SPCE 402 — MINI-PRESENTATION 2

Don’t forget the little guy: Space Security & International Law

Treaties, threat frameworks, and where the Pacific fits in

Ben | Victoria University of Wellington

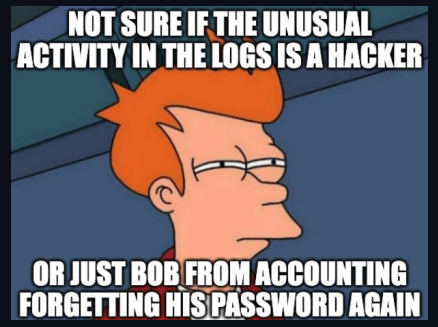
13 August 2026

We depend on space.

Communications, positioning/timing, finance, weather, and defence all now route through a few thousand objects in orbit.

But the legal architecture protecting them was built for two kinds of actor: states, and the entities states license. It has almost nothing to say about anyone else.

My goal today is to convince you not to forget about the little guy, as the little guy certainly wont forget about you.



1967 — Outer Space Treaty — still the only binding global space law framework

70+ — Nations signed the (non-binding) Artemis Accords as of mid-2026

0 — Individuals ever held internationally responsible for attacking a satellite

Outer Space Treaty, 1967

Grounded in the 1967 Outer Space Treaty (OST), still the constitution of international space law. Everything since, including Artemis, claims to build on it, not replace it.

Peaceful purposes

Space is to be explored and used for the benefit of all countries; no weapons of mass destruction in orbit.

Non-appropriation

No state may claim sovereignty over the Moon, other celestial bodies, or outer space itself.

State responsibility

Article VI: governments bear responsibility for ‘national activities’ in space, including those of authorised private companies.

Liability for damage

A launching state is liable for damage its space objects cause, on Earth or in space (Liability Convention, 1972).

The Artemis Accords

Signed 13 Oct 2020 by 8 founding nations (incl. Australia, UK, US, Japan). By mid-2026, **70 signatories**. A *non-binding political commitment* that operationalises Outer Space Treaty obligations.

KEY PRINCIPLES

- Transparency — notify others of activities & general location
- Interoperability — shared technical standards across missions
- ‘Safety zones’ — coordination to avoid harmful interference
- Orbital debris mitigation & safe spacecraft disposal
- Space resource utilisation is permitted, consistent with OST

SIGNATORY GROWTH

8 → 70

nations, Oct 2020 → Jul 2026

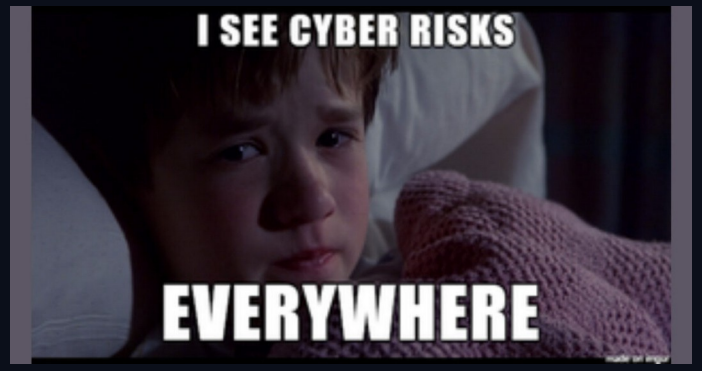
Its Amazing how many nations have signed on here, but the issue is that its not everyone.
And Crucially doesn’t include Russia or China!

The architecture protects states — and their licensees

Article VI makes an authorised private company, For example SpaceX a *'national activity'* once a state authorises and supervises it. Responsibility therefore flows back to the state.

But an individual, hacktivist collective, or independent crew has no obvious Article VI chain. Attribution can become a question of customary international law, Local Legislation and sometimes the pressure of the public

SPARTA makes the same distinction from the technical side: it can describe space-specific attacker behaviour, but a threat taxonomy cannot decide who bears international responsibility. (Buchan, 'Cyber Due Diligence', EJIL 32(3), 2021.)



STATE

authorises + supervises

↓

AUTHORISED PRIVATE ENTITY
(e.g. SpaceX)

Article VI responsibility attaches

INDEPENDENT ACTOR
(individual / unofficial group)

no authorisation → no obvious Art. VI

Viasat, 2022

An hour before Russia's invasion of Ukraine, the **AcidRain** wiper disabled tens of thousands of Viasat KA-SAT modems, disrupting Ukrainian military and civilian communications and causing wider European spillover.

24 Feb

2022 — attack lands roughly one hour before the invasion

5,800

German wind turbines affected as collateral spillover

75 days

until EU + Five Eyes publicly attributed the attack to Russia's GRU

0

prosecutions, ICJ cases, or compensation mechanisms that followed

Source: Kazi, Kazi & Bhosale, 'Invisible Battlefields: Analyzing the Viasat Attack and its Broader Implications', Scientific Bulletin 1(59), 2025.

And here it Is, a State Sponsored hacker, but no accountability. Seems there might be room for some work to be done here...

Attack #1 was already an independent actor

22 APRIL 1986

‘Captain Midnight’ hijacks HBO

A satellite-TV engineer, annoyed at HBO’s rising subscription prices, jammed its transponder signal and broadcast his own protest message for four and a half minutes,
described by Lin et al. as the first recorded cyberattack on a space system. No state involved.

Source: Lin et al., ‘Outer Space Cyberattacks: Generating Novel Scenarios to Avoid Surprise’, Cal Poly Ethics + Emerging Sciences Group, 2024.

Criminal penalty
$5,000 fine
1 year of unsupervised probation
Amateur radio license suspended for 1 year

Australia: ‘critical’ on paper, not yet in practice

The 2026 SOCI Act reforms add **space technology** as a recognised critical infrastructure asset class, alongside health, energy and research. On paper, satellites now sit next to dams and the power grid.

WATER & DAMS

CIRMP

Mandatory Critical Infrastructure Risk Management Program obligations are switched on: board-level accountability, periodic independent assurance, registered operators.

SPACE TECHNOLOGY

Defined — but no CRIMP

“The sector exists in legislation but has no operational content” (Nicholls, 2026) — no CIRMP switched on yet, despite Sky Muster serving 400,000+ homes and 200,000+ AU Starlink subscribers, including emergency services.

New Zealand's posture

GBSI regime

Outer Space & High-altitude Activities Amendment Act (2025) — ground-based space infrastructure operators need authorisation by 29 Jul 2026, or face NZ$250k fines.

GCSB & NZSIS

National security risk assessments sit inside the NZ Intelligence Community for all payloads and GBSI applications.

Operation Olympic Defender

NZ joined the US-led coalition on space-system resilience; posted a defence liaison officer to US Space Command.

RNZAF No. 62 Squadron

NZ's space squadron coordinates the Pacific regional cell of the Joint Commercial Operations space-domain-awareness programme.

09 — IMPLICATIONS

Everyone agrees space is critical. Nobody agrees who audits it.

	Is space formally ‘critical infrastructure’?	Audit / enforcement teeth
New Zealand	Not a CI sector — GBSI regime covers ground segment only	National security vetting (GCSB/NZSIS); no broad audit regime yet
Australia	Yes — space tech named as SOCI asset class (2026)	CIRMP not yet switched on for space
United States	No — not one of 16 CISA-designated CI sectors	SPD-5 gives voluntary cyber principles only; push for a 17th sector ongoing
United Kingdom	Yes — ‘Critical National Infrastructure’ since 2021 strategy	2026 defence review criticised for listing capabilities without prioritising them

We've built forty years of treaty law for states and their licensees. The first attacker was neither, and so is the next one.

So I Urge you…

Don’t forget the little guy:

Thank you for listening!

Ben | Victoria University of Wellington

13 August 2026

Bibliography

Novel attacks

Lin, P., et al. (2024). Outer Space Cyberattacks: Generating Novel Scenarios to Avoid Surprise. arXiv:2406.12041.

Policy Vs Obligation

Coco, A., & de Souza Dias, T. (2021). 'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law. European Journal of International Law, 32(3), 771–806. doi:10.1093/ejil/chab056.

Case Study

Kazi, A., Kazi, S., & Bhosale, S. (2025). Invisible Battlefields: Analyzing the Viasat Attack and its Broader Implications. Scientific Bulletin, 30(1), 59–67. doi:10.2478/bsaft-2025-0007.

Assisting Resources

NATO CCDCOE, "Viasat KA-SAT attack (2022)", UN – Outer Space Treaty , ARTEMIS Accords 2020, MITRE ATT&CK

Slide template Courtesy of LibreOffice Impress (Basically Open source powerpoint)
AI declaration : (local) Ai was used to help initally locate papers and to bounce some ideas while writing