Special Political and Decolonization Committee

Measures to Regulate the Use of Starlink in Armed Conflicts and to Ensure International Accountability.

-Committee Guide-

Erda Meholli
-Chairperson-
Zahra Kobeisi
-Chairperson-
Zoe Sandkühler
-Chairperson-

TABLE OF CONTENTS

I. INTRODUCTION

a. INTRODUCTION TO THE COMMITEE

to the work of the Fourth Committee. of the United Nations General Assembly, and as such, it consists of all 193 United Nations Member States. It is a plenary committee, meaning every country with a seat in the General Assembly is a member and can participate in its work. It was formed in 1990 when the Decolonization Committee and the Special Political Committee were combined. The UN established the “International Decade for the Eradication of Colonialism” from 1990 to 2000, marking an important time for the UN’s decolonization work. When the UN was founded, 750 million people lived under colonial rule. Since 1945, over 80 former colonies have gained independence, thanks to the work of the Fourth Committee. Today, fewer than two million people live in 17 non-self-governing territories, and SPECPOL holds hearings with petitioners, including civil society organizations and private individuals, from these areas. SPECPOL also covers issues related to Palestinian refugees as well as topics like the effects of atomic radiation, peacekeeping operations, space exploration, and international cooperation for peaceful uses of outer space.

b. INTRODUCTION TO THE TOPIC

The intersection of commercial space technology and modern warfare has fundamentally disrupted the traditional, state-centric architecture of global security. At the center of this paradigm shift is SpaceX’s Starlink, a low-Earth orbit (LEO) satellite constellation designed to provide global high-speed civilian internet. In contemporary conflicts, most notably the war in Ukraine, Starlink has transitioned from a humanitarian lifeline into a decisive, weaponized asset. This evolution exposes a critical vulnerability in the international legal order: the rapid commercialization of space has outpaced the legal frameworks designed to govern it. By examining the dual-use dilemma, the rise of corporate sovereignty, the gaps in international accountability, and the mechanisms for future regulation, it becomes evident that the privatization of battlefield infrastructure demands a radical restructuring of international humanitarian law (IHL) and state oversight.

II. FACTS AND CURRENT SITUATION

a. FACTS

State Responsibility under International Law: Under Article VI of the 1967 Outer Space Treaty (OST), the US government bears "international responsibility" for national activities in space, including those carried out by non-governmental entities like SpaceX. This means the US is responsible for authorizing and continuously supervising Starlink's operations, creating a direct link between private actions and state accountability.

Challenges to the Principle of Distinction: International Humanitarian Law (IHL) requires distinguishing between military objectives and civilian objects. Because Starlink terminals are used for both civilian internet and drone operations, it is unclear when they become lawful military targets.

Targeting Dual-Use Infrastructure: Legal debates focus on whether Starlink's satellite constellation could become a legitimate military objective if it makes an "effective contribution to military action".

Licensing and Regulatory Control: States are increasingly focusing on licensing and landing rights to control how Starlink operates within their territory. Iran and Russia have raised the issue of Starlink's activities at the United Nations, arguing its use violates sovereignty.

Proposed "Rules of Engagement" in Space: Experts propose new norms to prevent escalation, including:

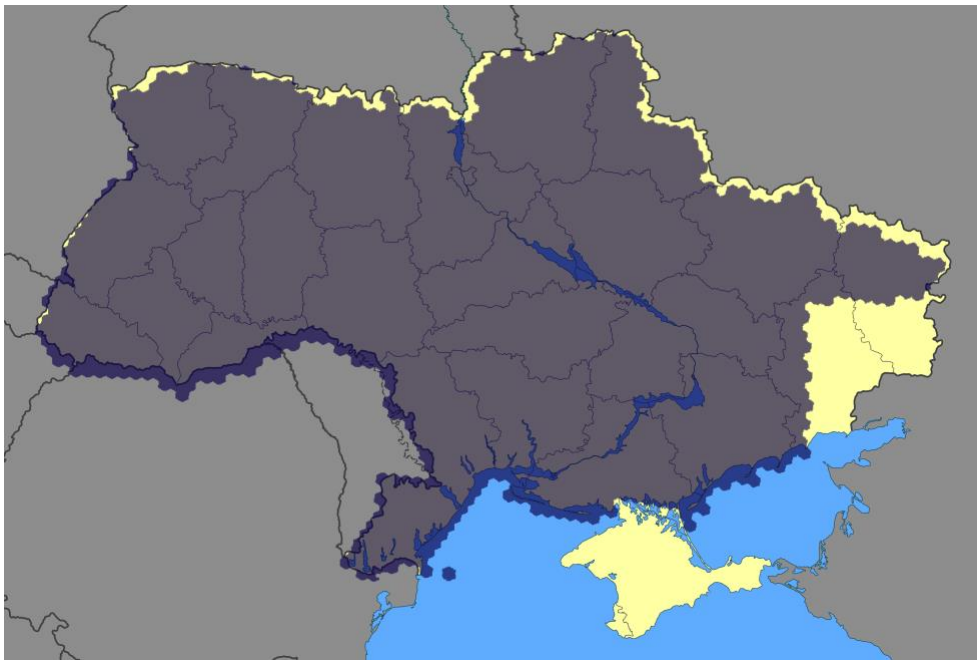
- Proximity thresholds: Minimum safe distances between satellites to prevent collisions.
- Tamper warning protocols: Automated alerts to warn of interference with satellite command systems.
- "Space hotlines": Emergency communication channels between nations to deconflict unexpected actions.

Export Controls and Contractual Limitations: The U.S. government has used contractual agreements to limit the misuse of terminals (e.g., prohibiting use for offensive drone operations).

Emerging International Norms: The work of the Open-Ended Working Group (OEWG) on Reducing Space Threats is active in creating transparency and confidence-building measures to reduce the risk of miscalculation involving commercial assets.

Data Privacy Concerns: The absence of transparency on where Starlink routes user data has led to calls for greater accountability regarding GDPR requirements.

b. CURRENT SITUATION



Approximate Starlink coverage of Ukraine as of September 2023, according to the official map on the Starlink website. Areas along the Belarusian and Russian borders, Crimea, and parts of the Donbas are not covered.

Critical infrastructure: Estimates suggest that over 20,000 terminals have been activated in Ukraine since the beginning of the war to maintain military and civilian communication.

A major shift has occurred from passive service provision to active technical gatekeeping in active combat zones:

The Ukraine Whitelist System: To combat the illicit use of smuggled Starlink terminals by Russian forces, SpaceX and the Ukrainian Ministry of Defense implemented a strict government whitelist system. Any terminal operating within Ukraine must now be formally verified and approved through Ukraine's DELTA combat system to prevent unvetted devices from accessing the network.

Neutralizing "Weaponized" Drones: In early 2026, Russian forces began mounting Starlink terminals directly onto long-range guidance drones to bypass electronic jamming. Following direct coordination between the Ukrainian defense minister and SpaceX, SpaceX successfully disabled unauthorized access for these specific configurations, demonstrating that a private corporation holds immediate, real-time control over tactical combat outcomes.

The U.S. Department of Defense is systematically transferring its reliance from commercial Starlink terms to fully controlled, classified military variants:

The MILNET System: The Pentagon has deepened its integration with Starshield – SpaceX's military-exclusive sister network. The U.S. Space Force Space Systems Command awarded SpaceX a 57 million Dollar contract to test the Link-182 space-to-space data network for its classified MILNET network. This effectively separates the U.S. military's tactical communication from the civilian Starlink infrastructure, resolving some International Humanitarian Law (IHL) concerns regarding the targeting of civilian infrastructure.

III. DEFINTION OF KEY TERMS

These are the core Technological and Operational terms:

Starlink (SpaceX): A satellite internet constellation operated by a private commercial entity (SpaceX) using Low Earth Orbit (LEO) satellites to provide global high-speed internet.

Dual-Use Technology: Technologies designed for civilian purposes but capable of being used for military purposes, such as Starlink providing communication to both civilians and combatants.

Satellite Internet Constellation: A large network of satellites working together to provide continuous, high-speed internet coverage globally, particularly useful in areas with destroyed or limited ground infrastructure.

Low Earth Orbit (LEO): The orbit (roughly 550 km to 2,000 km altitude) where Starlink satellites operate, providing low-latency internet comparable to terrestrial networks.

Ground Terminals/Receiving Stations: User equipment (dishes) that receive signals from satellites, essential for enabling internet access on the ground in conflict zones.

Geofencing/Geo-restriction: The technical capability to restrict Starlink satellite availability in specific geographic areas, often used to prevent the use of technology in designated battle zones.

These are a few of the Legal and Regulatory terms (based on International Law):

Outer Space Treaty (OST, 1967) - Article VI: Requires states (like the US) to provide authorization and "continuing supervision" of national non-governmental entities' (like SpaceX) activities in space.

International Responsibility: The obligation of a state to be responsible for national activities in outer space, whether carried out by governmental or non-governmental entities.

State Liability (1972 Liability Convention): A launching state is liable for damage caused by its space objects on Earth or to other space objects.

IV. MAJOR PARTIES INVOLVED

SpaceX and Elon Musk: As the operator of Starlink, the company controls the technology, with CEO Elon Musk holding significant, unelected influence over when the service is active in conflict zones.

United States Government: Under Article VI of the Outer Space Treaty (OST), the US is responsible for ensuring its non-governmental entities (SpaceX) comply with international law. Key agencies include the DoD, FCC, and FAA.

Ukraine: A primary user of Starlink for military communications, with the service often acting as the "backbone" of their front-line connectivity.

Russia: Has accused Starlink of being a party to the conflict and has threatened to target the satellites as legitimate military objectives.

Iran: Has challenged Starlink at the UN for violating national sovereignty and regulations by operating without local licensing.

International Bodies: The UN Office for Outer Space Affairs (UNOOSA) and the International Telecommunication Union (ITU) are involved in discussions regarding the regulation of satellite constellations.

V. EVALUATION OF PREVIOUS ATTEMPTS

Previous attempts of regulation have been fragmented, relying heavily on corporate policy, bilateral agreements, and retrospective technological fixes rather than comprehensive international treaties. These are a few of the Attempts to regulate Starlink:

Corporate Self-Regulation (Geofencing): SpaceX has used geofencing to restrict Starlink functionality in contested areas (e.g., restricting use over Crimea/Sevastopol) to limit the weaponization of its network, as highlighted in reports of a 2022 incident. These actions, while limiting immediate escalation, raise concerns about a private actor influencing the course of an armed conflict.

Ad-hoc State-Corporate Agreements: In response to potential misuse of terminals by adversaries, such as reports in 2024–2025 of Russia accessing Starlink through third parties, the U.S. DoD and Ukraine have tightened regulations, moving from unauthorized use to a structured, licensed, and secured service model.

Technical Countermeasures (2025–2026): To address unauthorized use by Russian forces on drones, SpaceX, working with Ukrainian authorities, implemented “whitelist” procedures and technical restrictions on terminal movements to ensure only authorized units have access.

Limitations of Previous Approaches: A **2025 USAID Inspector General report** revealed that initial terminal transfers to Ukraine lacked robust, enforced safeguards to prevent misuse by military actors, relying instead on over-arching transfer agreements.

IV. POSSIBLE SOLUTIONS

Regulation requires adapting existing treaties to private space actors. Under Article VI of the 1967 Outer Space Treaty, states bear responsibility for national space activities. The UN Office for Outer Space Affairs (UNOOSA) should formalize protocols translating this into direct legal liability for home states, making the US government legally accountable for the deployment of SpaceX technology. Additionally, updating the Geneva Conventions must establish clear rules for digital infrastructure. International law must define when a commercial satellite loses civilian immunity and becomes a legitimate military objective. Utilizing a network for active command-and-control functions, like drone targeting, compromises its protected status. Clear boundaries will prevent miscalculations and protect civilian infrastructure from retaliatory strikes.

Beyond treaty adjustments, regulatory bodies must mandate technical safeguards to prevent unauthorized utilization of satellite terminals. The most effective mechanism is the enforcement of dynamic geofencing paired with cryptographic "whitelists." National regulators should require satellite operators to maintain real-time registries of authorized military terminals. Terminals operating outside these strict geographic bounds or failing to authenticate with authorized state entities must be automatically deactivated, preventing adversarial forces from weaponizing captured hardware.

VI. USEFUL LINKS

- https://www.journal.privietlab.org/index.php/PSSJ/article/view/715 (Oct 2025)
- https://www.idsa.in/system/files/jds/03_17-1-2023-Kaushik-Ray_William-Selvamurthy.pdf (2023)
- https://www.swp-berlin.org/publications/products/comments/2026C02_EuropeanAutonomy_in_Space_Web.pdf(Jan 2026)
- https://www.ejiltalk.org/starlink-and-international-law-the-challenge-of-corporate-sovereignty-in-outer-space/
- https://www.aljazeera.com/news/2026/2/10/how-does-the-cutoff-of-starlink-terminals-affect-russias-moves-in-ukraine
- https://oig.usaid.gov/node/7845 (Aug 2025)
- https://documents.un.org/doc/undoc/gen/g23/013/94/pdf/g2301394.pdf (Jan 2023)
- https://en.wikipedia.org/wiki/Starlink_in_the_Russo-Ukrainian_war