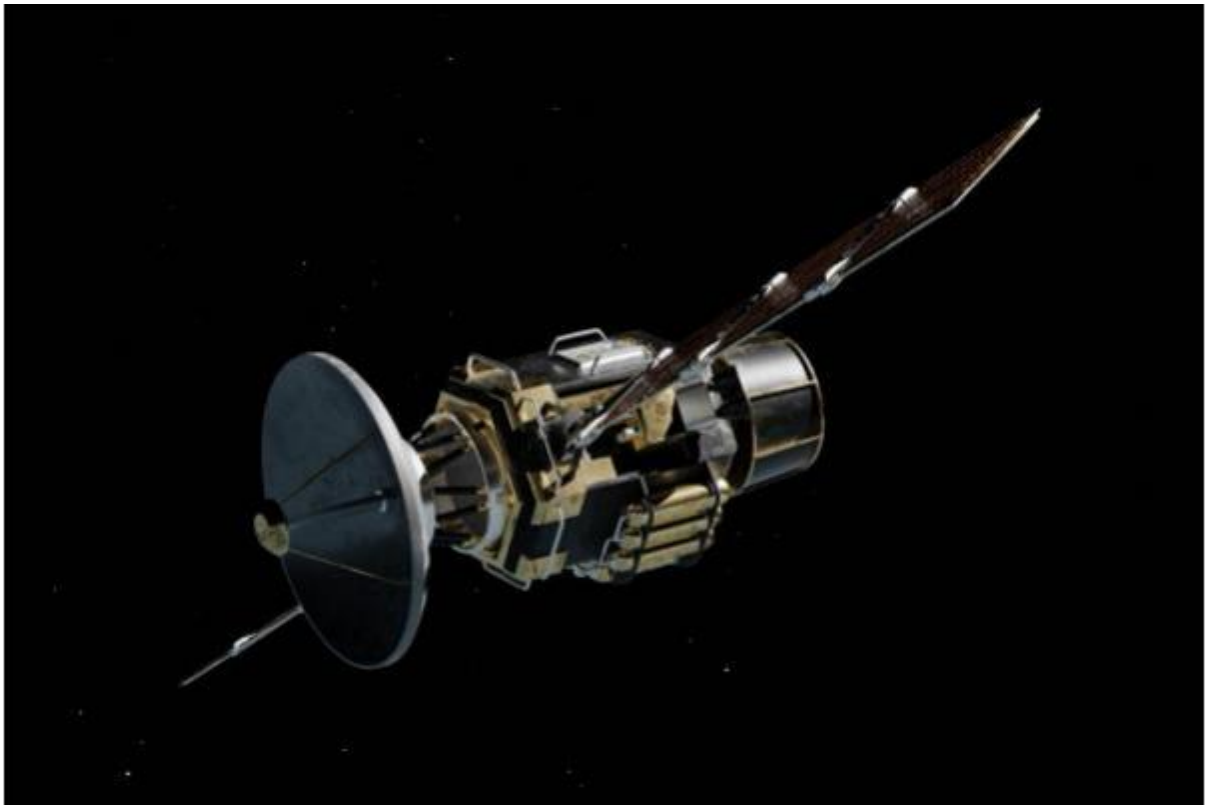
Junctions and thresholds in space and cyber security contexts

19 November 2024, Laetitia Cesari, Researcher - University of Luxembourg

The recent diplomatic discussions at the Conference on Disarmament highlight 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), 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 debated these topics at the multilateral level, especially during discussions at the First Committee of the United Nations General Assembly.

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. 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.

While there are no internationally accepted criteria yet for determining whether a non-kinetic counterspace capability is equivalent to an armed attack 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. Tepper considers that the scale and effects of some capabilities are so damaging that they come close to being classified as “use of force”. Adversely, for Smith, the impact of non-kinetic capabilities does not have the characteristics, in particular lethality, that would make them a weapon. 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). 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". This was the case with the interruption of services provided by the KA-SAT satellite to its European customers. 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, 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 discussions at the Conference on Disarmament have been instrumental in identifying risks and threats faced by space infrastructure, it may be necessary to work on the specificities of cybersecurity of outer space to ensure clear and coherent protection and mitigate potential disruptions.