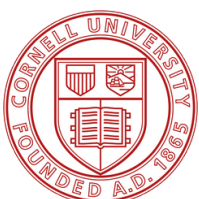




THE MILITARIZATION OF OUTER SPACE: LEGAL, ETHICAL AND STRATEGIC IMPLICATIONS OF COMMERCIAL INTERESTS

Harrison Mellor



Cornell Brooks Public Policy
Tech Policy Institute

EXECUTIVE SUMMARY

As governments grow increasingly dependent on commercial space systems for military advantage, private companies are thrust into an impossible bind: either enable one side and risk being seen as a belligerent or deny access and potentially alter the course of a war. This dilemma raises an important and difficult question. When commercial assets become legitimate military targets, does attacking them constitute an act of war?

Despite these pressing issues around commercial space assets, rules governing them are decades out of date. As private actors become operational gatekeepers in space warfare, a dangerous policy vacuum has emerged; no clear legal or institutional framework exists to guide their actions or assign responsibility. The line between commercial and military space has blurred.

It's time for international space policy to catch up.



BLURRING OF CIVILIAN AND MILITARY ROLES

Since the inception of spaceflight, space technology has been inherently dual-use.¹ The same rockets that place civilian communications satellites into orbit can be used to deliver ballistic ordnance. The same satellite navigation systems that guide a car through city streets can be used to guide a missile to its target. Historically, such technologies were developed, launched, and operated almost exclusively by states. Today, however, that paradigm is shifting. The rapid rise of private space ventures has introduced a new layer of complexity—operating with a growing level of independence, influence, and capability. Their platforms are no longer on the periphery of security strategy; they are becoming integrated, and sometimes indispensable, components of modern military operations.² The U.S. Department of Defense’s 2024 Commercial Space Integration Strategy directly acknowledges this shift, emphasizing that commercial providers are now being integrated into defense architectures across the full spectrum of conflict, and not simply as supplemental or peripheral services.³

SpaceX’s Starlink has become a defining example of this trend, as it has played a pivotal role in the conflict between Russia and Ukraine. Starlink terminals were deployed to maintain communications after conventional infrastructure was disrupted, enabling Ukrainian forces to coordinate battlefield movements, operate drones, and communicate securely across contested territory.⁴ Ukraine has become so dependent on this technology that the question of its continued access to the service has prompted significant concerns over the operational capability of their military forces.⁵

Earlier in the same conflict, at the outbreak of Russia’s 2022 invasion, communications network Viasat was crippled by a targeted cyberattack attributed to Russian military intelligence. This had an immediate impact on Ukraine’s ability to defend itself from incoming forces, but the effects were not limited to Ukraine’s military. Tens of thousands of users in other European countries faced weeks of internet outage as a result of the attack.⁶

These cases mark a profound shift not merely in the technology involved but in the locus of strategic authority. In previous decades, space-based assets remained largely under government control through direct ownership, contracting, or licensing. Today's commercial providers operate vast constellations at a global scale, often making service-level decisions on deployment, denial, or modification of their capabilities in real time. In moments of crisis, whether driven by commercial interest, ethical concern, or individual leadership discretion, these decisions can shape battlefield outcomes as decisively as state policy.

THE ORBITAL TROLLEY PROBLEM

As space commercial systems become a key part, and perhaps a target, of actual military conflict, the owners of these companies face a pressing ethical dilemma: continue to provide services at the risk of being complicit in military action or suspend services and potentially tip the conflict in the favor of the other side.

This is far from a hypothetical suggestion. In 2023, Elon Musk, owner of Starlink, reportedly restricted the service's availability near Crimea to prevent its use in a Ukrainian drone operation. His reasoning was that he didn't want Starlink to be involved in "a major act of war." But that decision, made by a private individual, may have directly altered the tactical environment on the battlefield.⁷ When Ukrainian officials voiced frustration, Musk argued that Starlink had never been activated in that region, and that turning it on would have constituted direct participation in hostilities. Whichever version is technically correct, the episode demonstrates an explicit awareness of the strategic dilemma by the actors themselves, and shows that a single corporate decision can enable or constrain military action in an environment without agreed rules to govern it.

Musk's position effectively reflects a belief that not pulling the proverbial lever is a form of neutrality.

Yet from Ukraine's perspective, withholding service was tantamount to choosing sides by denying a tool critical to their operations. This case underscores the ambiguity that arises when commercial actors operating dual-use infrastructure become entangled in war.

The strategic ambiguity grows even more acute when considering potential future conflicts involving other states, such as China. Unlike Russia, where economic and technological linkages to Western commercial actors are limited, China's deep integration into global supply chains, capital markets, and technology ecosystems would create far more complex dilemmas for commercial space providers. In a hypothetical Straits of Taiwan scenario, U.S.-based satellite operators might face simultaneous pressure from their home governments, shareholder interests, and global customer bases. Their decisions on whether to continue or suspend services to Taiwan could carry profound battlefield consequences while also risking severe economic retaliation from Beijing.⁸ This layered economic interdependence makes the question of commercial actor discretion not only a legal and ethical dilemma, but also a deeply strategic one, where space access could become a tool of indirect escalation or coercion. In this emerging reality, commercial operators cannot be treated as fully neutral bystanders when their systems exert operational influence in active conflicts. At the same time, commercial operators should neither be treated as combatants nor made to bear sole legal liability for the consequences of military uses of their services. Instead, responsibility must ultimately rest with states to establish clear legal and regulatory frameworks that define the obligations of private actors when operating in conflict zones. This includes transparency requirements, pre-agreed protocols for crisis decision-making, and coordinated oversight between governments and industry. Yet at present, a profound policy vacuum leaves these questions unresolved. Without such mechanisms, the power to shape battlefield outcomes will remain concentrated in private hands without the accountability structures appropriate to decisions of such magnitude.



REGULATORY AND LEGAL GAPS

International space law was built for a very different era; the Cold War was in full swing, the 'Space Race' was at its most intense, and states were the sole operators in space. The foundational treaties, such as the 1967 Outer Space Treaty and the 1972 Liability Convention, were designed to prevent the militarization of space between states, not to regulate the behavior or responsibilities of private actors operating dual-use systems in active war zones.⁹ In fact, the provisions of the treaty firmly establish that it is the responsibility of states to regulate activities in space.¹⁰ As commercial operators of space technology proliferate and act with increasing independence from state policy, these provisions look increasingly out of date.

Several questions remain unresolved in this area. For instance, should a private company be required to provide consistent service to all sides in a war to maintain neutrality? Should it be protected from retaliation by adversaries? Or does the very participation of such private space actors make it fair game as military targets?

Although no international treaty specifically covers commercial space actors in conflict, many experts argue that commercial assets supporting military operations are generally considered lawful military targets.^{11 12} This creates the disturbing possibility that dual-use satellites, even if primarily serving civilian functions and which may be providing critical, life-preserving services, could be lawfully attacked in war. Yet the danger to commercial satellites does not end here, since the destruction of any satellite in orbit can propagate risk to purely civilian satellites. If military powers begin targeting orbital assets with ordinance (something Russia has threatened),¹³ the risk of collisional cascading events—a chain reaction of debris capable of disabling wide swaths of orbital infrastructure—puts all space-based systems at risk.¹⁴

The ambiguity surrounding this issue is not only legal but strategic. As a recent report from CSIS states, U.S. and NATO signaling about consequences for attacks on satellites still lacks specific response thresholds, which weakens

deterrence and leaves commercial providers uncertain about the risks they face. If a U.S.-based satellite company is attacked, does that constitute an attack on the United States? Could it trigger collective defense obligations under NATO? These are not academic questions. The Viasat hack, conducted by Russian military intelligence on the eve of its invasion of Ukraine, was a direct cyberattack on a commercial satellite network. The consequences affected civilian users across Europe, yet, the event remains shrouded in ambiguity and the response to it has been inconsistent.

These legal ambiguities raise not only questions of targeting and protection but also of accountability. If commercial platforms actively enable military operations, should legal frameworks hold private companies directly accountable for the consequences? Existing treaties assign responsibility to states, but do not address the growing agency of private actors whose services can directly influence combat outcomes.

As commercial capabilities increasingly intersect with state military strategy, there is a growing argument for legal frameworks that define the obligations and duties of private providers in conflict scenarios. The current legal architecture offers no clear answers to these questions. In an age where billion-dollar space platforms are acting as the backbone of battlefield operations, this lack of clarity is not just a regulatory oversight, but also a strategic liability.

POLICY RECOMMENDATIONS: A SPACE COMMERCIAL SECURITY FRAMEWORK

To address the growing entanglement of commercial space assets in military operations, governments must develop a clear regulatory framework that defines the rights, responsibilities, and protections of private actors in space. In regulating this area, space policy should be updated to do three things:

1. CLARIFY LEGAL STATUS AND OBLIGATIONS

Commercial entities must be given clear guidance on what constitutes lawful conduct during conflict. This includes defining the point at which commercial services may become legitimate targets under the laws of armed conflict, as well as outlining obligations around neutrality, transparency, and notification when operating in or near a conflict zone. For the US, this includes coordinating with DHS/CISA to extend critical-infrastructure cybersecurity baselines, mission assurance planning, and contingency playbooks to space operators, with real-time information-sharing as a default during crises.

2. DEFINE ACCOUNTABILITY IN ESCALATION SCENARIOS

The U.S. and allies should publish clearer response frameworks for attacks on commercial satellites—specifying when responses are likely to be military vs. non-military. This is particularly complex for multinational corporations whose services may cross multiple legal jurisdictions and alliance frameworks. Clear accountability structures are needed to define state obligations for protecting commercial partners, assign liability in the event of hostile actions, and reduce ambiguity about whether and how such attacks constitute acts of war or trigger collective defense mechanisms.

3. ENCOURAGE INTERNATIONAL COORDINATION AND INDUSTRY PARTICIPATION

This framework should be developed in coordination with the international community, and it must actively include industry leaders in its formulation. Commercial operators have unique operational insights and risk profiles that should inform the regulatory architecture. To operationalize this, states could convene a multilateral working group under an existing body such as the UN Committee on the Peaceful Uses of Outer Space (COPUOS), or through a new dedicated forum focused specifically on dual-use commercial space governance.

If states remain committed to ensuring the peaceful use of outer space for future generations, action must be taken to preserve that commitment. Without clear rules, we are gambling with escalation, accountability, and the orbital infrastructure our world now depends on. The next conflict may not give us time to improvise.



SOURCES

- ¹ Falco, Gregory, Nicolo Boschetti and Ioannis Nikas. 2024. "Undercover Infrastructure Dual-Use Arctic Satellite Ground Stations." CIGI Papers No. 291 (April): 2.
https://www.cigionline.org/documents/2583/no.291_HM8ToWL.pdf
- ² Kim, Yool, et al. 2025. "Integrating Commercial Space Services into the DoD Architecture Understanding Operational and Policy Implications" Research Briefs – RAND Corporation.
https://www.rand.org/pubs/research_briefs/RBA2562-1.html
- ³ U.S. Department of Defense. "2024 Commercial Space Integration Strategy." Washington, D.C.: Office of the Secretary of Defense, April 2, 2024. <https://media.defense.gov/2024/Apr/02/2003427610/-1/-1/1/2024-DOD-COMMERCIAL-SPACE-INTEGRATION-STRATEGY.PDF>.
- ⁴ Pollet, Matthieu. 2025.
- ⁵ Barber, Harriet. 2025. "Elon Musk claims Ukraine front line will 'collapse' if Starlink is turned off." The Telegraph.
<https://www.telegraph.co.uk/world-news/2025/03/09/musk-ukranian-front-line-collapse-starlink-turned-off/>
- ⁶ Cyber Peace Institute. 2022. "Case Study: Viasat." <https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat>
- ⁷ Jordan, Dearbail. 2023. "Elon Musk says he withheld Starlink over Crimea to avoid escalation." <https://www.bbc.com/news/world-europe-66752264>
- ⁸ CSET, Which Ties Will Bind? Industry and Government in the Commercial Space Sector, July 2023.
<https://cset.georgetown.edu/wp-content/uploads/CSET-Which-Ties-Will-Bind.pdf>
- ⁹ Kilibarda, Pavle. 2017. "Space law revisited (3/3): The regime of international liability in space." <https://blogs.icrc.org/law-and-policy/2017/04/27/space-law-revisited-international-liability/>
- ¹⁰ Kopal, Vladimír. 2008. "Introductory Note." <https://legal.un.org/avl/ha/tos/tos.html>
- ¹¹ International Committee of the Red Cross. 2022. "Constraints under International Law on Military Operations in, or in Relation to, Outer Space during Armed Conflicts." 2. <https://www.icrc.org/en/document/constraints-under-international-law-military-space-operations>
- ¹² Kim, et al. 2025. "Operational and Policy Implications of Integrating Commercial Space Services into U.S. Department of Defense Operations" RAND Corporation. 64–65.
https://www.rand.org/pubs/research_reports/RRA2562-2.html
- ¹³ Tingley, Brett. 2022. "Russia says private satellites could become 'legitimate target' during wartime." <https://www.space.com/russia-private-satellites-legitimate-target-wartime-united-nations>
- ¹⁴ Kessler, Donald J. and Burton G. Cour-Palais. 1978. "Collision Frequency of Artificial Satellites: The Creation of a Debris Belt" Journal of Geophysical Research 83 (A6) 2637–2646. <https://doi.org/10.1029/JA083iA06p02637>

Harrison Mellor graduated with a Masters of Arts in International Relations at Durham University and Bachelors of Arts (Honors) in War and Security Studies at the University of Hull. His research primarily focuses on global space governance and security.

The article is intended for information and educational purposes only. The views and opinions expressed herein are those of the author and do not necessarily reflect the official policy or position of any institution or organization. While every effort has been made to ensure the accuracy and reliability of the information provided, the author and publisher make no representations or warranties, express or implied, regarding the completeness, correctness, or applicability of the content. The information contained in this document should not be construed as advice. Readers are encouraged to conduct their own research and seek appropriate guidance before making any decisions based on the material presented. The author and publisher disclaim any liability for any direct, indirect, or consequential damages arising from the use or reliance on this report/article. By accessing and using this document, the reader acknowledges and agrees to the terms of this disclaimer.