Leiden & McGill Academic Workshop on Air & Space Law 2026

Regulating Orbital Electronic Warfare and Signal Intelligence under United Kingdom and International Law

DRAFT

by Alexander Wallace Watson

Keywords: electronic warfare (EW), stalker satellites, UK Space Industry Act 2018, Article IX OST, SIGINT

Abstract:

Counter-space warfare has shifted from direct-ascent kinetic strikes toward non-kinetic, sub-threshold operations in the electromagnetic spectrum. Spacefaring powers deploy co-orbital "stalker satellites" executing Rendezvous and Proximity Operations (RPOs) to intercept, degrade, or disrupt critical space assets while maintaining plausible deniability. Existing international legal frameworks including Article IX of the Outer Space Treaty, Article 45 of the International Telecommunication Union Constitution, and the Tallinn Manual 2.0, suffer from normative ambiguity, steep evidential burdens, and a lack of enforcement mechanisms to address low-power electronic warfare.

To overcome this international paralysis, the United Kingdom can leverage its domestic regulatory and financial capabilities to enforce orbital resilience. The UK Civil Aviation Authority should mandate hardware-level electromagnetic hardening, integrate GCHQ signals intelligence into licensing via encrypted telemetry escrow, and establish a statutory "Trusted Operator" status alongside objective parameters for harmful interference. By conditioning access to London's space insurance and capital markets on these standards, the UK can export a market-enforced regulatory model across Five Eyes, AUKUS Pillar II, and NATO, creating an enforceable baseline for global space domain defence.

Introduction 4
International Law 4
Outer Space Treaty 1967 4
ITU Constitution 5
Tallinn Manual 2.0 5
UK Regulation 6
Opportunities for International Collaboration 6
Background 7
Active Electronically Scanned Arrays (AESAs) 7
Cognitive Software-Defined Radios (SDRs) 7
Low-power Telemetry Spoofing or Sensor Blinding 8
Attribution Gap 8
Stalker Satellite Activity 9
International Space Law 12
The Outer Space Treaty 1967 12
The Due Regard Standard 13
Evidential Burden and LPI Signals 13
Absence of Enforcement Mechanisms 14
The ITU Regime 15
Article 45 of the ITU Constitution 15
The Priority Rule & Master International Frequency Register (MIFR) 15
Technical Degradation vs Intent 15
Administrative Record of the Radio Regulations Board (RRB) 16
The ITU Enforcement Deficit 16
The Tallinn Manual 2.0 18
Use of Force 18
Armed Attack 19
Sovereignty Violations 20
UN COPUOS Guidelines on the Long-Term Sustainability of Outer Space Activities 22
Diplomatic Consensus 22
UK Regulations 23
Hardware Resilience Mandates 23
Automated Telemetry Escrow and Intelligence Pipelines 24
Trusted Operator Status and Legal Defensibility 26
Statutory Definition of "Harmful Interference" under English Law 27
Market Access and Insurance Enforcement 28
International Collaboration 29
UK Regulatory Leadership 29
Allied Security Frameworks 30
Outer Space Treaty Annex 30
Conclusion 31

Glossary of Terms and Abbreviations

AESA — Active Electronically Scanned Array

ASAT — Anti-Satellite (weapons or operations)

BER — Bit-Error-Rate

CAA — Civil Aviation Authority (United Kingdom)

DSSS — Direct Sequence Spread Spectrum

EW — Electronic Warfare

FHSS — Frequency Hopping Spread Spectrum

GCHQ — Government Communications Headquarters (United Kingdom)

GEO — Geostationary Earth Orbit

GNSS — Global Navigation Satellite System

Grey Zone — Operational space below the threshold of traditional armed conflict or an armed attack, characterized by sub-threshold, non-kinetic, or deniable adversarial actions

ITU — International Telecommunication Union

Jus ad Bellum — The legal principles governing the right of states to resort to armed force (*UN Charter*, art 2(4), 51)

Jus in Bello — International humanitarian law governing the conduct of parties during an armed conflict

Kinetic — Operations or weapons relying on physical force, momentum, or explosive energy to cause direct structural damage or destruction

LTS — Guidelines for the Long-Term Sustainability of Outer Space Activities (UN COPUOS)

MIFR — Master International Frequency Register (ITU)

NATO — North Atlantic Treaty Organization

OST — *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, 27 January 1967, 610 UNTS 205 (entered into force 10 October 1967) [Outer Space Treaty]

RF — Radio Frequency

RNSS — Radio Navigation Satellite Service

RPO — Rendezvous and Proximity Operations

RRB — Radio Regulations Board (ITU)

SAR — Synthetic Aperture Radar

SDA — Space Domain Awareness

SDR — Software-Defined Radio

SIA — Space Industry Act 2018 (United Kingdom)

SIGINT — Signals Intelligence

SIR — Space Industry Regulations 2021 (United Kingdom)

SSA — Space Situational Awareness

T/R — Transmit/Receive (modules)

UK — United Kingdom

UN — United Nations

Introduction

The strategic paradigm of counter-space warfare has undergone a structural transformation. Direct-ascent kinetic Anti-Satellite (ASAT) weapons were historically the primary vector for orbital neutralization, but are increasingly obsolete in statecraft. While kinetic strikes yield physical destruction, they generate orbital debris, trigger immediate attribution, and constitute an unambiguous jus ad bellum trigger under Article 51 of the United Nations Charter. Consequently, spacefaring adversaries have shifted operational emphasis toward non-kinetic, sub-threshold "grey-zone" capabilities. These offensive operations weaponize the electromagnetic spectrum and cyber-physical interfaces to degrade, intercept, and corrupt orbital assets without inflicting permanent physical destruction.

Central to this shift is the deployment of "stalker satellites", which are spacecraft designed to conduct Rendezvous and Proximity Operations (RPOs). These satellites deliberately manoeuvre into close physical proximity (spanning kilometres to mere metres) with high-value military, intelligence, or commercial satellites. By co-orbiting alongside target assets, stalker satellites secure continuous access to their target's transmission beam while evading detection and maintaining plausible deniability.

This operational model is well-documented across multiple orbital regimes. In Geostationary Earth Orbit (GEO), Russian Luch/Olymp-K (and its successor Luch-2) spacecraft have engaged in systematic shadow operations since 2014. These platforms have parked directly adjacent to Western military and commercial communication nodes, including Intelsat 37E (approached to within 4 km in 2022), Franco-Italian Athena-Fidus, and the UK's Skynet 4E array. In Low Earth Orbit (LEO), Russia deployed six Kosmos platforms (Kosmos-2609 through 2614) to shadow the Finnish ICEYE commercial Synthetic Aperture Radar (SAR) constellation. Operating at proximity distances as close as 13 km, these stalkers can intercept raw SAR imagery downlinks or project localized radio frequency (RF) disruption to blind radar sensors providing tactical intelligence to Ukrainian forces[1].

International Law

Outer Space Treaty 1967

Article I of the Outer Space Treaty (OST) 1967 guarantees outer space as free for exploration and use by all states. Major space powers invoke Article I to argue that co-orbital proximity operations constitute a lawful exercise of orbital freedom. Conversely, Article IX obligates

[1] CSIS, Space Threat Assessment 2023, by Makena Young & Kaitlyn Johnson (Washington, DC: Center for Strategic and International Studies, 2023) at 12–16; Secure World Foundation, Global Counterspace Capabilities: An Open Source Assessment, ed by Brian Weeden & Victoria Samson (Washington, DC: Secure World Foundation, 2024) at 2-15–2-22; US, Space Force, Competition in Space (Washington, DC: United States Space Force, 2024) at 8–11; Slava Khlebnikov & Victoria Samson, "Shadowing in GEO: Operational Patterns of the Luch/Olymp Series" (2023) 39:2 Space Policy 101542 at 3–7; European Union Institute for Security Studies, Rendezvous and Proximity Operations in LEO: The Kosmos-2609–2614 Campaign against Commercial SAR, EUISS Brief No 14 (Paris: EUISS, 2024) at 2–5.

states to conduct space activities with "due regard to the corresponding interests of other States" and to undertake international consultations if an activity causes "harmful interference". However, the OST fails to define quantitative distance thresholds for RPOs or technical parameters for "harmful" emissions. Moreover, proving deliberate breach of "due regard" becomes an almost impossible evidentiary hurdle given that stalker satellite signals often operate below the cosmic noise floor.

ITU Constitution

Article 45 of the International Telecommunication Union (ITU) Constitution strictly prohibits member states from causing "harmful interference" to registered radio services. Unlike general international law, the ITU regime focuses on objective technical signal degradation rather than political intent. However, recent administrative practice demonstrates that the ITU lacks enforcement power. Despite formal reports and directives issued by the Radio Regulations Board (RRB) regarding widespread Global Navigation Satellite System (GNSS) jamming in the Baltic Sea and Middle East (2024–2025), offending states routinely ignore RRB warnings, exposing the structural enforcement deficit of international telecommunications law[2].

Tallinn Manual 2.0

The *Tallinn Manual 2.0* provides an influential, but non-binding, expert framework for assessing how existing international law applies to cyber operations. Its relevance to stalker-satellite operations is necessarily limited, however, because electromagnetic interference is not necessarily a cyber operation. Rule 69 addresses the prohibition on the use of force under Article 2(4) of the United Nations Charter, while Rule 71 addresses the higher threshold of an armed attack for the purposes of Article 51. The Manual adopts a contextual, effects-based approach in which the scale, severity, immediacy, directness, invasiveness, and military character of an operation are relevant to determining whether the applicable threshold has been crossed.[3]

However, an adversary may be able to generate strategically significant disruption without producing the physical destruction traditionally associated with an armed attack, leaving the victim State to confront substantial operational harm while facing uncertainty over the legal basis for any kinetic response. The *Tallinn Manual* therefore illustrates, rather than resolves, the difficulty of applying existing jus ad bellum thresholds to technologically advanced counter-space operations.

---

[2] Dale Stephens, "The Regulation of Electronic Warfare in Outer Space" (2021) 97 Intl L Stud 81 at 98–101; Francis Lyall & Paul B Larsen, Space Law: A Authority and Interpretive Guide, 2nd ed (London: Routledge, 2018) at 234–238.

[3] Michael N Schmitt, ed, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2d ed (Cambridge University Press, 2017) at 330–43 (Rules 69, 71 and accompanying commentary); Charter of the United Nations, 26 June 1945, Can TS 1945 No 7, arts 2(4), 51.; Charter of the United Nations, 26 June 1945, Can TS 1945 No 7, art 2(4), 51; Dale Stephens, "The Regulation of Electronic Warfare in Outer Space" (2021) 97 Intl L Stud 81 at 94–98; CSIS, Space Threat Assessment 2023, by Makena Young & Kaitlyn Johnson (Washington, DC: Center for Strategic and International Studies, 2023) at 9–12.

In any case, sovereign space actors cannot assume international law will be observed by adversaries in the contested legal and geopolitical environments.

UK Regulation

Given the deadlock in international norm-setting, states must leverage domestic regulatory frameworks as proactive instruments of national security. Rather than treating orbital licensing as a passive administrative formality, the UK can leverage access to its space assets and infrastructure, insurance underwriting, and financial markets to enforce operational resilience across orbital activity. To execute this effectively, domestic regulation should be refocused around three core pillars: rigorously vetted hardware and supply chains, active intelligence integration, and market enforcement.

First, the Civil Aviation Authority (CAA) must shift from auditing paper policies to conducting mandatory, hardware-level technical assessments. License approvals should be strictly conditioned on verified anti-jamming architectures alongside rigorous scrutiny of foreign component supply chains to prevent embedded vulnerabilities.

Second, licensing must formalize a direct statutory link between the CAA and Government Communications Headquarters (GCHQ). By embedding GCHQ's signals intelligence (SIGINT) and electronic warfare (EW) capabilities directly into the regulatory lifecycle, the state establishes an active monitoring regime to track real-time spectrum anomalies, assess dynamic orbital threats, and co-develop immediate contingency protocols for licensed operators facing active interference.

Third, the UK can enforce compliance globally by leveraging London's dominance in space insurance and capital markets. By codifying GCHQ-verified resilience criteria into baseline underwriting conditions and statutory liability limits under the Space Industry (Indemnities) Act 2025, non-compliant operators will face prohibitive risk premiums or total market exclusion, incentivizing commercial operators to adopt UK resilience standards as the default global benchmark.

Opportunities for International Collaboration

Universal consensus on space-based electronic warfare within the UN remains politically unachievable due to adversary vetoes. Therefore, as an alternative way to achieve an international law based consensus, the UK should export its domestic technical-sovereign licensing model to common transatlantic security structures. By aligning regulatory frameworks across Five Eyes, AUKUS Pillar II, and NATO, allied nations can establish a plurilateral "technical annex" to the Outer Space Treaty. Unifying Western market share around these hardware standards will establish the UK model as the global default for space domain defence.

Background

The effective operation of stalker satellites depends on three advanced architectural components: active electronically scanned arrays, software-defined radios, and low-power telemetry.

Active Electronically Scanned Arrays (AESAs)

Active electronically scanned arrays (AESAs) are distinct from traditional mechanical dish antennas that rely on physical motors to steer beams and inadvertently expose target selection to optical tracking telescopes. Instead, AESAs comprise hundreds of solid-state transmit/receive (T/R) modules operating under the control of a central beamforming computer. Integrated digital phase shifters delay or advance released radio waves across microsecond intervals, enabling instantaneous, directional beam-steering and spatial "nulling" without mechanical movement, which effectively conceals operational intent from ground-based space domain awareness (SDA) networks.[4]

Traditional SDA networks rely heavily on ground-based optical telescopes to detect physical satellite reorientations. Stalker satellites equipped with AESAs steer their transmission beams electronically via digital phase shifters in microseconds. Because the spacecraft does not physically rotate or alter its orientation to target an asset, ground-based tracking systems register no visible change in attitude or operational intent.[5]

Cognitive Software-Defined Radios (SDRs)

To execute covert SIGINT and electronic warfare, these arrays pair with cognitive software-defined radios driven by real-time machine-learning algorithms that analyze target radio frequency environments. These systems utilize direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS) architectures to spread transmission energy across wide bandwidths. This technique drops the signal's power spectral density below the cosmic background noise floor, causing covert emissions to mirror thermal static or cosmic radiation to standard ground-based receivers.[6]

---

[4] Merrill I Skolnik, Radar Handbook, 3rd ed (New York: McGraw-Hill, 2008) at 13.1–13.14; Eli Brookner, "Phased-Array Radars" (2002) 111:1 IEEE Spectrum 42 at 43–46; Richard A Poisel, Electronic Warfare Target Location Pages (Boston: Artech House, 2012) at 89–94; CSIS, Space Threat Assessment 2023, by Makena Young & Kaitlyn Johnson (Washington, DC: Center for Strategic and International Studies, 2023) at 8–10.
[5] David L Wright, Laura Grego & Cameron Wright, The Physics of Space Security: A Reference Manual (Cambridge, Mass: American Academy of Arts and Sciences, 2005) at 112–116; Secure World Foundation, Global Counterspace Capabilities: An Open Source Assessment, ed by Brian Weeden & Victoria Samson (Washington, DC: Secure World Foundation, 2024) at 1-12–1-15; Dale Stephens, "The Regulation of Electronic Warfare in Outer Space" (2021) 97 Intl L Stud 81 at 86–89.
[6] Bruce A Fette, ed, Cognitive Radio Technology, 2nd ed (Burlington, Mass: Academic Press, 2009) at 145–152; Don Torrieri, Principles of Spread-Spectrum Communication Systems, 4th ed (Cham, Switzerland: Springer, 2018) at 45–58; Richard A Poisel, Modern Communications Jamming Principles and Techniques, 2nd ed

By employing cognitive SDRs alongside DSSS and FHSS techniques, non-kinetic operations distribute transmission energy across broad frequency bandwidths. This reduces the signal's power spectral density below the natural cosmic background noise floor, making malicious communications or electronic warfare signals appear to terrestrial receivers as harmless thermal static or cosmic radiation.[7]

Low-power Telemetry Spoofing or Sensor Blinding

Furthermore, rather than deploying high-power, brute-force jamming that invites rapid detection, stalker satellites employ low-power telemetry spoofing and localized sensor blinding. By matching target frequencies and geometry, a nearby stalker satellite can execute subtle data packet injections that introduce minute bit-error-rate (BER) spikes, corrupt command downlinks, or force subsystem reboots while evading standard detection protocols.[8]

Instead of high-power jamming that triggers immediate threat alerts, stalker satellites utilize low-power telemetry spoofing, targeted BER spikes, and localized sensor blinding. Because these interventions induce subtle subsystem reboots or corrupted data packets, space asset operators cannot easily distinguish between a targeted adversary action and routine operational anomalies, such as radiation-induced single-event upsets, solar weather, or component degradation.[9]

Attribution Gap

The combined use of these technologies enables hostile actors to conduct adversarial operations which remain below the threshold of clear detection and identification. Effective deterrence relies on the credible capability to identify an aggressor and retaliate proportionally. When non-kinetic grey-zone attacks obscure the identity and intent of the perpetrator, the target nation cannot confidently name the adversary. This allows adversaries to continuously degrade critical space assets with relative impunity, eroding the target's strategic advantage without risking direct escalation.

(Artech House, 2011) at 211–218; CSIS, Space Threat Assessment 2023, by Makena Young & Kaitlyn Johnson (Washington, DC: Center for Strategic and International Studies, 2023) at 9–11.

[7] John G Proakis & Masoud Salehi, Digital Communications, 5th ed (New York: McGraw-Hill, 2008) at 710–718; Dale Stephens, "The Regulation of Electronic Warfare in Outer Space" (2021) 97 Intl L Stud 81 at 94–97; Secure World Foundation, Global Counterspace Capabilities: An Open Source Assessment, ed by Brian Weeden & Victoria Samson (Washington, DC: Secure World Foundation, 2024) at 1-14–1-16.

[8] Richard A Poisel, Modern Communications Jamming Principles and Techniques, 2nd ed (Boston: Artech House, 2011) at 235–242; CSIS, Space Threat Assessment 2023, by Makena Young & Kaitlyn Johnson (Washington, DC: Center for Strategic and International Studies, 2023) at 9–12; Dale Stephens, "The Regulation of Electronic Warfare in Outer Space" (2021) 97 Intl L Stud 81 at 91–95.

[9] Secure World Foundation, Global Counterspace Capabilities: An Open Source Assessment, ed by Brian Weeden & Victoria Samson (Washington, DC: Secure World Foundation, 2024) at 1-14–1-17; David L Wright, Laura Grego & Cameron Wright, The Physics of Space Security: A Reference Manual (Cambridge, Mass: American Academy of Arts and Sciences, 2005) at 118–122; Thomas Rid & Ben Buchanan, "Attributing Cyber Attacks" (2015) 38:1 J Strategic Studies 4 at 10–14.

International frameworks governing warfare, such as Article 51 of the UN Charter, rely on a clear jus ad bellum trigger (an unambiguous armed attack) to justify self-defence or collective defence responses. Sub-threshold operations exploit this framework by causing operational disruption rather than physical destruction. Without definitive proof of deliberate state-sponsored hostility, decision-makers face legal and political paralysis, unable to justify retaliatory measures or escalate to diplomatic or military responses.

In orbit, response time is critical. When a satellite experiences subtle sensor blinding or packet corruption, operators must first rule out internal hardware faults or environmental interference before identifying an external threat. This diagnostic lag delays defensive manoeuvres, payload reconfigurations, or offensive countermeasures, allowing the stalker satellite extended windows of time to intercept data or corrupt telemetry unhindered.[10]

Stalker Satellite Activity

The strategic objective of RPOs has evolved over the past two decades, transitioning from experimental inspections to active signals exploitation, intentional harassment, and physical intervention.

The functional shift toward active, unannounced orbital maneuvering began in 2006, when the United States validated close-proximity capability in deep space (*MiTEx*). By deploying twin micro-satellites alongside a disabled defence communications asset, the operation proved that small platforms could dynamically approach and evaluate high-value targets, establishing a template for unannounced close-range surveillance.[11]

Between 2009 and 2014, the core purpose of proximity maneuvers expanded from visual inspection to signal exploitation and communications collection. The United States deployed specialized intelligence platforms (*PAN / USA-207* and *CLIO / USA-257*) that systematically drifted across geostationary orbit, stopping directly adjacent to commercial and military communications relay slots. Russia adopted this operational model shortly thereafter (*Luch / Olymp-K*), maneuvering near European military relays. Rather than physically damaging target hardware, these platforms were positioned to intercept directional downlinks, monitor signal traffic, and collect signals intelligence without triggering threat thresholds.[12]

---

[10] Secure World Foundation, Global Counterspace Capabilities: An Open Source Assessment, ed by Brian Weeden & Victoria Samson (Washington, DC: Secure World Foundation, 2024) at 1-14–1-18; CSIS, Space Threat Assessment 2023, by Makena Young & Kaitlyn Johnson (Washington, DC: Center for Strategic and International Studies, 2023) at 9–12; Dale Stephens, "The Regulation of Electronic Warfare in Outer Space" (2021) 97 Intl L Stud 81 at 91–96; Thomas Rid & Ben Buchanan, "Attributing Cyber Attacks" (2015) 38:1 J Strategic Studies 4 at 12–16.

[11] Secure World Foundation, Global Counterspace Capabilities: An Open Source Assessment, ed by Brian Weeden & Victoria Samson (Washington, DC: Secure World Foundation, 2024) at 1-8–1-11; CSIS, Space Threat Assessment 2021, by Todd Harrison et al (Washington, DC: Center for Strategic and International Studies, 2021) at 12–14; Defense Intelligence Agency, Challenges to Security in Space: Space Reliance in an Era of Competition and Expansion (Washington, DC: DIA, 2022) at 18.

[12] Slava Khlebnikov & Victoria Samson, "Shadowing in GEO: Operational Patterns of the Luch/Olymp Series" (2023) 39:2 Space Policy 101542 at 3–8; Secure World Foundation, Global Counterspace Capabilities: An Open Source Assessment, ed by Brian Weeden & Victoria Samson (Washington, DC: Secure World Foundation, 2024)

By 2014, major spacefaring states formalized dedicated, continuous patrol architectures. The United States launched a specialized inspection fleet (*GSSAP*) into near-synchronous paths to conduct ongoing neighborhood watch, mapping adversary assets and assessing payload configurations. Concurrently, Russia tested co-orbital sub-satellite release capabilities (*Cosmos 2504* and *Cosmos 2519/2521*). These operations demonstrated a dual-use threat: a parent spacecraft could deploy smaller sub-satellites capable of covert tracking, electronic interference, or kinetic intercept.[13]

From 2018 onward, operations increasingly focused on operational disruption, surveillance degradation, and coercive posture. Russian inspection platforms (*Cosmos 2542 / Cosmos 2543*) shadowed a classified US optical reconnaissance satellite (*USA 245*), executing synchronized close-approach maneuvers to degrade its operational opacity, create persistent collision hazards, and test target defensive reactions. China similarly expanded its high-thrust maneuvering operations (*Shijian-20*), demonstrating rapid repositioning across the geostationary belt.[14]

The functional threat model reached a new benchmark in 2021 with the operational validation of physical grappling capabilities. China deployed a specialized space debris mitigation platform (*Shijian-21*) that physically docked with a defunct navigation satellite (*Beidou-2 G2*), towed it into a graveyard orbit, and returned to service. While aligned with commercial life-extension and debris removal paradigms (*MEV-1 / MEV-2*), the dual-use capability to physically capture, alter the trajectory of, or disable an orbital asset provides a direct mechanism to neutralize adversary spacecraft without generating collateral debris.[15]

Recent deployments demonstrate the ongoing operationalization of these tactics across both low Earth and highly elliptical regimes. In May 2026, Russia launched a cluster of military spacecraft (*Cosmos 2610–2614 batch*), several of which executed high-energy orbital plane adjustments to match the inclination of a commercial synthetic aperture radar asset supporting Ukrainian targeting (*ICEYE-X36*), closing to within 13 kilometers. This demonstrated an intent to monitor, inspect, or degrade commercial infrastructure critical to

---

at 1-12, 2-18–2-21; US, Space Force, Competition in Space (Washington, DC: United States Space Force, 2024) at 8–10.

[13] US, Space Force, GSSAP Program and Neighborhood Watch Operations, Fact Sheet (Washington, DC: US Space Force, 2022); CSIS, Space Threat Assessment 2022, by Makena Young & Todd Harrison (Washington, DC: Center for Strategic and International Studies, 2022) at 14–18; Secure World Foundation, Global Counterspace Capabilities: An Open Source Assessment, ed by Brian Weeden & Victoria Samson (Washington, DC: Secure World Foundation, 2024) at 2-14–2-17.

[14] US, Department of State, "Shadowing of USA 245 by Kosmos 2542 and 2543" (Press Statement delivered at the Conference on Disarmament, Geneva, 25 February 2020); Joseph Trevithick, “A Russian ‘Inspector’ Spacecraft Now Appears To Be Shadowing An American Spy Satellite” The War Zone (4 February 2020), online: The War Zone; CSIS, Space Threat Assessment 2021, by Todd Harrison et al (Washington, DC: Center for Strategic and International Studies, 2021) at 15–19; Secure World Foundation, Global Counterspace Capabilities: An Open Source Assessment, ed by Brian Weeden & Victoria Samson (Washington, DC: Secure World Foundation, 2024) at 1-15, 2-20.

[15] Secure World Foundation, Global Counterspace Capabilities: An Open Source Assessment, ed by Brian Weeden & Victoria Samson (Washington, DC: Secure World Foundation, 2024) at 1-16–1-19; CSIS, Space Threat Assessment 2023, by Makena Young & Kaitlyn Johnson (Washington, DC: Center for Strategic and International Studies, 2023) at 6–8; US, Space Force, Competition in Space (Washington, DC: United States Space Force, 2024) at 11–13.

military operations. Simultaneously, adversary capabilities have expanded into systemic threat ambiguity and domain exploitation.[16]

Recent Chinese operations leverage non-standard orbital mechanics, unannounced sub-satellite deployments (*Shijian-29A / SJ-29B*), and coordinated co-planar convergences (*TJS-10 / TJS-3*) to deliberately obscure operational intent and bypass SDA tracking networks. This trend culminated in the deployment of a specialized surveillance platform into a highly elliptical Molniya orbit (*Shijian-31 / SJ-31*), which systematically drifts across the geostationary belt every 23 days from an asymmetric, high-altitude vantage point. By positioning payloads thousands of kilometres above traditional inspection slots, these platforms execute persistent observation and signals intelligence collection while remaining outside standard ground-based detection thresholds.[17]

[16] European Union Institute for Security Studies, Rendezvous and Proximity Operations in LEO: The Kosmos-2610–2614 Campaign against Commercial SAR, EUISS Brief No 14 (Paris: EUISS, 2026) at 2–5; CSIS, Space Threat Assessment 2024, by Kari A Bingen et al (Washington, DC: Center for Strategic and International Studies, 2024) at 14–17; Secure World Foundation, Global Counterspace Capabilities: An Open Source Assessment, ed by Brian Weeden & Victoria Samson (Washington, DC: Secure World Foundation, 2024) at 2-21–2-25.

[17] US, Space Force, Competition in Space (Washington, DC: United States Space Force, 2024) at 12–15; Secure World Foundation, Global Counterspace Capabilities: An Open Source Assessment, ed by Brian Weeden & Victoria Samson (Washington, DC: Secure World Foundation, 2024) at 1-18–1-22; Defense Intelligence Agency, Challenges to Security in Space: Space Reliance in an Era of Competition and Expansion (Washington, DC: DIA, 2022) at 22–25.

International Space Law

The governance of outer space operates within a complex international regime, composed primarily of treaty law, international telecommunications frameworks, and customary legal principles. Despite the growing paralysis of multilateral institutions, states and commercial operators remain deeply invested in demonstrating technical and regulatory compliance with these international instruments. This persistence is driven by critical commercial and strategic imperatives: maintaining insurable assets, satisfying statutory conditions for national launch and operation licences, avoiding international liability claims, and preserving sovereign legitimacy on the global stage.[18]

However, as counter-space capabilities transition toward sub-threshold, non-kinetic grey-zone warfare, public international space law has proven structurally incapacitated. Existing international frameworks suffer from severe normative vagueness, unworkable evidentiary burdens, and an absolute absence of enforcement or coercive deterrence mechanisms. Consequently, current international space law is fundamentally incapable of preventing or penalising state-sponsored orbital aggression.[19]

The Outer Space Treaty 1967

The fundamental governance architecture of public international space law rests upon a structural tension embedded within the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (Outer Space Treaty or OST)[20]. Article I of the OST establishes the foundational principle that outer space "shall be free for exploration and use by all States without discrimination of any kind".[21]

In grey-zone counter-space operations, adversary states exploit this broad guarantee to justify aggressive RPOs. Operating under the rubric of orbital freedom, an adversary stalker satellite can manoeuvre to within a just few metres of a sovereign or commercial payload without

---

[18] Francis Lyall & Paul B Larsen, *Space Law: A Authority and Interpretive Guide*, 2nd ed (London: Routledge, 2018) at 53–78; PJ Blount, *Repressing Aggression in Outer Space: The Law of International Space Security* (Cheltenham: Edward Elgar Publishing, 2021) at 112–128.
[19] Michael N Schmitt, ed, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed (Cambridge: Cambridge University Press, 2017) r 14, 69, 71; Dale Stephens, "The Regulation of Electronic Warfare in Outer Space" (2021) 97 Intl L Stud 81 at 94–101; CSIS, *Space Threat Assessment 2023*, by Makena Young & Kaitlyn Johnson (Washington, DC: Center for Strategic and International Studies, 2023) at 9–12; Cassandra Steer, "Space Security and the Challenge of Grey-Zone Conflict" in Cassandra Steer & Matthew Hersch, eds, *War and Peace in Space: Law, Policy, and Ethics* (Oxford: Oxford University Press, 2021) 145 at 152–160.
[20] *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, 27 January 1967, 610 UNTS 205 (entered into force 10 October 1967) [*Outer Space Treaty*].
[21] *Ibid*, art I.

committing an overt territorial trespass. Because international law recognises no upper vertical limit to terrestrial airspace sovereignty, adversaries assert that non-destructive co-orbital shadow operations are a lawful exercise of Article I rights.

This absolute assertion of orbital freedom directly clashes with the restrictive covenants of Article IX.[22] Article IX requires States Parties to conduct all activities in outer space "with due regard to the corresponding interests of all other States Parties" and mandates international consultations before proceeding with any activity or experiment that "would cause potentially harmful interference with activities of other States Parties".[23]

The Due Regard Standard

The primary legal inadequacy of Article IX lies in the normative vagueness of the "due regard" standard. Public international law has failed to codify precise legal, spatial, or operational parameters for what constitutes "due regard" in orbit. Unlike maritime law, which relies on the Convention on the International Regulations for Preventing Collisions at Sea (COLREGs) to establish clear distance thresholds and give-way rules,[24] space law possesses no binding instrument defining unsafe proximity thresholds or operational keep-out zones for RPOs.

Without codified safety corridors or quantitative metrics, an affected state cannot easily demonstrate that mere physical proximity constitutes a prima facie breach of "due regard" or an act of "harmful interference". Adversaries regularly defend stalker satellite positioning as routine space situational awareness, scientific calibration, or orbital debris avoidance, exploiting the subjective nature of Article IX to obscure hostile intent.[25]

Evidential Burden and LPI Signals

Even where an operation causes observable performance degradation, Article IX places a practically unworkable evidentiary burden on the victim state. To trigger the mandatory consultation mechanism under Article IX, the target state must establish that an adversary's activity is the direct cause of "potentially harmful interference".[26]

When applied to electronic warfare and signals intelligence, this threshold creates an insurmountable evidential vacuum. Because the victim state cannot isolate or prove the

---

[22] *Ibid*, art IX.
[23] *Ibid*.
[24] *Convention on the International Regulations for Preventing Collisions at Sea*, 20 October 1972, 1050 UNTS 16 (entered into force 15 July 1977).
[25] Dale Stephens, "The Regulation of Electronic Warfare in Outer Space" (2021) 97 Intl L Stud 81 at 88–92; Cassandra Steer, "Space Security and the Challenge of Grey-Zone Conflict" in Cassandra Steer & Matthew Hersch, eds, *War and Peace in Space: Law, Policy, and Ethics* (Oxford: Oxford University Press, 2021) 145 at 154–158; CSIS, *Space Threat Assessment 2023*, by Makena Young & Kaitlyn Johnson (Washington, DC: Center for Strategic and International Studies, 2023) at 9–12.
[26] *Outer Space Treaty*, *supra* note 1, art IX.

existence of a covert RF emission beneath the noise floor, it cannot meet the standard of proof required to invoke formal consultations under Article IX.

Absence of Enforcement Mechanisms

Article IX provides no compulsory judicial dispute resolution body, injunctive remedies, or punitive sanctions. If a state requests consultations regarding suspected orbital interference, the receiving state faces no treaty-based timeline or enforcement mechanism forcing compliance. An adversary can delay, deny, or dismiss consultation requests with complete legal impunity, leaving the target state without a binding international legal forum to halt ongoing non-kinetic aggression.

The ITU Regime

Article 45 of the ITU Constitution

While public international space law struggles with normative ambiguity, the international telecommunications framework offers a distinct, parameter-based legal regime. The Constitution of the International Telecommunication Union (ITU Constitution) establishes an explicit prohibition against operational RF disruption.[27] Article 45(1) mandates that "[a]ll stations, whatever their purpose, must be established and operated in such a manner as not to cause harmful interference to the radio services or communications of other Member States".[28]

Under the ITU Radio Regulations, "harmful interference" is defined as interference that "endangers the functioning of a radionavigation service or of other safety services or seriously degrades, obstructs or repeatedly interrupts a radiocommunication service operating in accordance with the Radio Regulations".[29]

The Priority Rule & Master International Frequency Register (MIFR)

The legal protection enforced by the ITU relies on the Master International Frequency Register (MIFR), administered by the Radiocommunication Bureau.[30] Under the ITU framework, international rights and protection against harmful interference accrue through the "first-come, first-served" priority rule.[31] Once an administration completes formal coordination and secures a priority recording in the MIFR, its orbital frequency assignments enjoy formal international recognition and protection.[32]

If a UK satellite operates on an MIFR-registered frequency assignment, and an adversary stalker satellite shadow-orbits the target while emitting on identical or adjacent channels, a prima facie technical violation of Article 45 occurs immediately upon signal degradation.

Technical Degradation vs Intent

The primary analytical strength of the ITU framework lies in its objective assessment model. Unlike general customary international law, which often requires victim states to demonstrate an adversary's mens rea, state sponsorship, or political coercion, the ITU regime evaluates operational breaches strictly through physical parameters. A violation is established by

---

[27] *Constitution of the International Telecommunication Union*, 22 December 1992, 1825 UNTS 331 (entered into force 1 July 1994) [*ITU Constitution*].
[28] *Ibid*, art 45(1).
[29] ITU, *Radio Regulations*, 2024 ed (Geneva: ITU, 2024) vol 1, art 1.169.
[30] *Ibid*, vol 1, art 8.1.
[31] *Ibid*, vol 1, art 8.3.
[32] *Ibid*, vol 1, art 8.4.

measuring empirical metrics, such as spikes in the bit-error-rate of downlinks, reductions in the signal-to-noise ratio, or uncoordinated carrier-to-interference ratios. By stripping away the requirement to prove subjective state intent, the ITU framework provides an immediate, technical finding of unlawful interference when a stalker satellite deploys localized RF disruption.

Administrative Record of the Radio Regulations Board (RRB)

Despite its technical precision, the practical efficacy of the ITU regime is severely constrained by systemic non-compliance. This institutional breakdown is evident in recent decisions of the Radio Regulations Board (RRB). Between 2024 and 2025, the RRB faced an unprecedented surge in formal complaints regarding sustained, intentional GNSS and Radio Navigation Satellite Service (RNSS) jamming and spoofing across the Baltic Sea region and the Middle East.[33]

European administrations and international bodies (including the European Union and NATO) presented extensive signal-location evidence proving that high-power ground and airborne emitters operating from Russian territory were systematically disabling civilian aviation and maritime navigation signals.[34]

In response, offending states routinely neutralized RRB directives by invoking Article 48 of the ITU Constitution, which grants Member States "entire freedom with regard to military radio installations", arguing that national security operations fall outside ITU oversight.[35] Moreover, states often dispute signal propagation modeling, or attribute emissions to unauthorized third-party actors. Ultimately, some space actors have simply ignored formal RRB determinations and joint agency warnings (such as joint ICAO/ITU/IMO statements) and maintained their violating operational activity.[36]

The ITU Enforcement Deficit

The systemic failure of the RRB in the Baltic and Middle Eastern theatres illustrates the core vulnerability of international telecommunications governance: the ITU possesses no coercive enforcement mechanisms. The RRB is an administrative body; it lacks the statutory authority

---

[33] See e.g. Council of the European Union, *Global Satellite Navigation Systems (GNSS) Jamming and Spoofing Threats: Call for Common Actions*, Doc No 9198/25 (22 May 2025) at 2–3.
[34] *Ibid* at 3–4.
[35] *ITU Constitution*, *supra* note 1, art 48(1).
[36] *Constitution of the International Telecommunication Union*, 22 December 1992, 1825 UNTS 3, art 48 (entered into force 1 July 1994); ITU, Radio Regulations Board, *Harmful Interference to RNSS Services*, Summary Record of Decisions, 98th–100th Meetings (Geneva: International Telecommunication Union, 2025); International Telecommunication Union, International Civil Aviation Organization & International Maritime Organization, *Joint Statement on Protecting Satellite Navigation from Harmful Interference* (Geneva: ITU, 25 March 2025); Francis Lyall & Paul B Larsen, *Space Law: A Authority and Interpretive Guide*, 2nd ed (London: Routledge, 2018) at 234–239; Dale Stephens, "The Regulation of Electronic Warfare in Outer Space" (2021) 97 Intl L Stud 81 at 98–101.

to issue binding injunctive relief, levy monetary fines, revoke orbital access, or authorize physical or electromagnetic countermeasures against non-compliant operators.

When an adversary state uses a stalker satellite to execute covert, sub-threshold RF operations in outer space, the ITU regime can accurately record the technical breach, but remains fundamentally incapable of halting the active orbital interference.

The Tallinn Manual 2.0

The *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Tallinn Manual) provides an influential, but non-binding, expert analysis of how existing international law applies to cyber operations. Electromagnetic interference is not always a cyber operation: jamming, spoofing, or other forms of electronic attack may disrupt a satellite's communications or sensors through the transmission or manipulation of electromagnetic signals without penetrating or manipulating the target's computer systems. Nevertheless, the Tallinn framework provides a useful analytical comparator where electromagnetic operations produce effects analogous to those capable of being produced through cyber operations.[37]

Use of Force

Rule 69 of the Manual addresses the prohibition on the use of force under Article 2(4) of the United Nations Charter. Rather than establishing a requirement of physical destruction, the Rule adopts a "scale and effects" approach, under which the consequences of a cyber operation are assessed against those associated with non-cyber uses of force. The commentary identifies a range of relevant factors, including severity, immediacy, directness, invasiveness, measurability of effects, military character, and State involvement. Accordingly, the Manual does not establish that physical destruction, injury, or death is a necessary condition for an operation to constitute a use of force.[38]

The treatment of temporary loss of functionality is correspondingly more nuanced than a strict physical-damage paradigm suggests. The fact that an effect is temporary or reversible does not, in itself, exclude an operation from the scope of Article 2(4). A severe, immediate, and militarily significant operation may potentially engage the prohibition even where the affected system subsequently returns to normal functionality. Conversely, relatively minor and transient disruption would ordinarily weigh against characterisation as a use of force. The Tallinn analysis therefore provides no categorical rule that interference requiring only rebooting, software reinstallation, or signal realignment necessarily falls outside Article 2(4).[39]

When an adversary stalker satellite utilises an AESA system to execute spatial nulling, or deploys low-power spoofing that temporarily blinds a target satellite's SAR sensors, the target

---

[37] Michael N Schmitt, ed, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed (Cambridge: Cambridge University Press, 2017) at 1–5, 11–14 [*Tallinn Manual 2.0*]; Dale Stephens, "The Regulation of Electronic Warfare in Outer Space" (2021) 97 Intl L Stud 81 at 84–89; PJ Blount, *Repressing Aggression in Outer Space: The Law of International Space Security* (Cheltenham: Edward Elgar Publishing, 2021) at 118–122.

[38] *Tallinn Manual 2.0*, *supra* note 1, r 69, paras 1, 8–10, 14, at 330, 332–337; *Charter of the United Nations*, 26 June 1945, Can TS 1945 No 7, art 2(4); *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)*, [1986] ICJ Rep 14 at para 195.

[39] *Tallinn Manual 2.0*, *supra* note 1, r 69, paras 11–13, at 334–336; Matthew Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)" (2011) 36:2 Yale J Intl L 421 at 431–438; Dale Stephens, "The Regulation of Electronic Warfare in Outer Space" (2021) 97 Intl L Stud 81 at 94–98.

spacecraft's physical hardware may remain entirely intact. That fact is legally relevant but not necessarily determinative. The more appropriate inquiry is whether the scale and effects of the electromagnetic operation, considered in context, are sufficiently severe, direct, invasive, measurable, and militarily significant to be comparable to a non-cyber use of force. Tallinn Manual 2.0 therefore cannot establish that localized RF disruption is inherently sub-threshold; rather, it demonstrates why the legal assessment should focus on the consequences of the operation rather than physical destruction alone.[40]

Armed Attack

The distinction between a use of force and an armed attack is also important when assessing electromagnetic counter-space operations. Rule 71 of the Tallinn Manual 2.0 treats an armed attack as requiring a higher degree of gravity than an unlawful use of force. The International Group of Experts (the Experts) who authored the Manual considered that a cyber operation causing serious injury or death to persons, or significant damage to or destruction of property, would satisfy this threshold, while recognising that the precise boundary remains unsettled. The Manual therefore does not establish that an armed attack necessarily requires catastrophic physical destruction, nor does it provide a definitive threshold for temporary functional disruption.[41]

Applied by analogy to stalker-satellite operations, a limited period of RF interference would therefore face a substantial, but not necessarily insurmountable, difficulty in satisfying the armed-attack threshold. Temporary disruption of a satellite's communications or sensing functions would generally require greater scale, severity, or strategic consequence before it could plausibly be characterised as an armed attack. Conversely, electromagnetic interference that disables critical military capabilities, produces grave consequences across a constellation, or contributes directly to consequences comparable to those associated with a kinetic attack cannot be excluded solely because the affected spacecraft remains physically intact.[42]

This threshold disparity nevertheless creates a significant legal problem for targeted states. A stalker satellite may impose strategically significant operational costs without necessarily producing effects sufficiently grave to trigger the right of self-defence under Article 51 of the United Nations Charter. The targeted state must therefore distinguish between the existence of an internationally wrongful act, an unlawful use of force, and an armed attack capable of

---

[40] *Tallinn Manual 2.0*, *supra* note 1, r 69; Merrill I Skolnik, *Radar Handbook*, 3rd ed (New York: McGraw-Hill, 2008) at 13.1–13.14; Cassandra Steer, "Space Security and the Challenge of Grey-Zone Conflict" in Cassandra Steer & Matthew Hersch, eds, *War and Peace in Space: Law, Policy, and Ethics* (Oxford: Oxford University Press, 2021) 145 at 152–158; CSIS, *Space Threat Assessment 2023*, by Makena Young & Kaitlyn Johnson (Washington, DC: Center for Strategic and International Studies, 2023) at 9–12.

[41] *Tallinn Manual 2.0*, *supra* note 1, r 71, paras 1–9, at 339–343; *Charter of the United Nations*, 26 June 1945, Can TS 1945 No 7, art 51; *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)*, [1986] ICJ Rep 14 at paras 191, 195.

[42] Dale Stephens, "The Regulation of Electronic Warfare in Outer Space" (2021) 97 Intl L Stud 81 at 94–98; Cassandra Steer, "Space Security and the Challenge of Grey-Zone Conflict" in Cassandra Steer & Matthew Hersch, eds, *War and Peace in Space: Law, Policy, and Ethics* (Oxford: Oxford University Press, 2021) 145 at 152–157; Matthew Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)" (2011) 36:2 Yale J Intl L 421 at 431–436.

triggering the right of self-defence. If the electromagnetic operation remains below the armed-attack threshold, a kinetic response against the stalker satellite cannot automatically be justified as an exercise of Article 51 self-defence; its legality must instead be assessed under the applicable rules governing countermeasures, necessity, and the prohibition on the use of force.[43]

Consequently, stalker satellites expose a potential gap between strategic effect and the gravity thresholds of the jus ad bellum. An adversary may be capable of producing substantial military disruption through reversible electromagnetic interference while leaving the targeted spacecraft physically intact, thereby creating uncertainty as to when the operation crosses from a technically sophisticated interference activity into a prohibited use of force or, at the higher threshold, an armed attack.[44]

Sovereignty Violations

Where an operation falls below the use-of-force threshold, the lawfulness of the conduct does not end with Article 2(4). The Tallinn Manual's treatment of sovereignty provides a further analytical framework, although again only by analogy where the underlying operation is electromagnetic rather than cyber. Rule 4 provides that a State must not conduct cyber operations that violate another State's sovereignty. In analysing territorial sovereignty, the Experts considered a spectrum of effects ranging from physical damage, through loss of functionality, to interference falling below the threshold of loss of functionality. Importantly, however, the Experts did not reach consensus on the precise threshold at which loss of functionality, or effects below that threshold, constitute a violation of sovereignty.[45]

This uncertainty is particularly relevant to orbital stalker satellites. A targeted spacecraft may constitute a sovereign governmental asset and may perform inherently governmental functions, including military command-and-control, intelligence collection, or strategic surveillance. An electromagnetic operation that interferes with those functions could therefore raise questions concerning sovereignty even where its effects fall below the use-of-force threshold. However, the Tallinn Manual does not establish that the same sovereignty rules automatically govern electromagnetic interference in outer space. The stronger proposition is that its effects-based analysis offers a useful framework for evaluating

---

[43] *Responsibility of States for Internationally Wrongful Acts*, GA Res 56/83, UNGAOR, 56th Sess, Supp No 10, UN Doc A/RES/56/83 (2001) arts 21, 25, 49–53; International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, UN GAOR, 53rd Sess, Supp No 10, UN Doc A/56/10 (2001) at 71–74, 80–84, 128–139; PJ Blount, *Repressing Aggression in Outer Space: The Law of International Space Security* (Cheltenham: Edward Elgar Publishing, 2021) at 142–155; *Oil Platforms (Islamic Republic of Iran v United States of America)*, [2003] ICJ Rep 161 at paras 51, 73–77.

[44] *Tallinn Manual 2.0*, *supra* note 1, r 69, 71; CSIS, *Space Threat Assessment 2023*, by Makena Young & Kaitlyn Johnson (Washington, DC: Center for Strategic and International Studies, 2023) at 9–12; Dale Stephens, "The Regulation of Electronic Warfare in Outer Space" (2021) 97 Intl L Stud 81 at 98–101; Michael N Schmitt, "Grey Zone Cyber Operations and the Law of State Responsibility" (2021) 97 Intl L Stud 78 at 82–88.

[45] *Tallinn Manual 2.0*, *supra* note 1, r 4, paras 1, 10–16, at 17, 20–24; Michael N Schmitt & Liis Vihul, "Respect for Sovereign Statehood in Cyberspace" (2017) 95:1 Tex L Rev 1639 at 1644–1652.

whether sufficiently serious interference with a State's governmental space capabilities could engage the underlying customary principle of sovereignty[46].

The principal difficulty remains attribution and proof. A State seeking to characterise covert electromagnetic interference as an internationally wrongful act must establish both the occurrence and legal character of the interference and, where State responsibility is alleged, a sufficient basis for attributing the conduct to another State. The technical difficulty of distinguishing deliberate RF interference from equipment malfunction, space weather, radiation effects, or other sources may therefore complicate the evidentiary case. Nevertheless, uncertainty of attribution should not be equated with the absence of a legal violation: it is an evidentiary and attribution problem rather than a substantive rule permitting otherwise unlawful conduct.[47]

When a stalker satellite employs low-power, spread-spectrum RF techniques such as DSSS or FHSS, the resulting signal may be difficult to distinguish from background noise or other sources of interference. This creates a particularly challenging evidentiary environment where the operation is designed to minimise observable signatures. The legal significance of such techniques therefore lies not in creating "complete legal deniability", but in increasing the practical difficulty of demonstrating the factual occurrence, State attribution, and legal consequences of the interference. The Tallinn Manual's sovereignty analysis is consequently best used to demonstrate the unresolved legal space between technically observable interference, provable internationally wrongful conduct, and conduct sufficiently grave to engage the prohibition on the use of force.[48]

---

[46] *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, 27 January 1967, 610 UNTS 205, art VIII (entered into force 10 October 1967); PJ Blount, *Repressing Aggression in Outer Space: The Law of International Space Security* (Cheltenham: Edward Elgar Publishing, 2021) at 88–95; Francis Lyall & Paul B Larsen, *Space Law: A Authority and Interpretive Guide*, 2nd ed (London: Routledge, 2018) at 53–62; Dale Stephens, "The Regulation of Electronic Warfare in Outer Space" (2021) 97 Intl L Stud 81 at 88–92.

[47] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, UN GAOR, 53rd Sess, Supp No 10, UN Doc A/56/10 (2001) arts 2, 4–8, at 34–45, 80–84; Thomas Rid & Ben Buchanan, "Attributing Cyber Attacks" (2015) 38:1 J Strategic Studies 4 at 10–18; Secure World Foundation, *Global Counterspace Capabilities: An Open Source Assessment*, ed by Brian Weeden & Victoria Samson (Washington, DC: Secure World Foundation, 2024) at 1-14–1-18.

[48] Don Torrieri, *Principles of Spread-Spectrum Communication Systems*, 4th ed (Cham, Switzerland: Springer, 2018) at 45–58; Richard A Poisel, *Modern Communications Jamming Principles and Techniques*, 2nd ed (Boston: Artech House, 2011) at 211–218; *Tallinn Manual 2.0*, *supra* note 1, r 4, 69; Michael N Schmitt, "Grey Zone Cyber Operations and the Law of State Responsibility" (2021) 97 Intl L Stud 78 at 88–94.

UN COPUOS Guidelines on the Long-Term Sustainability of Outer Space Activities

Diplomatic Consensus

In an effort to address operational risks in an increasingly congested and contested orbital environment, the United Nations Committee on the Peaceful Uses of Outer Space (COPUOS) adopted the *Guidelines for the Long-Term Sustainability of Outer Space Activities* in 2019 (LTS Guidelines). Among these voluntary recommendations, Guideline B.1 ("Provide updated contact information and share information on space objects and orbital events") encourages States and international intergovernmental organizations to exchange information concerning on-orbit spacecraft operations, conjunction assessments, and space objects and events. Guideline B.4 ("Perform conjunction assessment during all orbital phases of controlled flight") recommends the systematic assessment of current and planned spacecraft trajectories and the sharing of relevant information to reduce collision risks.[49]

The LTS Guidelines reflect a diplomatic consensus on voluntary practices for space safety, information-sharing, and collision avoidance, but they do not themselves establish binding legal obligations governing intentional counter-space operations. The LTS Guidelines therefore establish a voluntary baseline of information-sharing and conjunction-assessment practices against which the conduct of an orbital stalker satellite can be evaluated. Their principal limitation is not just that they are unenforceable, but that they do not prescribe a substantive prohibition on deliberate proximity operations or electromagnetic interference. Thus, while a State may invoke the Guidelines to support expectations of transparency, coordination, and collision avoidance, they provide limited normative guidance where the proximity operation is intentional, covert, and designed to produce military effects rather than avoid physical collision.[50]

[49] UN Committee on the Peaceful Uses of Outer Space, *Report of the Committee on the Peaceful Uses of Outer Space*, UNGAOR, 74th Sess, Supp No 20, UN Doc A/74/20 (2019), annex II, *Guidelines for the Long-Term Sustainability of Outer Space Activities*, Guidelines B.1 & B.4 [LTS Guidelines].
[50] *LTS Guidelines*, supra note 1, preamble; see also UNGA, *International Cooperation in the Peaceful Uses of Outer Space*, UNGA Res 74/82, UN Doc A/RES/74/82 (2019).

UK Regulations

The failure of public international space law to deter sub-threshold electronic warfare and proximity operations forces sovereign states to use domestic licensing, regulatory oversight, and market access rules to ensure technical resilience of their space assets.[51]

Beyond the development of state-level offensive capabilities,[52] the urgent focus of domestic regulators and policymakers must be to protect UK space assets from non-kinetic interference. This chapter critically evaluates five core aspects of the UK's regulatory architecture that governs the resilience of its space assets: commercial integration and the importance of hardware resilience mandates, automated telemetry escrow and intelligence pipelines, trusted operator status and legal defensibility, the statutory definition of "harmful interference", and market access and insurance enforcement.[53]

By establishing rigorous domestic hardware and technical resilience standards, the UK can position its regulatory framework as an exportable model for strategic partners across Five Eyes, AUKUS Pillar II, and NATO. Exporting these technical requirements unifies allied market standards, creating a cohesive, plurilateral regulatory posture that reinforces collective space domain defence against sub-threshold electronic warfare.[54]

Hardware Resilience Mandates

Military operations, intelligence gathering, and critical national infrastructure increasingly rely on civil and commercial satellite networks. Consequently, commercial space assets operating under UK jurisdiction form an integral layer of national security infrastructure, exposing sovereign capabilities to commercial supply-chain vulnerabilities[55].

However, the existing licensing regime under the Space Industry Regulations (SIR) 2021 evaluates technical competence primarily through the narrow lenses of launch safety, orbital

---

[51] *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, 27 January 1967, 610 UNTS 205 (entered into force 10 October 1967) arts VI, IX [*Outer Space Treaty*]; Francis Lyall & Paul B Larsen, *Space Law: A Authority and Interpretive Guide*, 2nd ed (London: Routledge, 2018) at 53–78; PJ Blount, *Repressing Aggression in Outer Space: The Law of International Space Security* (Cheltenham: Edward Elgar Publishing, 2021) at 112–128.

[52] In response to hostile orbital activity, the UK Government conducts its own defensive counter-space operations through state intelligence and defence bodies, authorized under the Royal Prerogative, the Intelligence Services Act 1994, and statutory national security exemptions. Private entities are strictly prohibited from engaging in offensive electronic warfare, jamming, or cyber operations under section 68 of the Wireless Telegraphy Act 2006 and the Computer Misuse Act 1990 without Crown authorization.

[53] UK, Ministry of Defence, *UK Space Power*, Joint Doctrine Publication 0-30 (Shrivenham: Development, Concepts and Doctrine Centre, 2022) at 24–32; UK, Department for Science, Innovation and Technology, *National Space Strategy* (London: DSIT, 2021) at 14–19.

[54] Ministry of Defence, *Defence Space Strategy: Operationalising the Space Domain* (London: MoD, 2022) at 18–22; AUKUS, *Joint Leaders Statement on AUKUS Pillar II Capability Priorities* (White House Press Release, 1 December 2023).

[55] UK Space Agency, *National Space Strategy* (2021) at 10–15; *Space Industry Act 2018* (UK), c 5, ss 8–12 [*SIA 2018*]; European Union Agency for Cybersecurity (ENISA), *Securing the Space Supply Chain: Cyber Security Measures for Space Systems* (Athens: ENISA, 2023) at 15–22.

debris mitigation, space situational awareness, and third-party liability risk. The statutory criteria remain silent on payload resistance to non-kinetic interference. Under Part 3 of the SIA 2018 and the SIR 2021, the Civil Aviation Authority (CAA) imposes no explicit statutory obligations on orbital licensees to demonstrate hardware-level electromagnetic resilience or anti-jamming survivability.[56]

Because UK regulations do not mandate electromagnetic hardening, commercial platforms frequently employ cost-optimised, off-the-shelf components. These unhardened systems remain highly vulnerable to sub-threshold counter-space operations executed by adversary stalker satellites, including low-power telemetry spoofing, AESA spatial nulling, and cognitive SDR signal manipulation[57].

The UK must expand the statutory role of the CAA's Space Regulation team, evolving it from an administrative compliance body into a dedicated regulatory technical authority. While the CAA currently assesses general operational risk and safety cases under section 9 of the SIA 2018, it lacks the explicit statutory mandate and internal technical framework required to evaluate payload electromagnetic survivability. Embedding technical resilience experts directly within the CAA's existing licensing directorate would enable the regulator to conduct active technical verifications of payload architectures prior to granting orbital licences.[58]

To address this regulatory deficit, the Secretary of State should amend the Space Industry Regulations 2021 (specifically expanding Part 11 operational safety and risk requirements) to make orbital licence grants conditional on verified baseline hardware resilience. The UK should establish a statutory supply-chain vetting framework for all licensed space infrastructure, drawing direct legislative inspiration from the risk management regimes under the Telecommunications (Security) Act 2021. Rather than relying on high-level vendor self-attestations, the Space Industry Regulations 2021 should mandate end-to-end provenance auditing across the entire space payload architecture, including microelectronics and software stacks.[59]

Automated Telemetry Escrow and Intelligence Pipelines

Commercial satellite operators view telemetry streams as commercially sensitive intellectual property and trade secrets, resisting raw data sharing with sovereign regulatory or intelligence bodies in the absence of explicit statutory compulsion. Operators routinely isolate onboard diagnostic metrics, bus health logs, and telemetry, tracking, and command data behind

---

[56] *The Space Industry Regulations 2021*, SI 2021/792, reg 18–25, pt 11; Civil Aviation Authority, *CAP 2221: Spaceflight Licensing Guidance – Safety Case and Risk Assessment* (London: CAA, 2021) at 34–41.
[57] CSIS, *Space Threat Assessment 2023*, by Makena Young & Kaitlyn Johnson (Washington, DC: Center for Strategic and International Studies, 2023) at 8–12; Richard A Poisel, *Modern Communications Jamming Principles and Techniques*, 2nd ed (Boston: Artech House, 2011) at 211–218.
[58] *SIA 2018*, *supra* note 4, s 9; Civil Aviation Authority, *CAP 2210: Regulating Licensed Space Activities* (London: CAA, 2021) at 12–16.
[59] *Telecommunications (Security) Act 2021* (UK), c 31, ss 1–5; *The Space Industry Regulations 2021*, *supra* note 5, pt 11.

proprietary corporate firewalls. This creates a critical intelligence blind spot, and prevents sovereign defence bodies from detecting co-orbital threats.[60]

Commercial mission control centers typically attribute non-kinetic orbital anomalies (such as a sudden BER spike, carrier-to-noise degradation, or temporary optical sensor blinding) to internal hardware fatigue, single-event upsets caused by cosmic radiation, or solar flare activity, failing to recognize deliberate, low-power electronic warfare or proximity spoofing executed by an adversary stalker satellite. When a UK-licensed commercial satellite encounters operational degradations the operator will often lack real-time orbital intelligence to successfully diagnose the anomaly.[61]

Conversely, state intelligence and defence organisations (namely GCHQ, RAF Space Command, and the UK Space Operations Centre) possess sophisticated, classified space domain awareness and signals intelligence capabilities capable of identifying hostile orbital manoeuvres and RF emissions. However, under the existing regulatory framework, there is no statutory operational mechanism or secure pipeline for real-time, bi-directional intelligence sharing between these defence entities and commercial licensees. The flow of threat data remains ad-hoc, manual, and unsuited to high-speed orbital interference events.[62]

The Space Industry Regulations 2021 should be amended to introduce a mandatory, encrypted "telemetry escrow" requirement as a standard condition for obtaining and retaining an orbital licence under the Space Industry Act 2018. Under this regime, operators must configure satellite bus architectures to automatically escrow encrypted, real-time streams of raw telemetry metrics (including signal-to-noise ratios, bus voltage stability, attitude control anomalies, and payload BER logs) into a secure sovereign vault maintained under government authority.[63]

Legislation should formalize a direct statutory intelligence interface connecting licensed commercial space operators with GCHQ and the UK Space Operations Centre. Raw, anonymized diagnostic and telemetry telemetry logs would stream continuously at machine speed from commercial payloads into a secure processing enclave hosted by GCHQ and the UK Space Operations Centre. Automated algorithmic cross-referencing of telemetry across multiple commercial constellations would allow state signals analysts to rapidly detect wide-area or localized electromagnetic attack patterns.[64]

---

[60] Secure World Foundation, *Global Counterspace Capabilities: An Open Source Assessment*, ed by Brian Weeden & Victoria Samson (Washington, DC: Secure World Foundation, 2024) at 1-14–1-18; Francis Lyall & Paul B Larsen, *Space Law: A Authority and Interpretive Guide*, 2nd ed (London: Routledge, 2018) at 234–238.
[61] David L Wright, Laura Grego & Cameron Wright, *The Physics of Space Security: A Reference Manual* (Cambridge, Mass: American Academy of Arts and Sciences, 2005) at 118–122; Thomas Rid & Ben Buchanan, "Attributing Cyber Attacks" (2015) 38:1 J Strategic Studies 4 at 10–14.
[62] Ministry of Defence, *Defence Space Strategy: Operationalising the Space Domain* (London: MoD, 2022) at 24–28; UK Space Agency, *Civil-Military Space Co-operation Policy* (London: UKSA, 2023) at 8–12.
[63] *SIA 2018*, *supra* note 4, s 13; *The Space Industry Regulations 2021*, *supra* note 5, reg 22.
[64] *Intelligence Services Act 1994* (UK), c 13, s 3; UK Space Command, *Space Domain Awareness Operational Concept Paper* (High Wycombe: UK Space Command, 2023) at 14–19.

In return, GCHQ and the UK Space Operations Centre should be statutorily authorized to push automated, machine-speed threat warnings and orbital attribution vector alerts directly to commercial operators when state assets detect an unannounced RPO or LPI jamming source in the satellite's vicinity.[65]

To operationalize this intelligence pipeline, the CAA and GCHQ should require licensees to establish pre-cleared, automated contingency response protocols as part of their operational safety cases. When the sovereign pipeline flags active, targeted interference, these protocols would allow the satellite's software-defined payload to automatically execute dynamic frequency-hopping algorithms, beamforming null adjustments, or temporary sensor-shuttering routines to neutralize the threat before permanent operational degradation occurs.[66]

Trusted Operator Status and Legal Defensibility

Under public international law, victim states and commercial satellite operators face an almost insurmountable evidential burden when attempting to prove that transient radio frequency interference or sensor degradation was caused by deliberate state-sponsored aggression rather than cosmic background radiation, solar weather, or internal hardware failure. Since non-kinetic counter-space operations leave no physical wreckage, the resulting attribution gap leaves commercial primes and state actors in a position of legal paralysis. Without verified, legally defensible attribution, operators are unable to seek civil remedies, successfully invoke insurance indemnity, or justify proportional state-level defensive countermeasures.[67]

To resolve this evidential deadlock, the UK should establish a formal statutory designation of "Trusted Operator" within the Space Industry Regulations 2021. This status would be granted exclusively to commercial licensees that satisfy mandated hardware resilience standards and actively participate in the automated telemetry escrow and intelligence pipeline with GCHQ and the UK Space Operations Centre.[68]

Crucially, achieving Trusted Operator status would introduce a statutory rebuttable presumption of operational integrity under English civil and commercial law. In the event of an orbital anomaly or operational degradation, a Trusted Operator's space asset would be legally presumed to have been operating free of internal hardware manufacturing defects, software glitches, or maintenance failures. This presumption effectively shifts the evidential

---

[65] Bruce A Fette, ed, *Cognitive Radio Technology*, 2nd ed (Burlington, Mass: Academic Press, 2009) at 145–152.
[66] Don Torrieri, *Principles of Spread-Spectrum Communication Systems*, 4th ed (Cham, Switzerland: Springer, 2018) at 45–58; *The Space Industry Regulations 2021*, *supra* note 5, pt 11.
[67] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, UN GAOR, 53rd Sess, Supp No 10, UN Doc A/56/10 (2001) arts 2, 4–8, at 34–45, 80–84; Michael N Schmitt, "Grey Zone Cyber Operations and the Law of State Responsibility" (2021) 97 Intl L Stud 78 at 82–88.
[68] *The Space Industry Regulations 2021*, *supra* note 5, pt 3.

burden in English litigation and arbitration, requiring insurers or opposing parties to prove that the loss resulted from an internal system failure rather than external electromagnetic interference.[69]

This evidentiary shift provides commercial primes and operators with more robust legal protection. By establishing a legally defensible foundation of operational health, Trusted Operators can confidently assert force majeure clauses in commercial service agreements and validate war-risk insurance claims. Moreover, through the proposed escrow pipeline, the UK Government would acquire the requisite evidentiary basis (real-time diagnostic telemetry) to pursue diplomatic remedies or counter-measures under international law.[70]

Statutory Definition of "Harmful Interference" under English Law

A fundamental flaw of the international legal framework governing space operations is its normative ambiguity. Neither of the OST or ITU frameworks codify quantitative spatial distance thresholds or objective signal physics metrics to define when the threshold of "harmful interference" has been crossed. Simultaneously, English law lacks a codified, parameter-based statutory definition of unlawful orbital interference, creating a regulatory vacuum that hinders effective domestic enforcement.[71]

To eliminate this ambiguity, the UK should amend the Space Industry Act 2018 to enact a precise statutory definition of "harmful interference" enforceable under English jurisdiction.[72] Rather than relying on subjective determinations of adversary intent, the statutory definition should codify objective, empirical physical criteria:

$$\Delta \text{BER} > \text{Threshold}_{\text{crit}} \vee (\text{RPO}_{\text{distance}} < D_{\text{safety}} \wedge \text{RF}_{\text{uncoordinated}} = 1)$$

Under this statutory model, harmful interference is established when a satellite experiences a BER degradation exceeding critical operational thresholds relative to baseline thermal noise, or when an unannounced secondary spacecraft enters a defined spatial keep-out corridor (for instance, less than 10 kilometres in geostationary orbit or less than 2 kilometres in low Earth orbit) while emitting uncoordinated radio frequency signals.[73]

---

[69] *Senior Courts Act 1981* (UK), c 54, s 49; Adrian Keane & Paul McKeown, *The Modern Law of Evidence*, 13th ed (Oxford: Oxford University Press, 2020) at 88–104.
[70] *Draft Articles on State Responsibility*, *supra* note 16, arts 49–53; PJ Blount, *Repressing Aggression in Outer Space: The Law of International Space Security* (Cheltenham: Edward Elgar Publishing, 2021) at 142–155.
[71] *Outer Space Treaty*, *supra* note 1, art IX; *Constitution of the International Telecommunication Union*, 22 December 1992, 1825 UNTS 3, art 45 (entered into force 1 July 1994) [*ITU Constitution*]; *Wireless Telegraphy Act 2006* (UK), c 36, ss 68–70.
[72] *SIA 2018*, *supra* note 4, s 69; Dale Stephens, "The Regulation of Electronic Warfare in Outer Space" (2021) 97 Intl L Stud 81 at 98–101.
[73] Merrill I Skolnik, *Radar Handbook*, 3rd ed (New York: McGraw-Hill, 2008) at 13.1–13.14; ITU, Radio Regulations Board, *Harmful Interference to RNSS Services*, Summary Record of Decisions, 98th–100th Meetings (Geneva: International Telecommunication Union, 2025).

Codifying these technical parameters into domestic legislation provides UK courts, regulators, and arbitral tribunals with an objective statutory standard. This enables UK authorities to make definitive legal findings of unlawful interference independently of prolonged and consensus-bound international bodies, establishing clear legal liability under domestic law.[74]

Market Access and Insurance Enforcement

The commercial space sector faces severe financial risk due to grey-zone counter-space operations, placing London's space insurance and underwriting market in a precarious position. Underwriters at Lloyd's of London routinely struggle to assess non-kinetic orbital risks, leading to widespread reliance on standard "War Exclusion" clauses to deny coverage when a satellite suffers performance loss. Since electronic warfare is often difficult to diagnose and attribute, establishing whether an operational failure constitutes an uninsurable act of war or a covered commercial loss leads to costly and protracted legal disputes. Furthermore, while the statutory liability framework under the Space Industry (Indemnities) Act 2025 limits operator liability, it fails to condition these indemnity caps on electromagnetic survivability.[75]

The UK can resolve this market failure by leveraging London's global position in space insurance, risk underwriting, and capital markets to enforce resilience standards worldwide. Access to UK statutory indemnity limits under the 2025 Act and eligibility for commercial underwriting within the London market should be statutorily conditioned on an operator attaining Trusted Operator status and verifying baseline hardware resilience.[76]

Simultaneously, the UK Government should issue statutory guidance clarifying the application of war exclusion clauses to non-kinetic space operations. The guidance should specify that sub-threshold, non-destructive electronic warfare (which falls below the thresholds of Tallinn Manual Rules 14 and 17) does not trigger standard war exclusion clauses unless the incident is formally attributed to a sovereign state actor by UK intelligence authorities or the CAA.[77]

By tying market access, insurance eligibility, and liability protection directly to domestic resilience standards, the UK extends its regulatory reach globally. Foreign satellite operators seeking insurance coverage or capital market listings in London will be incentivized to adopt UK hardware resilience and telemetry protocols, establishing the UK statutory framework as a leader in space domain defence.[78]

---

[74] *Wireless Telegraphy Act 2006*, *supra* note 20, s 68; Francis Lyall & Paul B Larsen, *Space Law: A Authority and Interpretive Guide*, 2nd ed (London: Routledge, 2018) at 234–239.
[75] *Space Industry (Indemnities) Act 2025* (UK), c 12, ss 1–4; Lloyd's Market Association, *Space Insurance Joint Space Committee War and Anti-Satellite Exclusion Clauses* (LMA Specimen Clause LMA5501, 2021); Joint War Committee, *Space Hull War and Extension Clauses* (London: LMA, 2022).
[76] *Space Industry (Indemnities) Act 2025*, *ibid*, s 3; *SIA 2018*, *supra* note 4, s 12.
[77] Michael N Schmitt, ed, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed (Cambridge: Cambridge University Press, 2017) r 14, 17, 69, 71; *Insurance Act 2015* (UK), c 4, ss 10–11.
[78] *Financial Services and Markets Act 2000* (UK), c 8, s 137A; UK Space Agency, *Global Space Market Access Guidelines* (London: UKSA, 2024) at 11–15.

International Collaboration

UK Regulatory Leadership

The structural paralysis of consensus-based international space governance necessitates a strategic pivot towards plurilateral regulatory export. Since multilateral forums such as the UN COPUOS and the ITU remain incapacitated by adversary vetoes and normative ambiguity, the UK should leverage its comparative advantages in legal architecture, risk underwriting, and intelligence integration to establish de facto global standards.[79] These regulations must specifically focus on hardware resilience mandates, automated telemetry escrow pipelines, and the Trusted Operator framework. By exporting its domestic regulatory apparatus, the UK can construct an interoperable regulatory and security zone among aligned middle powers and transatlantic allies.[80]

The demand for UK regulatory leadership stems from acute operational and market failures across Western space economies. Commercial satellite constellations providing critical communications, earth observation, and maritime tracking now operate under heightened exposure to un-attributable, sub-threshold electronic warfare in low Earth and geostationary orbits.[81] Commercial operators and primary risk underwriters currently lack a neutral, legally binding evidentiary mechanism to distinguish internal hardware failure from hostile electromagnetic interference.[82]

Comparative regulatory models fail to resolve this institutional friction. The US maintains a bifurcated regulatory landscape, fractured between defence-led operational commands and commercially deregulated federal agencies.[83] France prioritises a state-centric "active defence" doctrine that offers limited integration for commercial market mechanisms.[84] Conversely, the UK uniquely consolidates English governing law, the Lloyd’s space

---

[79] UN COPUOS, *Report of the Committee on the Peaceful Uses of Outer Space*, UN GAOR, 78th Sess, Supp No 20, UN Doc A/78/20 (2023) at 12–18; PJ Blount, *Repressing Aggression in Outer Space: The Law of International Space Security* (Cheltenham: Edward Elgar Publishing, 2021) at 88–105; Stephan Hobe, *Space Law* (Munich: CH Beck, 2019) at 45–52.
[80] UK, Ministry of Defence, *Global Strategic Trends: Out to 2050*, 7th ed (Shrivenham: DCDC, 2024) at 112–118; Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford: Oxford University Press, 2020) at 25–48.
[81] CSIS, *Space Threat Assessment 2024*, by Makena Young & Kaitlyn Johnson (Washington, DC: Center for Strategic and International Studies, 2024) at 14–22; Secure World Foundation, *Global Counterspace Capabilities: An Open Source Assessment*, ed by Brian Weeden & Victoria Samson (Washington, DC: SWF, 2024) at 2-10–2-18.
[82] Lloyd's Market Association, *Space Insurance Joint Space Committee War and Anti-Satellite Exclusion Clauses* (LMA Specimen Clause LMA5501, 2021); Joint War Committee, *Space Hull War and Extension Clauses* (London: LMA, 2022); Francis Lyall & Paul B Larsen, *Space Law: A Authority and Interpretive Guide*, 2nd ed (London: Routledge, 2018) at 234–240.
[83] National Space Strategy for the United States of America (Washington, DC: The White House, 2023) at 8–14; US, Federal Communications Commission, *Mitigation of Orbital Debris in the New Space Age*, Report and Order, FCC Doc 20-54 (2020).
[84] France, Ministère des Armées, *Space Defence Strategy: 2019–2025* (Paris: DGRIS, 2019) at 16–22; Julien Mariez, "French Space Legislation and National Defence Concerns" (2020) 45:2 Air & Space L 189 at 192–198.

underwriting market, and the signals intelligence capabilities of GCHQ.[85] Foreign operators and allied sovereigns would be thus structurally incentivised to adopt UK technical standards to access London capital markets, secure commercial insurance underwriteability, and maintain statutory liability indemnities.[86]

Allied Security Frameworks

Accordingly, following the policy proposals set out in the preceding chapter, the UK should integrate its automated telemetry escrow requirements and hardware resilience standards into Five Eyes intelligence-sharing architectures and AUKUS Pillar II advanced capability frameworks.[87] Mandating common technical specifications for payload bus encryption, LPI detection, and machine-to-machine threat alerts will construct a unified technical perimeter across allied sovereign and commercial fleets. Concurrently, the Department for Business and Trade and the CAA should execute mutual recognition agreements with key European and Commonwealth regulators, ensuring that Trusted Operator status granted under English law confers reciprocal market access and liability protections across allied jurisdictions.[88]

Outer Space Treaty Annex

Over the medium term, the UK should convene a coalition of like-minded spacefaring nations to draft a plurilateral Technical Annex to the Outer Space Treaty.[89] This instrument would codify quantitative physical metrics for "harmful interference" under Article IX OST, establishing legally binding orbital keep-out zones and empirical bit-error-rate degradation thresholds.[90] By embedding these objective criteria into NATO operational doctrines and London insurance covenants, the UK can formalize an enforceable, market-backed standard of care that transforms open-textured public international space law into an actionable regime for orbital resilience.[91]

---

[85] *Space Industry Act 2018* (UK), c 5, ss 8–13; *Intelligence Services Act 1994* (UK), c 13, s 3; UK, Department for Science, Innovation and Technology, *National Space Strategy* (London: DSIT, 2021) at 14–20.
[86] *Space Industry (Indemnities) Act 2025* (UK), c 12, ss 1–4; *Financial Services and Markets Act 2000* (UK), c 8, s 137A; UK Space Agency, *Global Space Market Access Guidelines* (London: UKSA, 2024) at 8–14.
[87] AUKUS, *Joint Leaders Statement on AUKUS Pillar II Capability Priorities* (White House Press Release, 1 December 2023); UK Space Command, *Combined Space Operations Initiative Memorandum of Understanding* (High Wycombe: UK Space Command, 2023).
[88] *The Space Industry Regulations 2021*, SI 2021/792, reg 18–25, pt 11; Civil Aviation Authority, *CAP 2210: Regulating Licensed Space Activities* (London: CAA, 2021) at 18–24.
[89] *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, 27 January 1967, 610 UNTS 205 (entered into force 10 October 1967) art IX [*Outer Space Treaty*]; Bin Cheng, *Studies in International Space Law* (Oxford: Clarendon Press, 1997) at 383–402.
[90] *Constitution of the International Telecommunication Union*, 22 December 1992, 1825 UNTS 3, art 45 (entered into force 1 July 1994); Dale Stephens, "The Regulation of Electronic Warfare in Outer Space" (2021) 97 Intl L Stud 81 at 95–102.
[91] NATO, *NATO's Overarching Space Policy* (Brussels: NATO Public Diplomacy Division, 2019) at 3–7; Michael N Schmitt, ed, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed (Cambridge: Cambridge University Press, 2017) r 14, 17, 71.

Conclusion

International space governance has stalled through normative ambiguity and structural paralysis; domestic statutory frameworks must therefore step in to establish operational order. The vague "due regard" obligation under Article IX of the OST, the enforcement limitations of the ITU, and the physical damage thresholds of the Tallinn Manual fail to address non-kinetic electronic warfare. Resolving this security deficit requires shifting focus from multilateral treaties to market-enforced domestic regulatory leadership and plurilateral standards.

The UK Government must take legislative action. First, it should amend Part 11 of the Space Industry Regulations 2021 to make Orbital Operator Licences conditional on verified hardware-level electromagnetic resilience and automated telemetry escrow compliance. Second, it should incorporate GCHQ and the National Cyber Security Centre into the licensing apparatus within the CAA as a joint Regulatory Technical Authority. Third, it should enact a precise statutory definition of "harmful interference" under English domestic law based on empirical bit-error-rate degradation thresholds and spatial keep-out corridors.

International partners across Five Eyes, AUKUS Pillar II, and NATO should be encouraged to coordinate with these domestic reforms. They should adopt the proposed technical licensing framework as an international baseline, recognize "Trusted Operator" status across jurisdictions to ensure reciprocal market access, and draft a plurilateral Technical Annex to the Outer Space Treaty that formalizes objective operational standards for proximity operations.

Implementing these recommendations will harden critical space infrastructure against non-kinetic attack, close the attribution gap through automated diagnostic telemetry, resolve insurance war exclusion disputes under English law, and establish market-backed standards for space domain defence. Failing to implement them will leave Western satellite constellations vulnerable to un-attributable disruption, render commercial operators uninsurable under standard underwriting terms, and allow adversary states to gain operational control of critical orbital spectrums without triggering legal repercussions.