Flinders University

Jeff Bleich Centre for Democracy and Disruptive Technologies

Protecting Australia: Counterspace Technologies and National Security Threats

Dr Rodrigo Praino
Dr Melissa de Zwart
Sumen Rai

MARCH
2026

Suggested Citation: Praino, R., de Zwart, M., Rai, S. (2026). “Protecting Australia: Counterspace Technologies and National Security Threats” Jeff Bleich Centre for Democracy and Disruptive Technologies, Flinders University, South Australia
DOI: https://doi.org/10.25957/dry3-bv32

jbc@flinders.edu.au

Table of Contents

1 INTRODUCTION

1.1 Background and Rationale

Space infrastructure critically underpins Western-style lifestyle and warfare, with associated space services being a critical enabler for a wide range of commercial and defence activities. Space assets constitute critical infrastructure, and its disruption represent an enormous threat to national security.

The 2020 Defence Strategic Update consistently states that assured access to space is critical to ADF warfighting effectiveness, situational awareness, and delivery of real-time communications and information. This is not new, as space technology has historically been used for intelligence gathering purposes, and more recently, during conflicts as a complement to existing weaponry.[1] This complementary use of space technology for modern militaries can take the form of precise navigation, missile guidance, and secure communication systems. Space technology has contributed to the establishment of trust by facilitating the verification of treaties, whilst simultaneously increasing geopolitical tensions, as dependence on space-based systems has been also increasing the vulnerability and value of space assets as possible targets.

The development of counterspace technologies is not new either. Since the 1960s, technologies for space control like Kinetic Physical Direct Ascent Anti-Satellite (DA-ASAT) have had a significant presence. However, it only recently that normalization of space as a military operational domain and the development of weaponry increased. Categories of threats have also broadened beyond DA-ASAT, with counterspace technologies including Non-Kinetic Physical, Directed Energy, Electronic, and Cyber.[2] Examples of these threats include the use of nuclear devices to produce an electromagnetic pulse (EMP) in a high-radiation environment (Non-Kinetic Physical), laser offensive systems (Directed Energy), jamming or spoofing of satellites (Electronic), and targeted attacks on data streams (Cyber).[3]

This is because the strategic value of space has grown considerably in the past decades as capabilities advance and nations grow increasingly dependent on space-based services, including for military operations. The extent of this integration was not seen through the Cold War, when geopolitical competition between the U.S. and the USSR culminated in an arms race in space. Despite a period of relative cooperation and collaboration that followed – with both countries partnering to develop the International Space Station (ISS) and wider international efforts emerging to limit the potential for another arms race in space – global tensions have resurfaced. The geopolitical context has however shifted and is now being shaped in part by advancing capabilities and the new level of

[1] Zulfikar Abbany, "Modern Spy Satellites in an Age of Space Wars," Dw.Com, August 26, 2020, https://www.dw.com/en/modern-spy-satellites-in-an-age-of-space-wars/a-54691887.

[2] Aerospace, "Counterspace Timeline, 1959-2022," Space Security, March 31, 2023, https://aerospace.csis.org/counterspace-timeline/.

[3] Swope et al., "Space Threat Assessment 2025," pp. 4-5.

societal and military integration with space-based assets.

In addition, the emergence of commercial actors as key stakeholders in the space sector raises new questions, including concerns about the security of space activities.[4] Russia's current conflict with Ukraine has been one of the most significant demonstrations of both the vulnerability of space assets and of the integration of commercial space capabilities in a conflict.[5] The introduction and contributions of a non-State space actor, SpaceX, in a geopolitical conflict came in the form of communication services. In parallel, the development of alternate forms of counterspace capabilities is expected to ramp up. Indeed, counterspace capabilities targeting single systems are not expected to have the power to dismantle constellations like Starlink, which contains more than 5,000 satellites.[6]

Without identifying the major threats to space infrastructure that are critical for Australian defence and economic activities, and without devising a set of possible responses to these threats, ADF will not be able to fulfill the goals set by the 2020 Defence Strategic Update.

1.2 Objectives of the Study

This project aims to identify the potential threats to space infrastructure that are critical for Australian defence and economic activities and elaborate possible responses. It will do so by developing robust and realistic space security scenarios applicable in an Australian regional context. Similar works to date (e.g., Schriever wargames, CSIS et al) take a US-centric approach. This study is designed to significantly increase both the quality and the quantity of discourse around the role of Defence and Government in space and, more broadly, on Australian space policy.

It will assist with Defence's ongoing objective of expanding Defence's capabilities in the space domain and devising a cohesive strategy to protect space infrastructure that enhances national preparedness and increases the resilience of the growing Australian space infrastructure. It will contribute to the elaboration of this strategy in two ways. First, it will provide the first Australia-centred comprehensive framework summarising the most common and developing types of threats to space infrastructure that Australia relies upon for critical military and economic activities.

Second, it will develop real-world Australia-centred scenarios that will then be tested against industry stakeholders in order to elaborate appropriate responses and actions for Australia to the threats devised.

Possible responses to space-centred attacks are complex to elaborate because no single organisation or agency possesses the full range of expertise required to explore the ramifications of attacks to space infrastructure in all relevant areas. Increasingly, a whole-of-

[4] Rishi Iyengar, "Starlink Ukraine: Why Elon Musk Is the Go-To Internet Provider," Foreign Policy, January 9, 2023, https://foreignpolicy.com/2022/11/22/ukraine-internet-starlink-elon-musk-russia-war/.

[5] Jonathan Beale, "Space, the Unseen Frontier in the War in Ukraine," BBC News, October 5, 2022, https://www.bbc.com/news/technology-63109532.

[6] Mike Stone and Joey Roulette, "SpaceX's Starlink wins Pentagon contract for satellite services to Ukraine," Reuters, June 1, 2023, https://www.reuters.com/business/aerospace-defense/pentagon-buys-starlink-ukraine-statement-2023-06-01/.

nation approach (Defence, Government, Industry, and Academia) seems essential.

Overall, the report aims to generate new insight on how to enhance Australia's strategic position in space. Given the specific scenarios that will be developed, it will be possible to identify how Defence and/or other particular Government agencies can contribute to increasing Australia's protection of its strategic space assets. In addition, it will be possible to use the information, data, and materials produced to design policy strategies and specific policy advice to Defence and other Government agencies.

1.3 Approach and Structure of the Report

In the United States, the Center for Strategic and International Studies (CSIS) has identified the broad spectrum of possible threats to space assets, and canvassed appropriate responses through the elaboration of possible scenarios presented to key stakeholders. Their work provided options on how the U.S. military and government should react to space-centred attacks, and guidance on capability development options. This project aims to build upon the CSIS-developed scenarios outlined in its 'Defence Against the Dark Arts in Space' report in order to produce the first Australia-centred effort to identify strategically-significant space vulnerabilities and provide Defence with evidence-based strategic policy advice resulting from independent research that will be able to influence and shape the Australian strategic policy debate and force development options.

Understanding the mechanics of space attacks requires expertise in conventional weaponry, physics and photonics, engineering, and cybersecurity, to name a few areas. It also requires technical expertise typically only possessed by satellite manufacturers and operators.

Responses to these attacks must address the international legal framework that regulates space activities, national legal constraints, and politico-diplomatic ramifications. As most space technologies are inherently dual use and many space operations now depend upon the private sector, these laws can give rise to complex networks of obligations and liabilities. The research team assembled to carry-out this project harnesses a multi-disciplinary group to address strategic policy and force development options in light of this complex and fast-changing environment.

The report is organised in four main sections. The first will provide an overview of the governance framework[7] set up at Commonwealth level to deal with space security issues and of the relationship between Australia's legal and policy framework and the governmental actors that operate such framework. The section will more specifically cover the top-level governmental structures at Commonwealth level and describe their main responsibilities. It will then analyse the most important policy and legal documents and implementation frameworks, by looking in particular at documents that set out strategic orientations at governmental level or those specifying the actions undertaken by the various stakeholders to implement the strategic orientations of the above documents. The section will also

[7] Governance in this context refers to the organisational framework set up to materialise and operate such policies, evidencing which bodies, agencies and departments are responsible for implementing and supervising certain guidelines, in a coherent and efficient structure with clear and determinate attributions.

review Australian capabilities in the sector and international cooperation channels.

The second section will provide considerations of the current global state of both offensive and defensive counterspace capabilities – from major spacefaring states to the current growth from other actors. It will also provide considerations for Australia and develop a matrix of possible offensive and defensive measures.

In the third part, the report will deploy four real-world Australia-centred scenarios that will then be tested against institutional, industrial and academic stakeholders in order to elaborate appropriate responses and actions for Australia to the threats devised.

In the final part, the report will summarise key findings and propose a set of possible pathways to assist with Defence's ongoing objective of expanding Defence's capabilities in the space domain while devising a cohesive strategy to protect space assets that enhances national preparedness and increases the resilience of the Australian space infrastructure.

2 THE AUSTRALIAN PERSPECTIVE

2.1 National Governance

Australia's close diplomatic relationship with the United States has resulted in a similar division of military forces and bodies.[8] Following the 100th anniversary of the Royal Australian Air Force (RAAF) in March 2021, it was announced that Australia's Defence Space Command (DSpC) would be established.[9] In January 2022, the DSpC was formally organised and RAAF Vice-Marshal Catherine Roberts was sworn in as Defence Space Commander.[10] As of June 2024, Major General Greg Novak, AM, was appointed as Defence Space Commander.[11]

The main organisations that collaborate on space defence issues in Australia are:

- Australian Defence Force (ADF) – including the RAAF, the Australian Army, the Royal Australian Navy (RAN) and the Australian Public Service Commission (ASPC) – contribution to operational preparation.
- Australian Space Operations Centre (AUSSpOC) – prioritisation of operational coordination and international relations.
- Australian Space Agency (ASA) – Whole-of-Government coordination, and identification of dual-use technologies for civil and military use.
- National Security Space Inter-Departmental Committee (NSSIDC) – coordination of priorities and trade-offs, and development of national security science and technology.

The DSpC operates as a single point of contact for all external agencies seeking information on the Space domain due to the Whole-of-Government approach.[12] Australia's current governance and reporting processes for the DSpC involve a variety of governmental organisations, including the Department of Foreign Affairs and Trade (DFAT) and the Department of Industry, Science, and Resources (DISR). The NSSIDC, co-chaired by DFAT and the Department of Defence (DoD), is a working group of the Space Coordination Committee (SCC) specifically aligned to assist with identifying civil Space issues that intersect with national security.[13]

[8] Tristan Moss, "The Space between Alliance and Self-Reliance: The Evolution of the Australia-US Defence Space Relationship," United States Studies Centre, August 28, 2023, p. 6. https://www.ussc.edu.au/the-evolution-of-the-australia-us-defence-space-relationship.

[9] Andrew Greene, "RAAF Planning for New Military Space Command as It Celebrates 100th Anniversary," ABC News, March 30, 2021, https://www.abc.net.au/news/2021-03-31/raaf-looks-to-space-as-it-celebrates-100-years/100039914.

[10] Andrew Greene, "Royal Australian Air Force Air Vice-Marshal Catherine Roberts to Become Australia's First Space Commander," ABC News, May 7, 2021, https://www.abc.net.au/news/2021-05-08/air-force-vice-marshal-catherine-roberts-australia-space-command/100124660.

[11] Andrew McLaughlin, "Founding Head of Defence Space Command Hands over to New Leader," PS News, December 22, 2023, https://psnews.com.au/founding-head-of-defence-space-command-hands-over-to-new-leader/125008/.

[12] Department of Defence, "National Defence: Defence Strategic Review 2023," pp. 31-33.

[13] Australian Space Agency, "State of Space 2021," Australian Space Agency, July 1, 2022, p. 51. https://www.space.gov.au/about-agency/publications/state-space-2021.

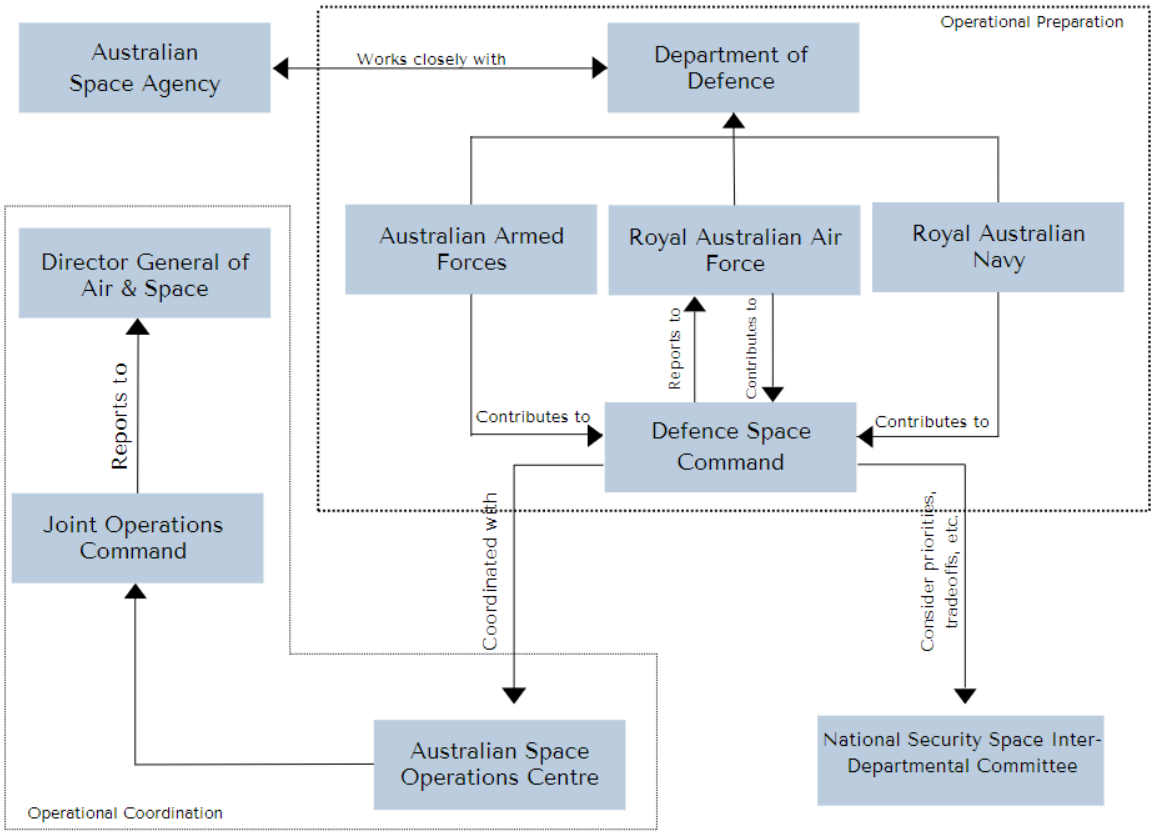

Figure 1: Overview of the Australian Space defence governance

Defence Space Command (DSpC)

The DSpC is a new addition to the role of the DoD in Australia. Following its establishment in 2022, the DSpC has pursued four goals:

- Develop and advocate for Space specific priorities across Whole-of-Government, industry, allies, and international partners.
- Create, train, and sustain Australians. Assign trained Space specialists to the Chief of Joint Operations when needed.
- Conduct strategic Space planning, assist in the development of refinement of Space policy, guide scientific and technological Space priorities, define a resilient and effective Space architecture in close collaboration with allies.
- Ensure the design, construction, maintenance, and operation of Defence Space capabilities are in accordance with Defence standards and limitations.

To achieve these goals, the DSpC is working in conjunction with the previously mentioned military departments, Government bodies, and other agencies.[14] As part of an integrated Whole-of-Government approach to Space, the DSpC at first reported to the Chief of Air Force, whilst working in a joint force with the RAN, Australian Army, and the APSC to address

[14] Belinda Smith, "What Is Australia's Space Division, and Why Is It in the Military?" ABC News, May 13, 2021, https://www.abc.net.au/news/science/2021-05-13/australia-space-division-military-satellites-air-force-commander/100127978.

preparation of future military operations.[15] The Whole-of-Government approach is significant as the DSpC is also engaging with a workforce that includes public servants and individual contractors from external agents to provide alternate views. However, the DSpC was not established as a new branch of military, unlike the U.S., with the division rather formed similarly to the United Kingdom Space Command. Another priority chosen for the DSpC was Space Traffic Management (STM), as it was established as a threat to safety and security by the DoD.[16] The 2020 Force Structure Plan outlined an AUD $7 billion investment into key areas identified by the DoD for contributions to war fighting outcomes.[17] War fighting contributions include Space Domain Awareness (SDA), Satellite Communications and Assurance, and Terrestrial Operations in Contested Space.[18]

The DSpC was moved from the Royal Australian Air Force to the Joint Capabilities Group (JCG) on 1 July 2023.[19] The JCG consists of the Space, Cyber, and Defence Networks and aims to 'prepare Space and Cyber Power, and Logistics capabilities, in order to enable the integrated force in competition and conflict'.[20] The DSpC is recognised as the space domain lead and reports to the Chief of Joint Capabilities.[21]

The No. 1 Space Surveillance Unit (1SSU) is the first dedicated Joint Space Unit in Australia.[22] 1SSU commenced operation of Defence's space domain awareness capabilities in January 2023 at RAAF Base Edinburgh.[23] The C-Band Radar and Space Surveillance Telescope located in Exmouth, Western Australia, are the 1SSU's key operational capabilities.[24] The C-Band Radar and Space Surveillance Telescope are joint initiatives between the United States Air Force and the Australian Defence Force.[25]

On 1 September 2023, DSpC joined the Joint Task Force - Space Defence Commercial Operations (JCO), which is 'a U.S. Space Force-led initiative that utilises commercial providers to deliver diverse, timely space domain awareness (SDA) capabilities and drive critical partnerships'.[26] As part of this initiative, 1SSU will commence 'site lead duties' which

[15] Royal Australian Air Force, "Defence Space Strategy - Defence Space Power eManual," Defence Space Command, 2022, p. 19. https://www.airforce.gov.au/our-work/strategy/defence-space-strategy.

[16] Australian Space Agency, "Real-time traffic management in space," Australian Space Agency, n.d., https://www.space.gov.au/real-time-traffic-management-space.

[17] Department of Defence, "2020 Force Structure Plan," Defence Strategic Planning, 2020, p. 63. https://www.defence.gov.au/about/strategic-planning/2020-force-structure-plan.

[18] Ibid.

[19] Department of Defence, "Joint Capabilities Group", https://www.defence.gov.au/about/who-we-are/organisation-structure/joint-capabilities-group.

[20] Ibid.

[21] Ibid.

[22] Peter O'Rourke, "A big day for the space domain", Department of Defence (3 July 2023) https://www.defence.gov.au/news-events/news/2023-07-03/big-day-space-domain.

[23] Ibid.

[24] Ibid.

[25] Department of Defence, "Australia's Space Surveillance Radar reaches Full Operation Capability" (7 March 2017) https://www.minister.defence.gov.au/media-releases/2017-03-07/australias-space-surveillance-radar-reaches-full-operational-capability.

[26] Bridget Bonnette, "Defence Space Command Joins JCO global construct", US Space Command (1 September 2023) https://www.spacecom.mil/Newsroom/News/Article-Display/Article/3514330/defence-space-command-

will lead to JCO-Pacific in order to 'provide timely SDA contribution to the global space community as part of a planned broader Pacific Cell'.[27] The JCO aspires to become a global system and operate across the three regional cells of America, Pacific, and Meridian.[28]

Australian Space Operations Centre (AUSSpOC)

Australia has established a Space Command and force structure those established in its allies of the AUKUS partnerships. As the U.S. separated preparation and implementation of operations between two military Space entities, so has Australia. The implementation and coordination of efforts, along with the exchange of expertise, will be performed by AUSSpOC, like the missions of the U.S. Space Command. However, like what happens in the UK, the two Space entities are still contained within an existing military structure, as the DSpC reports to the RAAF, and AUSSpOC was put under the responsibility of Commander Joint Operations Command (CJOPS). This decision was made by the Director General of Air and Space for increased interoperability across all domains, including Space. [29]

AUSSpOC was considered a turning point for Australia in Space. Working in conjunction with the DSpC. AUSSpOC's responsibilities for planning and executing Space control measures, and integration and coordination of Space operations will support joint forces, including the Joint Operations Command (JOPS).[30] AUSSpOC is hosted by JOPS and will report to the Director of General Air and Space. One of the missions overseen by AUSSpOC is Operation Dyurra, with Dyurra being the word for 'stars' in the Indigenous Australian Ngunnawal language.[31] This operation is part of Australia's contribution to the United States-led Operation Olympic Defender, which aims to provide Space support to all contributing nations.[32] Australia is also a member of the Combined Space Operations Initiative (CSpO), alongside the United States, United Kingdom, New Zealand, Canada, France, Germany, Italy, and Norway. In this context, AUSSpOC was nominated as the organisation representing Australia and coordinates multilateral Space engagement and integration on an international scale.

Australian Space Agency (ASA)

With a growing space sector, 2018 saw the Australian Government establish the Australian Space Agency (ASA). The ASA works in partnership with the National Aeronautics and Space

joins-jco-global-construct/; Department of Defence, "Following the sun for space domain awareness" (1 September 2023) https://www.defence.gov.au/news-events/news/2023-09-01/following-sun-space-domain-awareness.

[27] Bridget Bonnette, "Defence Space Command Joins JCO global construct", US Space Command (1 September 2023) https://www.spacecom.mil/Newsroom/News/Article-Display/Article/3514330/defence-space-command-joins-jco-global-construct/.

[28] Department of Defence, "Following the sun for space domain awareness" (1 September 2023) https://www.defence.gov.au/news-events/news/2023-09-01/following-sun-space-domain-awareness.

[29] Royal Australian Air Force, "Defence Space Strategy - Defence Space Power eManual," p. 20.

[30] Department of Defence, "Organisation structure," Who we are, n.d., https://www.defence.gov.au/about/who-we-are/organisation-structure.

[31] Department of Defence, "Operation Dyurra," Defence Activities, n.d., https://www.defence.gov.au/defence-activities/operations/dyurra.

[32] Royal Australian Air Force, "Defence Space Strategy," p. 12.

Administration (NASA) on the Moon to Mars Initiative and with other Australian industry partners to progress Australia's Space influence.[33]

Since its creation, the Australian Space Agency (ASA) has worked primarily in the civilian Space policy and activity domain. ASA has also been an important decision-maker regarding the use of Space, international cooperation, and key strategic areas of development. In conjunction with the Australian Civil Space Strategy,[34] ASA works towards the Whole-of-Government approach, coordinating the various governmental organisations that also contribute to Space power elements. These organisations include Geoscience Australia, the Bureau of Meteorology, and the Commonwealth Scientific and Industrial Research Organisation (CSIRO).[35] The civil nature of ASA does not limit its involvement in the military field, as developments in dual-use technologies has enabled both civil and military capability, and as ASA maintains a close working relationship with the DoD. The two organisations developed technical roadmaps to ensure a complementary growth of the Space sector between its civil and military dimensions.[36] One of these roadmaps include the combined development of robotics, automation, and Artificial Intelligence (AI) for both commercial and military capability.[37] A Memorandum of Understanding (MoU) was also signed in 2023 between ASA and the DoD subdivision Defence Aviation Safety Authority (DASA), with the intent to regulate Space safety for both civil and defence-focused activities.[38]

Department of Defence (DoD)

The DoD has been maintained as the primary responsive body for existing and future Space capabilities. As previously mentioned, the Defence Space Strategy released in 2022 establishes Lines of Effort (LOEs), which are goals that the DoD specifically needs to review and achieve to contribute to a greater military presence in the Space domain. With the introduction of the DSpC, LOE 1 has been achieved, and LOE 2 and 3 are part of the short-term outcomes sought after by the DoD (for full list of LOEs, please refer to section '2.1 Policies and Strategies').[39]

The DoD maintains a strategic role in the Space sector. Responsibility for operations and/or utilisation of Space capabilities, which include Positioning, Navigation and Timing (PNT), Satellite Communications (SATCOM), Intelligence, Surveillance and Reconnaissance (ISR), and Space Domain Awareness (SDA), are performed by the DoD. Project management is organised through sub-groups such as DASA and the Defence Science and Technology

[33] Australian Space Agency, "Advancing Australia's position in the global space economy," Moon to Mars Initiative, n.d., https://www.space.gov.au/moon-mars-initiative.

[34] Department of Industry, Science and Resources, "Australian Civil Space Strategy 2019-2028," Data and Publications, April 1, 2019, https://www.industry.gov.au/publications/australian-civil-space-strategy-2019-2028.

[35] Royal Australian Air Force, "Defence Space Strategy - Defence Space Power eManual," p. 22. https://www.airforce.gov.au/our-work/strategy/defence-space-strategy.

[36] Australian Space Agency, "State of Space 2021," p. 50.

[37] Australian Space Agency, "Robotics and Automation on Earth and in Space Roadmap," Australian Space Agency, January 24, 2022, p. 16. https://www.space.gov.au/about-agency/publications/state-space-2021.

[38] Barrie Bardoe, "Making Space Safer," Department of Defence News, 27 March, 2023, https://www.defence.gov.au/news-events/news/2023-03-27/making-space-safer.

[39] Royal Australian Air Force, "Defence Space Strategy," p. 37.

Group (DSTG). The DSTG operations include the Resilient Multi-Mission Space is for the purpose of increased Space-based surveillance capabilities for intelligence and Space Surveillance Awareness (SSA) purposes.[40] The civilian capabilities that are part of the DoD's role due to their dual-use nature include Geospatial Intelligence and SSA.[41] As outlined in the Defence Space Strategy, the DoD is charged with maintaining the previously existing agreements, relationships, and prospective future of the Space domain more than the DSpC.

2.2 Policies and Strategies

Key documents for Australian Space Defence:

In order of publication release:

- Defence Strategic Review (2020)
- Force Structure Plan (2020)
- Defence Strategic Update (2020)
- Defence Space Strategy (2022)
- National Defence: Defence Strategic Review (2023)
- National Defence Strategy (2024)

In recent years, Australia has been improving its defence capacities due to the changing scope of the Indo-Pacific Region. For Australia, shifting its posture means increasing international partnerships to strengthen the region to create a free and open Indo-Pacific that is secure and stable.[42] Australia has stated its intentions with the publication of the National Defence Strategy (2024), the Defence Space Strategy (2022) and the Defence Strategic Review (2020). Further investing in national industry partners and boosted training programs for all levels has increased the Budget (FY 2023-2024) for the Space sector. The increase in international partnerships include AUKUS (Australia, the United Kingdom, and the United States), the QUAD (Australia, the United States, India, and Japan), and the Memorandum of Understanding (MoU) with New Zealand.

Australia's Defence and Strategy

The Defence Space Strategic Update, published in July 2020, was Australia's catalyst of many recent official documents which provide an in-depth explanation of the country's intentions for the Space sector. On the same month the Department of Defence (DoD) published the Force Structure Plan. The two 2020 reports have the same focus – strengthening Australia's Defence plan. The Defence Strategic Update focuses on new policy strategies for national Defence and what new capabilities to invest in. Meanwhile, the Force Structure Plan details how to implement the new investments into the national Defence plan. Whilst both documents have big intentions for Australia in the Space sector, collectively they only set intentions

[40] Defence, Science and Technology Group, "Resilient Multi-Mission Space," DST Strategy 2030, n.d., https://www.dst.defence.gov.au/strategy/star-shots/resilient-multi-mission-space.

[41] Department of Defence, "Geospatial intelligence services," Products and services, n.d., https://www.defence.gov.au/defence-activities/products-services/geospatial-intelligence-services.; Tristan Moss, "The Space between Alliance and Self-Reliance: The Evolution of the Australia-US Defence Space Relationship," United States Studies Centre, August 28, 2023, p. 30. https://www.ussc.edu.au/the-evolution-of-the-australia-us-defence-space-relationship.

[42] Prime Minister of Australia, "Joint Leaders Statement on AUKUS," Joint Statement, March 14, 2023, https://www.pm.gov.au/media/joint-leaders-statement-aukus.

related to 'investing in Defence's Space related capabilities' and 'improving in allied partnerships' without providing any recommendation structured plan.

In April 2023, the Australian Government commissioned one of the most ambitious defence documents since those released in the Cold War era.[43] The National Defence: Defence Strategic Review is a comprehensive review of Australia's current defence situation with details on their allies, potential threats, and goals they aim to achieve to better prepare the nation considering the changing climate of the Indo-Pacific region.[44] The Review states that Defence must develop the cyber and Space capabilities spanning maritime, land, and air departments, which is reflected in the most recent 2023-2024 Australian National Budget. The Defence Strategic Review consistently made the point of a 'Whole-of-Government' approach which encapsulates not just the Australian Government working as one entity on the same goals but a Whole-of-Nation understanding for the future of Australia.[45] The Defence Strategic Review was written and published to illustrate the Governments intentions for Australia moving forward. Hence, education and increased industry training are a general focus, with specific reference to the Space sector by defining career pathways.

In 2024 Australia released the National Defence Strategy (NDS) and the 2024 Integrated Investment Program (IIP)[46], which provide a framework for the evolution of the Australian Defence Force (ADF) from a balanced force to an "integrated, focused force", across the five key domains (land, air, maritime, space and cyber) through a "coherent, logical and affordable plan". The NDS aims to ensure the ADF's five primary tasks are achieved being: defend Australia and immediate region; deter through denial any potential adversary attempt to project power against Australia through Australia's northern approaches; protect Australia's economic connection to the region and the world; contribute with partners to the collective security of the Indo-Pacific; and contribute with partners to the maintenance of the global rules-based order.

This evolution is focused along three epochs. Firstly, the "Enhanced Force-in-Being" which will see immediate enhancements on current forces by 2025. For the period of 2026-2030 there will be the "Objective Integrated Force", which will see the advancement of essential capabilities. Finally, from 2031 and beyond, the "Future Integrated Forces" will be the evolved ADF fit for purpose to respond to evolving challenges. This will be facilitated through an increase in defence funding, with an additional $7.3bn over the next four years, $50.3bn over the next decade, resulting in an estimated increase of $100bn by 2033/34, with a total funding of $765bn over the next decade. The IIP highlighted eleven capability investment priorities and their total expenditure until 2033/34: undersea warfare ($63bn-$76bn); maritime capabilities for sea denial and localised sea control operations ($51bn-$69bn); targeting and long-range strike ($28bn-$35bn); space and cyber ($27bn-$36bn); amphibious capable combined-arms land system ($36bn-$44bn); expeditionary air operations ($28bn-$44bn);

[43] Rod Mcguirk, "Australia Plans Major Overhaul of Defences as China Rises," AP News, April 24, 2023, https://apnews.com/article/australia-defense-strategic-review-china-be313bcbd58e6793a8c85b79682c0e34.

[44] Department of Defence, "National Defence: Defence Strategic Review 2023," Reviews Inquiries, 2023, https://www.defence.gov.au/about/reviews-inquiries/defence-strategic-review.

[45] Ibid., pp. 31-33.

[46]Department of Defence, "National Defence Strategy", 2024, https://www.defence.gov.au/about/strategic-planning/2024-national-defence-strategy-2024-integrated-investment-program

missile defence ($14bn-$18bn); theatre logistics ($15bn-21bn); theatre command and control ($11bn-$15bn); guided weapons and explosive ordnance ($16bn-$21bn); enhanced and resilient northern bases ($14bn-$18bn). Further defence expenditure will go towards Advanced Strategic Capabilities Accelerator ($3.6bn-$3.8bn) enterprise infrastructure ($17bn-$22bn) and enterprise data and ICT ($8.5bn-$11bn).

The cornerstone of Australian defence strategy is the newly introduced Strategy of Denial (SoD). This prioritises deterrence as the key strategic defence strategy for future ADF capabilities. This is a clear shift of the previous strategic defence objectives of shaping Australia's strategic environment, deterring actions against Australia's interest, and responding with credible military, which were weighted equally. The SoD will look to deter conflict prior to its inception, avoid foreign coercion, support regional prosperity and uphold regional balance. This will be done through increasing capacity building exercises with like-minded nations, especially within the Indo-Pacific and the U.S. ADF is strongly focused on ensuring international law and norms of the rule-based order are upheld throughout the Indo-Pacific. Australia, being a medium power State, benefits from their partnerships with other nations, and clear focus is given on ensuring current security relationships are upheld. This will be done through the continued development of Australia's multilateral, bilateral and trilateral agreements and partnerships such as the AUKUS agreement.

Focus has been given on the continued evolution of the ADF through the investment into personnel as well as innovation, science and technology. Currently the ADF is 4,400 personnel below strength, and budget has been provided to ensure greater retention on staff, as well as enhancing recruitment processes. The investment into next-generation capabilities of the ADF is being conducted through innovation, science and technology. The support of this sector will be a key pillar in ensuring Australia is able to adequately respond to the changing security environment.

The updated NDS and rebooted IIP sets out Australia's defence objectives for the future. This has a strong focus on increasing regional dialogue, enhancing strategic partnerships, and focusing on deterrence models to ensure international law and rule-based principles are upheld.

The Conceptual Delivery of Intentions

The Defence Space Strategy was published in 2022 by the DoD.[47] This document has a similar structure to the previous 2020 documents with a newly stated 2040 goal. This goal is backed by a year-by-year project plan, and a strong strategy with Lines of Effort (LOEs) which demonstrate how the Australian Government will be working toward being a stronger Space capable nation.

The key LOEs from The Defence Space Strategy which the DoD are working towards are:

[47] Royal Australian Air Force, "Defence Space Strategy," Defence Space Command, 2022, https://www.airforce.gov.au/about-us/defence-space-command.

1. ENHANCE DEFENCE'S SPACE CAPABILITY TO ASSURE JOINT FORCE ACCESS IN A CONGESTED, CONTESTED AND COMPETITIVE SPACE ENVIRONMENT.

This LOE has a foundational objective that calls on the Australian authorities to plan, organise, and act in the Space domain to strengthen Australia's sovereignty (1a-1b). Also to enable reliability on incentivising the use of Space for developing military purposes and gaining an understanding of Space as a critical infrastructure (1c-1f).

2. DELIVER MILITARY EFFECTS INTEGRATED ACROSS WHOLE OF GOVERNMENT AND WITH ALLIES AND PARTNERS IN SUPPORT OF AUSTRALIA'S NATIONAL SECURITY.

LOE 2 addresses governance aspects at a ministerial level with a holistic Governmental understanding to prioritise national Space capabilities (2a-2c). With a vertical basis through all Government levels, military, and regional partners, it will provide a focus on allies, partners, and a Whole-of-Government approach to raising awareness of Space capabilities (2d-2e).

3. INCREASE THE NATIONAL UNDERSTANDING OF THE CRITICALITY OF SPACE.

This LOE promotes the requirement of periodically reviewing the goals set by Defence in the roadmap and redirect where necessary (3a). It also promotes the safe and responsible use of Space with the Whole-of-Government, international partners, and the global domain (3b).

4. ADVANCE AUSTRALIAN SOVEREIGN SPACE CAPABILITY TO SUPPORT THE DEVELOPMENT OF A SUSTAINABLE NATIONAL SPACE ENTERPRISE.

Cooperation with other Australian departments including Defence actors to get Australia prepared with technology and innovation for when it is needed is promoted in LOE 4 (4a-4c). A specific focus is placed on developing and preserving the longevity of the Australian Space industry (4d-4f).

5. EVOLVE THE DEFENCE SPACE ENTERPRISE TO ENSURE A COHERENT, EFFICIENT AND EFFECTIVE USE OF THE SPACE DOMAIN.

The last LOE promotes organisational and strategic aspects of Australia in Space at a Defence level (5a-5c). It emphasises the goal of investing in a workforce plan to upskill training, keep personnel, stay updated and prepare the nation for the future with Space as a warfighting domain (5d-5e).[48]

The basic outline of the 2040 goal, as stated in the publication, is as follows:

Epoch	Foundation	Evolve	Mature
Focus	• Organisation • Concepts, roadmaps, architecture & plans. • Whole-of-Government integration. • Understanding of Space • Industry engagement.	• IIP Delivery: SATCOM, SDA, Space Control, Space ISR. • Integrated Space Control effects. • Industry Partnership. • Strengthened allied integration. • Architecture transformation.	• Mature workforce capability and capacity. • Space architecture transformation complete. • Additional Space capability. • Sustainable sovereign Space enterprise.
Timeframe	2021 – 2023	2024 – 2030	2031 – 2040

Table 1: Defence Space Strategy's 2040 goal.

Australia as a Launching State: The Launches and Returns Act 2018

Australia's advantageous geographic location has already provided a key role in the space sector as a launching State, primarily for suborbital flights. In possession of two permanent launch sites and five temporary but functional locations (which will be discussed), there has also been a push for an additional two sites.[49] Thus far, these launching sites have only taken either Australian-owned or U.S. (NASA) payloads. Yet there is an increasing demand in the market for launch sites with geolocation advantages, which would further grow Australia's position as a Space capable State.

In order to fulfil its obligations under international space law , Australia enacted the Space Activities Act 1998,[50] to regulate domestic space activities.

The Act introduced a set of permits related to various space activities; space license, launch permit, overseas launch permit, return authorisation, and an exemption certificate. Every separate licence has distinct and specific conditions per type of activity.[51] It also introduced a series of federal criminal offences related to these licensing regimes.

[48] Royal Australian Air Force, "Defence Space Strategy," pp. 17-34.

[49] Bec Shrimpton, "The Time Is Right for Australia to Re-establish Its Reputation as a Global Space Power," The Strategist, June 7, 2021, https://www.aspistrategist.org.au/the-time-is-right-for-australia-to-re-establish-its-reputation-as-a-global-space-power/.

50 Federal Register of Legislation, 1998, "Space Activities Act 1998", Available at: https://www.legislation.gov.au/Details/C2004C01013#:~:text=to%20establish%20a%20system%20for,regulated%20by%20this%20Act%3B%20and

51 Annette Froehlich and Vincent Seffinga, National Space Legislation (Springer, 2018) vol 15, Studies in Space Policy (Annette Froehlich and Vincent Seffinga eds)

In response to industry feedback, a major review of the legislation was undertaken in 2016-2017, in the context of increasing space activities by Australian startups and academia. The Space Activities Amendment (Launches and Returns) Act 2018 introduced a range of reforms intended to support Australian innovation and participation in space activities, whilst continuing to enforce Australia's obligations under international law.[52] Key elements of the reform were intended to support new technologies and capabilities, such as launches from aircraft in flight and launches of high-power rockets, by reducing barriers and bureaucracy for the new actors, simplifying approval processes, lowering insurance requirements, and expanding the regulatory frameworks to include those new technologies.[53]

The 2018 revisions served to modernise the Space Activities Act, and enacted significant changes, especially regarding insurance requirements, regulations of launches from aircraft and high-power rockets,[54] amendments to the overall penalties,[55] and the inclusion of a mandatory Debris Mitigation Strategy[56] when applying for a Launch Permit and an overseas payload permit.

In case of accidents[57] or incidents,[58] involving a space object or high powered rocket launched from or returned to a facility in Australia or from an aircraft that is in the airspace over Australian territory, the Minister for Industry and Science must appoint a person with suitable qualifications and experience as the Investigator of the accident to analyse the circumstances surrounding the relevant fact. In this point is valuable to highlight that immediately after an accident occurs, the Australian launch permit, Australian high power rocket permit, return authorisation or authorisation certificate under which the relevant launch or return was carried out is taken to be suspended and will only be resumed with the Minister's revoke of suspension, making it essential for the company implicated in the accident or incident to fully cooperate with the investigations.

The purpose of the investigation is not to apport blame or determine the liability of any person, but to, by scrutinizing the circumstances surrounding any accident or incident, prevent others from happening. When the completion of the investigation, the Minister must be provided with a written report and any other relevant documents that it required, this report does not necessarily may be published, however, the Minister may opt for partial or total divulgation if considers in the interest of promoting safety in the space industry.

The Security of Critical Infrastructure Act 2018

52 Federal Register of Legislation, 2018, Space (Launches and Returns) Act 2018, Available at: https://www.legislation.gov.au/Details/C2021C00394

53 Ian McGill and Connie Ye, "The Launches and Returns Act: one of the most significant updates to the Space Activities Act since its implementation", https://www.allens.com.au/insights-news/insights/2019/09/the-launches-and-returns-act-one-of-the-most-significant-updates-to-the-space-activities-act-since-its-implementation/

54 Space (Launches and Returns) Act 2018 (Cth), pt 3, div 4.

55 Space (Launches and Returns) Act 2018 (Cth), pt 3, div 1 and pt 6.

56 Space (Launches and Returns) Act 2018 (Cth), Pt 3, div 3.

57 Space (Launches and Returns) Act 2018 (Cth), s 85.

58 Space (Launches and Returns) Act 2018 (Cth), s 86.

The Security of Critical Infrastructure Act 2018[59] created an initial framework for managing risks to national security relating to critical infrastructure, it provided a series of obligations to critical technology administrators, such as the necessity of keeping information related to critical infrastructure assets, to provide certain information in relation to it, and to proceed to notify if certain events occurred concerning the asset.

The Act also created some powers for the Minister for Home Affairs, allowing it to require certain entities relating to a critical infrastructure asset to do, or refrain from doing, an act or thing if the Minister is satisfied that there is a risk of an act or omission that would be prejudicial to security; and Secretary of the Department of Home affairs, allowing it to require certain information or documents, and to undertake an assessment to determine if there is a risk to national security relating to critical infrastructure assets.

The initial four areas determined to be critical infrastructure assets under this Act, were electricity, ports, water, and gas. [60]

Recent amendments to this Act by the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022, expanded coverage to 11 sectors, including communications, data storage or processing, space technology and defence industry, in order to adapt to the complex national security risks of sabotage, espionage and coercion posed by foreign involvement in Australia's critical infrastructure.

In this new version, the Act enhances the powers of the Minister and Secretary, builds a clearer picture of critical infrastructure ownership and control in high-risk sectors, in a Register of Critical Infrastructure Assets, and requires responsible entities to create, and follow, a critical infrastructure risk management program. It also pays special attention to cyber threats, instituting a mandatory cyber incident reporting to the ACSC within a determined time frame, and providing government assistance as a last resource if an asset experienced a serious cyberattack and did not possess the means to respond efficiently.

2.3 International Agreements and Cooperation Frameworks

International collaboration allows for the sharing of resources and expands Australia's capabilities in space. For Australia it has been historically important to advance its position for innovation, exploration, and sustainability in a collaborative manner. With the increasing need for Space Situational Awareness (SSA), alliances bolster the nation's safety and innovation abilities.

International Treaties

Treaty Name	Signed by Australia	Year Implemented
Principles on Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies (Outer Space Treaty (OST))	ü	1967

59 Federal Register of Legislation, 2018, Security of Critical Infrastructure Act 2018, Available at: https://www.legislation.gov.au/Details/C2018A00029

60 Ibid. Section 9 (1) and Section 51 (1).

Treaty Name	Signed by Australia	Year Implemented
The Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched in Outer Space (ARRA)	ü	1968
The Convention of Liability for Damage Caused by Space Objects (LIAB)	ü	1972
The Registration of Object Launched into Outer Space (REG)	ü	1974
Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (The Moon Agreement)	ü	1979
Comprehensive Nuclear Test Ban Treaty (CTBT) (not in force)	ü	1998
Square Kilometre Array Observatory (SKAO) (entered into force in 2021)	ü	2020

Table 2: Overview of treaties signed by Australia, sorted by year implemented.

Australia was one of the 18 original members of the Committee on the Peaceful Uses of Outer Space (COPUOS). Instrumental in the creation of the five treaties of Outer Space, COPUOS was tasked with studying arising legal problems due to the exploration of Space, encouragement of research programs, and promotion of the use of the cosmos for the benefit of all. The COPUOS Secretariat is held by the United Nations Office for Outer Space Affairs (UNOOSA), bringing together United Nations delegates to aid in adopting resolutions on international cooperation in Space. However, COPUOS does not deal with Space security matters and rather addresses safety and sustainability issues.[61]

Bilateral Agreements

Agreement Name	Agreement Type	Country Involved	Year Signed
Agreement on the cooperation in the sphere of research and peaceful use of Outer Space	Research Agreement	Russia	2004
Artemis Accords	Outline of Principles	United States	2020
Memorandum of Understanding	Cooperation Agreement	India	2021
Space Bridge	Trade Agreement	United Kingdom	2021
Memorandum of Understanding	Cooperation Agreement	United States	2023
Memorandum of Understanding	Cooperation Agreement	New Zealand	2024

Table 3: Overview of bilateral agreements signed by Australia, sorted by year signed.

[61] United Nations Office for Outer Space Affairs, "Committee on the Peaceful Uses of Outer Space," Secretariat of COPUOS, n.d., https://www.unoosa.org/oosa/en/ourwork/copuos/index.html.

Australia has signed several bilateral agreements relating to Space affairs with different partners. The most recent one was a MoU signed between ASA and the New Zealand Space Agency (NZSA), along with the SmartSat Cooperation Research Centre, on February 1, 2024.[62] A new joint research initiative between the two States has been organised, and the leading Space research organisations who have pledged to work on three objectives:

- Earth Observation covering – biosecurity, crop health, pasture condition, emission monitoring, and Maritime Domain Awareness.
- Space Situational Awareness (SSA) – developing new technologies and techniques to monitor orbital movement.
- Optical Communications – working on a joint adaptive optics to explore a network of Australasian optical ground stations which can actively support Space exploration.[63]

The Artemis Accords, created by the U.S. Department of State and NASA, are a series of bilateral agreements. These include principles that signatories are to follow in their current projects, particularly through the Artemis program.[64] The key points of this document include transparency of exploration, registration of Space objects, deconfliction of activities, and protection of the historically significant evidence of human activity in Space.[65] The Accords were signed by Australia in October 2020. Australia has always maintained the position that the Artemis Accords are consistent with Australia's international obligations.[66] At the 63rd session of the COPUOS Legal Subcommittee held in April 2024, Australia stated that:[67]

> *'Australia considers that the Artemis Accords are consistent with Australia's international obligations. Australia considers that the Moon Agreement and the Artemis Accords provide frameworks that will guide and enable Australia's planned future activities on the Moon.'*

The Artemis Accords are not a treaty, although they now have over 50 signatories This means that their provisions do not constitute international law. It should also be noted that China is

[62] Alison Bowman, "SmartSat and New Zealand Space Agency Collaborate on Joint R&D Initiatives to Advance Space Sector Innovation - SmartSat CRC," SmartSat CRC, January 30, 2024, https://smartsatcrc.com/smartsat-and-new-zealand-space-agency-collaborate-on-joint-rd-initiatives-to-advance-space-sector-innovation/.

[63] Australian Space Agency, "Trans-Tasman collaboration to advance space sector innovation," Australian Space Agency, January 31, 2024, https://www.space.gov.au/news-and-media/trans-tasman-collaboration-advance-space-sector-innovation.

[64] Australian Space Agency, "Team Artemis Australia," Australian Space Agency, n.d., https://www.space.gov.au/team-artemis-australia.

[65] National Aeronautics and Space Administration, "The Artemis Accords," About the Accords, February 1, 2024, https://www.nasa.gov/artemis-accords/.

[66] Statement – Australia, Item 14, 60th Legal Subcommittee,

https://www.unoosa.org/documents/pdf/copuos/lsc/2021/statements/item_14_Australia_ver.1_4_June_PM.pdf; Statement – Australia, Item 9, 63rd Legal Subcommittee, https://www.unoosa.org/documents/pdf/copuos/lsc/2024/Statements/9_Australia.pdf.

[67]Statement – Australia, Item 9, 63rd Legal Subcommittee, https://www.unoosa.org/documents/pdf/copuos/lsc/2024/Statements/9_Australia.pdf.

also pursuing a multinational lunar mission, which will be supported by a similar set of principles and guidelines the International Lunar Research Station).[68]

The MoU between the U.S. Space Command and Australia's Defence Space Command (DSpC) seeks to extend military cooperation between the countries. With a specific focus on Space capabilities, the Enhanced Space Cooperation MoU was signed between the Space commanders of both countries in 2023. It is a framework for coordination, resilience, education, and development with the intent to extend mutual interests.[69]

Membership in Multilateral Frameworks

Framework Name	Type of Framework	Members	Member Since
International Telecommunication Union (ITU)	United Nations body	193	1878
Committee on the Peaceful Uses of Outer Space (COPUOS)	United Nations body	102	1959
Asia-Pacific Regional Space Agency Forum	International Space Forum	84	1993
Association of South East Asian Nations Regional Forum (ARF)	International Security Forum	26	1994
Combined Space Operations Initiative (CSpO)	International Cooperation Initiative	7	2005
Quadrilateral Security Dialogue (QUAD)	International Strategic Forum	4	2007
Square Kilometre Array Observatory (SKAO)	Cooperation Agreement	9	2021
Australia United Kingdom United States (AUKUS)	Security Agreement	3	2021

Table 4: Overview of multilateral frameworks signed by Australia, sorted by membership.

The recent change in Australia's defence posture revolves around increased military influence with strong relationships with key allies.[70] AUKUS is a military security agreement between Australia, the United Kingdom, and the United States.[71] The technology and information

[68] Fabio Tronchetti and Hao Liu, "Australia Between the Moon Agreement and the Artemis Accords - Australian Institute of International Affairs," Australian Institute of International Affairs, June 3, 2021, https://www.internationalaffairs.org.au/australianoutlook/australia-between-the-moon-agreement-and-the-artemis-accords/.

[69] United States Space Command, "USSPACECOM and Australian Defence Space Command Sign Enhanced Space Cooperation MOU," April 20, 2023., https://www.spacecom.mil/Newsroom/News/Article-Display/Article/3369772/usspacecom-and-australian-defence-space-command-sign-enhanced-space-cooperation/.

70 Michelle Neumann And Melissa de Zwart 'Securing Australia Through Space: Australia's Defence Partnerships' ACSG Policy Paper Series, November 2024, www.spacegovcentre.org.

[71] The White House, "Implementation of the Australia – United Kingdom – United States Partnership (AUKUS): Fact Sheet," Policy Paper, April 5, 2022, https://www.whitehouse.gov/briefing-room/statements-

shared between the three AUKUS nations see them working together on Space efforts.[72] The advanced capabilities and benefits which come from this partnership include the nuclear submarine training, along with multiple military bases which will be located along the Northern coastline of Australia.[73] The increase in innovation, technology, and information being shared between the allied States is fundamental to the longevity of the military security agreement.

Although space technology is not included as one of the eight AUKUS advanced capabilities, the AUKUS partners are collaborating on the Deep-Space Advanced Radar Capability (DARC) program. DARC consists of a ground system that 'will provide 24-hour continuous, all-weather global coverage to detect, track, and identify objects in deep space and increase space domain awareness'.[74]

The first infrastructure site will be fully operational by 2026 and located near Exmouth in Western Australia.[75] The remaining two DARC sites, respectively located in the United States and the United Kingdom, will be operational by the end of the decade.[76] In this manner, the geography of the three AUKUS partners is leveraged. DARC will strengthen Australia's space domain awareness capabilities and ability to share intelligence with defence partners.[77] It also expands Australia's detection and monitoring capabilities concerning geosynchronous orbit.[78]

The four areas in the Defence Strategic Review which are influenced by the AUKUS partnership include:

- Economic – investing in supply chains and industry,
- Military – updating technology,
- Strategic – training new recruits, and
- Diplomatic – strengthening alliances with Australia's key powers of the U.S., India, and Japan.[79]

releases/2022/04/05/fact-sheet-implementation-of-the-australia-united-kingdom-united-states-partnership-aukus/.

[72] Ibid., p. 72.

[73] Prime Minister of Australia, "AUKUS Nuclear-Powered Submarine Pathway," Media, March 14, 2023, https://www.pm.gov.au/media/aukus-nuclear-powered-submarine-pathway.

[74] AUKUS Defense Ministers Meeting Joint Statement" (2 December 2023), https://www.minister.defence.gov.au/statements/2023-12-02/aukus-defense-ministers-meeting-joint-statement.

[75] Department of Defence, "New Defence space capability boosts regional security," Media Releases, December 2, 2023, https://www.minister.defence.gov.au/media-releases/2023-12-02/new-defence-space-capability-boosts-regional-security.

[76] "AUKUS Defense Ministers Meeting Joint Statement" (2 December 2023), https://www.minister.defence.gov.au/statements/2023-12-02/aukus-defense-ministers-meeting-joint-statement.

[77] Malcom Davis, 'Seeing through the DARC, deep into space' The Strategist (19 December 2023),

https://www.aspistrategist.org.au/seeing-through-the-darc-deep-into-space/.

[78] Ibid.

[79] Department of Defence, "National Defence: Defence Strategic Review 2023,"pp. 33-34.

The Quadrilateral Security Dialogue (QUAD) between Australia, the U.S., India, and Japan has become ever more influential since its first establishment.[80] The QUAD has committed itself to supporting 'a free and open Indo-Pacific that is inclusive and resilient'.[81] During the initial breakout of Covid-19, the QUAD alliance worked on vaccines, climate change, and innovation of technology. In response to China increasing their military movements, the QUAD has shifted their attention to the military sector of information and technology sharing - including satellites.[82] One of the QUAD's areas of cooperation is Space.[83] Australia has strong ties in the Space sector with the U.S., along with a long-standing weather satellite sharing arrangement with Japan. India has recently shown their increased Space intentions leading to the QUAD potentially investing in shared Earth Observation satellites for disaster mitigation. Each member of the QUAD therefore has unique space capabilities. The three areas of focus regarding space which were identified at the 2023 Quad Leaders' Summit are extreme precipitation events, commercial space cooperation, and space situational awareness.[84]

The Combined Space Operations Initiative (CSpO) is a multinational partnership which aims to '[g]enerate and improve cooperation, coordination, and interoperability opportunities to sustain freedom of action in space, optimize resources, enhance mission assurance and resilience, and prevent conflict'.[85] It was founded by Australia, the United States, the United Kingdom, and Canada in 2014.[86] New Zealand, Germany, France, Italy, Japan, and Norway have later joined the CSpO.[87] The objectives of the CSpO are to prevent conflicts, unity of effort, space mission assurance, and defence protection.[88] The CSpO Vision 2031 statement provides lines of effort by which the CSpO participants seek to achieve these four objectives.[89] For Australia, the CSpO provides an avenue to engage with a wider range of countries possessing space capabilities regarding issues of space security.

2.4 Programmes and Capabilities

Australian space capabilities, often developed in partnerships with other countries like the U.S. and Japan, are unique and multifaceted. Australia is home to several launch sites and

[80] Sheila A. Smith, "The Quad in the Indo-Pacific: What to Know," Council on Foreign Relations, May 27, 2021, https://www.cfr.org/in-brief/quad-indo-pacific-what-know.

[81] "Quad Leaders' Vision Statement – Enduring Partners for the Indo-Pacific" (20 May 2023), https://www.pm.gov.au/media/quad-leaders-vision-statement-enduring-partners-indo-pacific.

[82] Department of Foreign Affairs and Trade, "The Quad," International Relations, n.d., https://www.dfat.gov.au/international-relations/regional-architecture/quad.

[83] "Quad Leaders' Summit Fact Sheet" (20 May 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/quad-leaders-summit-fact-sheet/.

[84] Ibid.

[85] Combined Space Operations Vision 2031, p. 1.

[86] Cheryl Pellerin, "Stratcom, DoD Sign Space Operations Agreement With Allies" DOD News (23 September 2014), https://www.defense.gov/News/News-Stories/Article/Article/603303/stratcom-dod-sign-space-operations-agreement-with-allies/.

[87] David Vergun, "More Nations Meet to Address Space Security" DOD News (7 December 2023), https://www.defense.gov/News/News-Stories/Article/Article/3610656/more-nations-meet-to-address-space-security/.

[88] Combined Space Operations Vision 2031, pp 2–3.

[89] Ibid, p 3.

has strong suborbital launching abilities. It is also set to improve its orbital launching capabilities soon. Australian universities have been working on CubeSats to test research abilities. Three military CubeSats were launched from 2018 to 2021 by the Department of Defence (DoD) from Cape Canaveral.[90] The country has been seeking to launch a Moon rover, initially scheduled for 2025, as a demonstration of its space abilities.

Australia's Spending in the Space Sector

The Australian Federal Budget for 2023-2024 sets out how much the Government will spend on Space.[91] With AUD $34.2 million dedicated to the sector, which will be used to continue core functions at the ASA and to enhance Space activity regulations.[92] The Australian Federal Government funding, along with the ASA's separate budget will go towards:

- Technical expertise, training, and direction.
- International engagement.
- Funding opportunities.
- Policy advice to all State levels of the Australian Governments to progress each States individual Space capabilities.
- Regulating Australian Space activities with allied nations, with AUD $25.2 million set for 2022-2023 to further invest in researchers and businesses working with the Indian Space Research Organisation and the Indian Space sector.
- Initiatives to inspire the young and old from the nation and build a secure future Space workforce.
- A joint promise of 20,000 additional jobs in the Australian Space sector and related fields.[93]

Launchers and Launch Sites

Australia has a long history of suborbital launch vehicles, including a modified United Kingdom launcher, as well as domestically designed rockets.[94] The latest development has been the Eris launcher, designed and created by Gilmour Space, a Queensland launch services company. The Eris project is intended to launch into Low Earth Orbit (LEO) in three stages, with a hybrid engine. Its first launch is planned to occur in early 2024 from the Bowen Orbital Spaceport, Abbot Point in Queensland, making it the first orbital launch in Australia.[95]

---

[90] Gunter D. Krebs, "Military Spacecraft – Australia," Gunter's Space Page, April 4, 2023, https://space.skyrocket.de/directories/sat_mil_aus.htm.

[91] Department of Industry, Science and Resources, "Announcing the 2023-2025 Budget," News, May 10, 2023, https://www.industry.gov.au/news/announcing-2023-24-budget.

[92] Australian Space Agency, "About the Agency," Australian Space Agency, n.d., https://www.space.gov.au/about-agency.

[93] Andrew Tillett and Tom McIlroy, "AUKUS Will Create 20,000 Jobs and 'Safeguard Economy,'" Australian Financial Review, March 12, 2023, https://www.afr.com/politics/federal/aukus-will-create-20-000-jobs-and-safeguard-economy-20230312-p5crej.

[94] Ibid., "Launch Vehicles – Australia."

[95] Gilmour Space, "LAUNCH," Our Launch Services, n.d., https://www.gspace.com/launch.

Australia has two permanent launch sites, with another two to be constructed, and five that are temporary but functional.[96] The Woomera and Koonibba sites in regional South Australia have launched several suborbital rockets including the Lorikeet, Corella, Cockatoo, and Kookaburra High Altitude Density (HAD) Gosling rockets in the 1960's. In 2022, The Arnhem Space Centre launched a National Aeronautics and Space Administration (NASA) commercial suborbital sounding rocket. It was their third successful launch, the first NASA launch in Australia in 25 years, and the first commercial launch by NASA outside of the United States.[97]

Whaler's Way and Toowoomba Airport are two sites to be developed to properly support orbital launch. Whaler's Way on the Eyre Peninsula in South Australia offers orbital launch abilities on a 4000-acre complex on the Great Australian Bight.[98] The decision to develop the Toowoomba Airport, located in Queensland, for Space launches came after Virgin Orbit announced it would alter a few Boeing 747s to provide satellite launch services.[99] The plans failed before demonstrator launch in Australia, and the status of the airport project is now unknown.[100]

Military Spacecraft

The Australian DoD has seven active satellites in orbit. Three of these satellites are providing communications to Australia, with the remainder being CubeSats, utilised for research and technology purposes.[101] Australia's military research satellites are several CubeSats designed and built by the University of New South Wales. The Royal Australian Airforce (RAAF) M1 CubeSat was launched in 2018 on a SpaceX Falcon 9 from Vandenberg Space Centre, California. It was built to test SSA capabilities, as well as tracking and radio software for maritime and aircraft signals but failed to communicate after deployment.[102] Its successor, the RAAF M2 Pathfinder, was focused on testing communication technologies only. Launched by Rocket Lab from Onenui Station in New Zealand, it has been operational since June 2020.[103] The latest RAAF M2 is a larger 12U CubeSat, designed to split into two 6U satellites testing Earth Observation, Artificial Intelligence (AI), and communication technologies. The satellites also include re-programmable radios allowing objectives to be controlled and

[96] Gunter's Space Page, "Launch Sites", n.d. https://space.skyrocket.de/directories/launchsites.htm

[97] Matt Garrick, "NASA Successfully Launches Its First Rocket from Newly Created Arnhem Space Centre," ABC News, June 26, 2022, https://www.abc.net.au/news/2022-06-27/nasa-launch-rocket-arnhem-land-success/101183776.

[98] Southern Launch, "Whalers Way Orbital Launch Complex," Launch Information, n.d., https://www.southernlaunch.space/whalers-way-orbital-launch-complex.

[99] Len Varley, "Toowoomba Airport Selected as Virgin Orbit Space Launch Site," AviationSource News, September 20, 2022, https://aviationsourcenews.com/news/toowoomba-airport-selected-as-virgin-orbit-space-launch-site/.

[100] Peter Hoskins, "Virgin Orbit: Branson's Rocket Dream Ends after Mission Failure," BBC News, May 24, 2023, https://www.bbc.com/news/business-65692302.

[101] Gunter's Space Page, "Military Spacecraft – Australia", n.d. https://space.skyrocket.de/directories/sat_mil_aus.htm

[102] Ibid., "RAAF M1."

[103] Ibid., "RAAF M2 Pathfinder (M2PF)."

changed whilst in orbit. Launched in March 2021 by Rocket Lab in Onenui, the units separated in September that same year.[104]

Space Situational Awareness (SSA)

Australian Space Situational Awareness (SSA) capabilities stem from the unique geographic position it inhabits in the far south of the globe. Domestic infrastructure includes the Defence Science and Technology (DST) telescopes in South Australia, and Murchison Widefield Array and Raven telescopes in Western Australia.[105] An expansion by the DoD, called the JP9360 Space Domain Awareness (SDA) program, intends to allow independent Australian access to data, with the intention to develop the organisation's own mission and analysis capabilities.[106]

Collaborations and agreements with international agencies allow Australia to host various other SSA abilities. These include the United States' C-Band Surveillance Radar and Space Surveillance telescope in Western Australia, along with the United States Air Force Falcon telescope in the Australian Capital Territory.[107]

Research and Technology

Australia's military research satellites are several CubeSats designed and built by the University of New South Wales. The RAAF M1 CubeSat was launched in 2018 on a SpaceX Falcon 9 from Vandenberg Space Centre, California. It was built to test SSA capabilities, as well as tracking and radio software for maritime and aircraft signals but failed to communicate after deployment.[108] Its successor, the RAAF M2 Pathfinder, was focused on testing communication technologies only. Launched by Rocket Lab from Onenui Station in New Zealand, it has been operational since June 2020.[109] The latest RAAF M2 is a larger 12U CubeSat, designed to split into two 6U satellites testing Earth Observation, AI, and communication technologies. The satellites also include re-programmable radios allowing objectives to be controlled and changed whilst in orbit. Launched in March 2021 by Rocket Lab in Onenui, the units separated in September that same year.[110]

Australia awarded a contract to Lockheed Martin in April 2023 to build the Australian Defence Satellite Communications System (Project JP9102).[111] The contract is intended to provide a sovereign military satellite communications system (both Space and ground segment) to the Australian Defence Force (ADF). In addition, two satellites launched by the United States

[104] Ibid., "RAAF M2."

[105] European Space Policy Institute, "Emerging Spacefaring Nations," Reports, June 21, 2021, p. 65. https://www.espi.or.at/reports/emerging-spacefaring-nations/.

[106] Secure World Foundation, "Global Counterspace Capabilities Report 2025," Counterspace Report, May 26, 2025, pp. 187-188. https://swfound.org/counterspace/.

[107] European Space Policy Institute, "Emerging Spacefaring Nations," p. 64.

[108] Gunter's Space Page, "Military Spacecraft – Australia", n.d. https://space.skyrocket.de/directories/sat_mil_aus.htm

[109] Ibid., "RAAF M2 Pathfinder (M2PF)."

[110] Ibid., "RAAF M2."

[111] Lockheed Martin, "Lockheed Martin Selected as Preferred Bidder for JP9102," News Releases, April 3, 2023, https://news.lockheedmartin.com/2023-04-03-Lockheed-Martin-selected-as-preferred-bidder-for-JP9102.

National Reconnaissance Office in 2022 are owned and operated by Australia, however not much is known about the details of the spacecraft, such as their orbit or purpose.[112]

Communications

In 2003, Australia launched the Japanese-made Optus and Defence C1 communications satellite from France's Guiana Space Centre. The dual-use satellite, equipped with 16 antennae to cover beams from Asia to Polynesia, provides military communications to the DoD through the service provider Singtel Optus.[113] At the time of launch, it was the largest dual-use satellite ever put in orbit. Optus also uses the satellite to provide subscription TV, and Aurora free-to-air TV and Radio to the Australian outback.[114]

Australia is also involved in the U.S. Wideband Global Satcom (WGS) programme, with financial contribution made in exchange for its own satellite.[115] The WGS-6 is the Australian-owned component of this constellation, with 19 coverage areas on an expected 14-year lifespan. The programme provides communications for the U.S. Space Force, the Departments of Defence for the U.S. and Australia, as well as the North Atlantic Treaty Organisation (NATO).[116] The satellite was commissioned by Australia in 2007, manufactured by Boeing Aerospace, and launched from Cape Canaveral, Florida, in 2013.[117]

Australia also benefits from the U.S. Advanced Extremely High Frequency (AEHF) constellation system, which started operations in 2010. This system of six military communication satellites is the successor to the Milstar constellation of geosynchronous communication satellites. It acts as a secure, high priority military communications provider for the United States, but also allied countries: Canada, the United Kingdom, the Netherlands, and Australia.[118] Contracted to Lockheed Martin and developed since 2001, the system has ground, naval, and airborne terminals with access to communications worldwide.[119]

Australian Military Satellites			
	Communications	Research	Unknown
National	• Optus C1 • Australian Defence Satellite Communications System (upcoming)	• RAAF M1 • RAAF M2 Pathfinder	

[112] Gunter's Space Page, "Military Spacecraft – Australia", n.d. https://space.skyrocket.de/directories/sat_mil_aus.htm

[113] Ibid., "Optus C1 (Optus and Defence C1)."

[114] Optus, "Optus C1 Satellite," Living Network, n.d., https://www.optus.com.au/living-network/satellite/fleet/c1.

[115] Andrew Davies, "Australia's WGS Communications—What Went Wrong?" The Strategist, September 21, 2015, https://www.aspistrategist.org.au/australias-wgs-communications-what-went-wrong/.

[116] United States Space Force, "Wideband Global SATCOM Satellite," Fact Sheets, February, 2023, https://www.spaceforce.mil/About-Us/Fact-Sheets/Article/2197740/wideband-global-satcom-satellite/.

[117] Gunter's Space Page, "WGS 4, 5, 6, 7 (WGS Block 2)", n.d., https://space.skyrocket.de/doc_sdat/wgs-4.htm

[118] United States Space Force, "Advanced Extremely High Frequency System (AEHF)," Space Operations Command (SpOC), August, 2021, https://www.spoc.spaceforce.mil/About-Us/Fact-Sheets/Display/Article/2381348/advanced-extremely-high-frequency-system-aehf.

[119] Ibid.

		• RAAF M2	
Collaborations with United States	• Wideband Global SATCOM 6 • SSA • Advanced Extremely High Frequency		• NROL 161/166

Table 5: Summary of Australian military satellites

Other

Since 2002, Australia has had 40 satellites successfully launched by the United States, New Zealand, France, and Japan. The U.S. has assisted with launches at the Cape Canaveral or Vandenberg sites, and New Zealand at the Onenui launch site. Over 20 of the most recent launches have been CubeSats, manufactured by Australian universities, the RAAF or Skykraft, an Australian air traffic surveillance company. Since 2021, SpaceX has carried recent Australian payloads, with the Falcon 9 rockets being utilised to launch technology demonstration or telecommunications capabilities. Prior to this, Australia had worked with companies including Rocket Lab, United Launch Alliance (ULA), and ArianeSpace for payload launches.

Customer	Type of Mission			
	Communication	Technology	Science	Orbital Servicing
Optus	Optus C1 Optus D3 Optus D1 Optus 10 Optus D2			
National Broadband Network (NBN)	Sky Muster 01/NBN-Co 1A Sky Muster 02/NBN-Co 1B			
Curtin University		Binar-1		
University of Adelaide			SUSat	
University of New South Wales		Buccaneer RMM	UNSW-EC0	
University of Sydney		CUAVA 1	i-INSPIRE 02	
Melbourne Space Program		ACRUX 1		
Fleet Space	Proxima 1 Centauri 3 Proxima 2 Centauri 4 Centauri 1 Centauri 5 Centauri 2			
Sirion Global		Sirion Pathfinder 2		

Customer	Type of Mission			
	Communication	Technology	Science	Orbital Servicing
Skykraft	Skykraft 1 Skykraft 2 Skykraft 3 Skykraft 3A Skykraft 3B Skykraft 3C Skykraft 3D Skykraft 4			Skykraft Deployer 1 Skykraft Deployer 3
Myriota	Myriota 7			
Echostar Global	EG 3			

Table 6: Non-military Australian satellites launched in the last two decades

3 Space Control: Offensive and Defensive Measures

This section provides an overview of the different types of offensive space control measures as well as of the protections that can be deployed against these possible attacks – from the technical measures involving software or hardware solutions, to the wider operational practices embedded across a system, right up to the use of policy, legal and diplomatic tools which used to deter threats or limit the potential and scale of escalation. A matrix matching offensive and defensive measures for space control is also developed at the end of the section.

3.1 Offensive Measures for Space Control

Counterspace offensive weaponry covers different areas of capabilities and are often classified differently within the literature. This report adopts a fourfold typology, namely physical, directed energy, electronic, and cyber weaponry, as these capabilities provide distinct means of attack against space infrastructure. Physical counterspace destroys or disables space hardware – either kinetically or non-kinetically – with a direct collision attack or via the use of nuclear weaponry. Directed energy uses offensive lasers for the purpose of dazzling, blinding, or overheating satellite components. Electronic weapons interfere with the transmission of data to and from a satellite, often preventing information from being received. Cyber-attacks interfere with the software of a satellite or ground control infrastructure to prevent and/or capture information.

The overlap between various counterspace offensive weapons can provide unclear distinctions. Directed energy capabilities are sometimes classified as a non-kinetic physical type of attack, due to the physical effects that can be experienced by targeted satellites. The intersection of cyber-attacks and electronic warfare capabilities within military definitions have caused arguments for the merger of the two fields, including beyond space.[120] This is demonstrated with radar systems that wirelessly utilise cyberspace and simultaneously access the electromagnetic spectrum, as seen with Russia's defence in January 2017 against Unmanned Aerial Vehicle (UAVs). Whilst seven of the thirteen UAV drones were shot down via the Pantsir air-defence missile system, the remaining six drones were reported to have experienced both uplink jamming and remote hacking to cause three to crash, and three to land safely.[121] For clarity within this report, physical, directed energy, electronic, and cyber weaponry will be recognised as separate categories, with brief summaries defining why.

3.1.1 Physical Measures

Taxonomy and categorisation

[120] Joint Chiefs of Staff, "USG Compendium of Interagency and Associated Terms," DoD Terminology Program, November, 2019, pp 269-299, https://www.jcs.mil/Doctrine/DOD-Terminology-Program/

121 Col. Mandeep Singh, "Drone Swarms: The Emerging Threat," Indian Defence Review, September 1, 2019, https://www.indiandefencereview.com/news/drone-swarms-the-emerging-air-threat/

Physical counterspace means are direct attacks to physically damage spacecraft or ground infrastructure. These measures can be further classified as either kinetic or non-kinetic, due to the way a physical attack can occur.

- Kinetic Physical -Physical compromising of Space hardware through direct contact. This can be done with Direct Ascent Anti-Satellite (DA-ASAT) missiles, ground-station attacks, and co-orbital satellites utilised as weapons. These attacks can be attributed to a perpetrator by tracking launch data and causes recordable damage.
- Non-kinetic Physical – physical destruction of satellite components without direct contact during an attack. This can be done by utilising nuclear radiation to generate an electromagnetic pulse and radioactive environment, or weaponry utilised by co-orbital satellites, such as chemical sprays. These attacks are less attributable than kinetic physical attacks, as there is not a tangible, trackable object launched with intent to destroy.

Presentation of the threat and potential consequences

Both forms of physical counterspace capabilities have considerable effects that can affect infrastructure, environment, and diplomatic relationships.

Kinetic Physical Weapons

DA-ASATs are missiles, typically launched from ground bases and fighter jets to hit a satellite, in order to permanently disable the service it provides. These missiles are usually based on a country's existing Intercontinental Ballistic or Anti-Ballistic Missile (ABM) capabilities. Given that there is some time between the launch of the attack and engagement with target, this allows actors to move and protect satellites in orbit and is also easily trackable. Due to this, the attack can be attributed to a specific actor, which can be used either to negotiate or counter the threat. Kinetic physical attacks often release debris, even when actors are testing their systems against their own (defunct) satellites.

Co-orbital ASATs are attacks from other satellites in orbit. These satellites are launched with tracking and physical targeting capabilities to hit and physically disable other satellites. Co-orbital ASATs are often dual-use satellites, as they may originally be launched to remove debris or service another satellite, but these abilities can very easily be repurposed for offensive goals. This makes it harder to attribute threats unless actively tracking the satellite itself and can be excused as an unplanned collision, which can contribute to political tension.

Terrestrial infrastructure attacks: Attacks against ground stations actively target the control centre of satellites through regular military efforts to disable constellations and can lead to death of the operators themselves. These attacks can also target other terrestrial infrastructure, such as data centres. Due to the ability to rebuild ground stations and data centres, these attacks are considered less permanent against infrastructure than DA- and Co-orbital ASAT threats against satellites.

Effects: Kinetic physical attacks often release debris, even when actors are testing their systems against their own (defunct) satellites. Artificial Space debris has existed since the

Space Race, with pieces of debris still in orbit some 50 years later.[122] There are already several thousand pieces of debris in orbit due to normal space operations. However, the increase of DA-ASAT tests in the past decade have contributed to this issue of debris not re-entering Earth's atmosphere in a short timeframe and remaining in orbit.[123][124] This poses a threat to other satellites in the area, creating risks of extra collisions and obstructing orbit and launch abilities. The Kessler syndrome, first described in 1978 by NASA's Donald Kessler in Collision Frequency of Artificial Satellites: The Creation of a Debris Belt, is a concerning theory stating that an increasing amount of debris in orbit will lead to more collisions with satellites, thus creating more debris. This could become hazardous as the debris could hit the International Space Station (ISS), prevent launches, and stop technology, exploration developments and even investments in space.

Kinetic Weapons			
Types of Attack	Ground Station Attack	Direct-Ascent Attack	Orbital ASAT
Origin to Destination	Ground-to-ground	Ground-to-space	Space-to-Space
Permanence of Attack	Permanent	Permanent	Permanent
Scale of Attack Effects	Widespread, if node supports multiple satellites	Widespread, if orbital debris creation	Limited to Widespread, dependent on the model of attack
Attributability of Attack	Variable attribution, depending on mode of attack	Launch site can be attributed	Can be attributed by tracking previously known orbit
Require Space Launch Capability	No	Yes	Yes
Require Space Domain Awareness	No	Yes	Yes

Table 7: Effects of different Kinetic Physical space threats (CSIS Space Threat Assessment 2025 Report, p. 5)

Non-kinetic Physical Weapons

Directed Energy and Nuclear detonations: Electromagnetic pulses (EMPs) happen when a nuclear detonation occurs in space. This would disturb all satellites immediately within a nearby range, and increase radiation levels in the area, degrading satellites further than the radioactive Space environment. Not much is known about the long-term effects this would have on satellites in orbit, as nuclear tests in Space were banned in 1963 under the Partial Nuclear Test Ban Treaty, however testing of nuclear weapons in Space has occurred

[122] LeoLabs, "Low Earth Orbit Visualization", n.d., https://platform.leolabs.space/visualization

[123] ESA, "The current state of space debris", November, 2020, https://www.esa.int/Space_Safety/Space_Debris/The_current_state_of_space_debris

[124] Secure World Foundation, "Global Counterspace Capabilities Report 2025, p. 184.

before.[125] The 1962 Starfish Prime Test by the United States tested how the Van Allen magnetic fields react to nuclear detonation, and the resulting EMP was reported by Oahu, some 1300km away from the Johnston Atoll where the detonation occurred.[126] In February 2024, Russia has been accused by the United States of designing a Space-based nuclear weapon, with the ability to target satellites in orbit, drawing much criticism as placing and detonating such a weapon in Space would violate the 1963 Partial Nuclear Test Ban Treaty and the 1967 Outer Space Treaty.[127] Capability specifications are currently unknown.

Co-orbital chemical weaponry: Co-orbital satellites may be equipped with payloads containing chemical products in order to disable satellite functions. Russia has been accused of developing aerosol payloads on satellites in order to block radio and optical transmissions[128]. Further development of this technology could place corrosives and other chemicals as payloads in order to physically damage other satellites internal and external hardware. By dousing other satellites with damaging chemicals, this could permanently disable the satellite without collision. However, co-orbital satellites are tracked extensively, and it is attributable to the perpetrator.

Non-kinetic Weapons		
Types of Attack	Nuclear Detonations	Directed Energy
Origin to Destination	Ground-to-Ground; Ground-to-Space; Space-to-Space	Ground-to-Ground; Ground-to-Space; Space-to-Space
Permanence of Attack	Permanent	Varies, dependent on the mode of attack
Scale of Attack Effects	Widespread	Limited and Regional, dependent on mode of attack
Attributability of Attack	The launch site can be attributed	Limited attribution
Requires Space Launch Capability	No	No
Requires Space Domain Awareness	No	Yes

Table 8: Effects of different Non-kinetic Weapons (source: CSIS Space Threat Assessment 2025 Report, p. 5)

Ongoing and operational projects in major spacefaring nations

Whilst ASAT weapons have not been utilised in military settings, States have made significant attempts to showcase individual counterspace capabilities within the last few decades. As

[125] CSIS, "Counterspace Weapons 101", October 2019, https://aerospace.csis.org/aerospace101/counterspace-weapons-101/

[126] Ibid.

[127] Mark Trevelyan, "Explainer: What is the Test Ban Treaty and why would a country conduct a nuclear test?", Reuters, October 2023, https://www.reuters.com/world/europe/what-is-nuclear-test-ban-treaty-why-is-russia-changing-its-position-2023-10-17/

early as 2007, China demonstrated kinetic ASAT capabilities and, afterwards, made several tests without directly striking a satellite.[129] The following year saw the U.S.'s Operation Burnt Frost take effect, with a defunct spy satellite, US-193, shot out of orbit. In 2019, Mission Shakti saw a demonstration of ASAT capabilities by Indian forces with the destruction of a Microsat-R satellite.[130] Russia performed its own DA-ASAT test in 2021, by shooting a defunct Soviet satellite out of Lower Earth Orbit with its Nudol system. These tests all produced debris, although not all with the same lifetime.

The United States has demonstrated ample ASAT technology since the Cold War. The most recent DA-ASAT test has been the Aegis system in 2008.[131] Their co-orbital abilities have had several successes, with the Prowler, MsTE and Pan programs from 1990-2013.[132] Several older programs have since been decommissioned.

Like the U.S., Russia also has historically demonstrated DA-ASAT and co-orbital abilities. Utilising older Soviet technology, Russia has made the successful Kontakt (2009) and Nudol (2020) systems.[133][134] The recent Burevestnik and Rockot systems were tested in the 2010's and have since been deemed inactive as the systems are no longer performing co-orbital reconnaissance.[135][136]

China has tested ASAT abilities since the 1990s. The State began testing Direct Ascent abilities since the 1990's, and the SC19 and DN3 have had recent tests attributed to them in 2014 and 2018. Chinese Co-orbital tests have been successfully launched since 2008, and several have been decommissioned, however the SJ-21 remains unregistered to the UN.

India has successfully demonstrated DA-ASAT ability with its Mission Shakti test in 2019, however, co-orbital tests have not been demonstrated yet. See more about Mission Shakti in the Case Study below.

These four countries have demonstrated historical and current ASAT capabilities, with both Russian and U.S. abilities beginning during the Cold War. Some systems are now defunct and/or decommissioned, however technology and findings from these attempts have been re-used and inform future programs. Refer to Annex B, Part 2 for full list of recent ASAT capabilities by country.

---

[129] William J. Broad and David E. Sanger, "China Tests Anti-Satellite Weapon, Unnerving U.S.," The New York Times, January 18, 2007, https://www.nytimes.com/2007/01/18/world/asia/18cnd-china.html.

[130] Doris Elin Urrutia, "India's Anti-Satellite Missile Test Is a Big Deal. Here's Why.," Space.Com, August 10, 2022, https://www.space.com/india-anti-satellite-test-significance.html.

[131] "Ground-Based Midcourse Defense (GMD)", Missile Defense Advocacy Alliance, January 2019, https://missiledefenseadvocacy.org/defense-systems/ground-based-midcourse-defense/

[132] Marco Langbroek, "A Nemesis in the sky", The Space Review, October 2016, https://www.thespacereview.Com/article/3095/1.

[133] Global Security, "79M6/95M6 Kontakt Miniature ASAT", n.d., http://www.globalsecurity.org/space/world/russia/mini.htm

[134] Military Russia, "Complex 14Ts033 Nudol, missile 14A042", October 2023, n.d., http://militaryrussia.ru/blog/topic-806.html

[135] Bart Hendrickx, "Burevestnik: A Russian air-launched anti-satellite system", April 2020, https://www.thespacereview.com/article/3931/1.

[136] "Rockot launch vehicle", n.d., http://www.russianspaceweb.com/rockot.html.

Case study

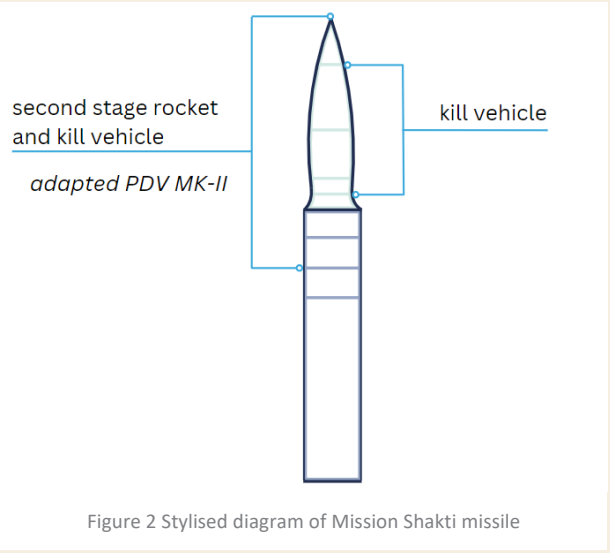

Figure 2 Stylised diagram of Mission Shakti missile

The Mission Shakti DA-ASAT test by India in 2019 used a successfully adapted PDV MK-II missile interceptor to destroy a replication of a military satellite.[137] Launched from the Dr APJ Abdul Kalam Island site on March 27, the rocket successfully hit the Microsat-R satellite – launched in January 2019 – in Low Earth Orbit (LEO) within a minute of launch.[138] The rocket, an adapted PDV Mk-II three-stage missile, utilised solid fuel as a propellant and liquid fuel for its Kill Vehicle. It was built by the Defence Research and Development Organisation (DRDO) of India, is part of PM Narendra Modi's push to update India's defence abilities, with the aim to create "futuristic deterrence technology" independently. The project, greenlit in 2016, was developed in secrecy within two years by 150 scientists at DRDO facilities, with the target satellite assembled and launched by the Indian Space Research Organisation (ISRO) as a customer launch. The satellite was specifically built to resemble foreign defence satellites, at 740kg and orbiting at 8km/s.[139] This test makes India the 4th country to successfully demonstrate DA-ASAT abilities, ensuring its position in any future negotiation regarding testing bans.

India demonstrated its intention at limiting the life of debris generated by the test, by choosing a small target satellite and interception on a downward trajectory.[140] Despite these measures, the test still created some 400 pieces of debris, with 130 large pieces tracked by NASA, which returned to Earth by June 2022, with some pieces remaining in higher orbit.[141]

What is Australia's position on DA-ASAT testing?

- Australia has not been undertaking DA-ASAT tests. In 2022, it voted in favour of UN resolution A/RES/77/41, which calls upon all States to commit not to conduct destructive direct-ascent anti-satellite missile tests.
- Like the US, Australia has expressed the view that orbital debris are among the most significant threats to the space environment and that the intentional destruction of satellites using kinetic force contributes to exacerbating such threats

[137] Secure World Foundation, "Global Counterspace Capabilities Report 2025, pp 175-178.

[138] Ashley J. Tellis, "India's ASAT Test: An Incomplete Success", Carnegie Endowment for International Peace, April 2019, https://carnegieendowment.org/research/2019/04/indias-asat-test-an-incomplete-success?lang=en.

[139] [139] Secure World Foundation, "Global Counterspace Capabilities Report 2025, p 175.

[140] Ashley J. Tellis, "India's ASAT Test: An Incomplete Success", Carnegie Endowment for International Peace, April 2019, https://carnegieendowment.org/research/2019/04/indias-asat-test-an-incomplete-success?lang=en.

[141] "NASA calls India's mission Shakti 'terrible', as it added 400 dangerous pieces to Earth's Orbit", India Times, April 2019, https://www.indiatimes.com/technology/science-and-future/mission-shakti-created-400-pieces-of-dangerous-debris-that-can-harm-space-station-says-nasa-364702.html.

- Debris mitigation of DA-ASATs is possible but not reliable, Australia does not have current and effective Space debris mitigation to use
- To continue the public mission on space debris mitigation with a focus on sovereign and autonomous origin.

3.1.2 Directed Energy Measures

Taxonomy and categorisation

Directed Energy Weaponry (DEW), primarily lasers, are generally electronically-based weapons that can cause physical effects on Space systems without contact.[142] Lasers can be utilised to target satellites and blind or dazzle satellite sensors, as well as overheat internal systems. High-Powered Microwave (HPM) energy is a specifically designed laser that can cause damage to electronic circuitry and processors, with a possibility of discomfort experienced by humans.[143]

The classification of DEW counterspace capabilities is organised into two categories:

1. Dazzling of a satellite's imaging sensor.

   Laser dazzling is considered a countermeasure as opposed to a weapon due to a non-permanent effect. This causes saturation of pixels, which obscures the image that was to be produced. Whilst the effects may persist for an unknown number of images following the incident, it does not require operator intervention to eventually clear and allow satellites to return to regular operations. Due to the sensitivity of imaging sensors, it is estimated that a 10-Watt laser would be sufficient to dazzle and obscure an area.[144]

2. Damage to the satellite bus or its subsystems.

   If a continuous beam of energy with a power level as low as 40-Watts was utilised, this could damage part of the sensor array. The difference between dazzling and damaging an imaging sensor is technically an unknown area. It is assumed that damage to optics requires a higher power than dazzling, despite the risk of damage being carried by a dazzling attempt on a satellite. Whilst it would only affect a few pixels, it would still be classified as permanent damage.

   The satellite will presumably not experience a disruption to operations if the optical sensor was damaged, due to other functions not related to imaging still being able to be controlled and operated.[145] In addition to this, there are two forms of specifically

[142] Secure World Foundation, "Global Counterspace Capabilities Report 2025, p. 75.

[143] Ibid, p. 76.

[144] David Wright, Laura Grego, and Lisbeth Gronlund, "The Physics of Space Security", American Academy of Arts and Science, 2005, pp 125-130, https://www.ucsusa.org/sites/default/files/2019-09/physics-space-security.pdf.

[145] Yousaf Butt, "Effects of Chinese Laser Ranging on Imaging Satellites," Science & Global Security 17, no. 1 (June 26, 2009): 20–35, https://doi.org/10.1080/08929880902864376.

designed laser systems that have the express purpose of causing damage to the satellite bus or its subsystems.

2(a) Thermal effects from very High-Powered Lasers to sensor arrays deal damage to a satellite bus. Thermal regulation systems, batteries, or altitude controls systems can experience failure due to the absorption of high energy, causing a complete failure of the satellite.[146] However, this form of laser energy has a high power requirement, causing it to be costly compared to the alternatives.

2(b) Due to the requirement of high power, a focused beam of HPM energy is an alternative to still causing damage. By targeting satellite functionality utilising its own antennae or entering through gaps in electrical shielding and connections, the HPM energy attacks are harder to attribute. This is due to a wider range of angles where an attack could originate from. Antennae-targeted HPM attacks occur within the vision field of satellite antennae, establishing a pathway. Gaps in shielding and connections can be targeted when manufacturing faults are discovered, and HPM energy is directed from any angle through the flaws.

Presentation of the threat and potential consequences

With the ability to be ground-based or Space-based, the requirement for operating these systems is more demanding compared to other alternatives. Ground-based DEW requires higher sources of power, which are likely to be chemical or electrical in nature.[147] The size and type of DEW is also limited, due to the financial investment required by States.[148] Space-based systems are more efficient with regards to the level of power that is required, however the lack of available power sources compared to ground-based systems puts them at a disadvantage.[149] In addition, some building blocks are necessary to make this counterspace capability effective:

- High fidelity SSA.
- High power laser device.
- Precise beam tracking and control.
- Adaptive optics to counteract atmospheric turbulence (for ground-based development).[150]

The accurate tracking of satellites to utilise lasers and HPM weapons effectively is perhaps the most difficult aspect of DEW. Adaptive optics may be required if being used through atmospheric levels, high beam quality requires significant power to maintain its level, and advanced control operations to steer the beam precisely are essential.[151] Effective laser utilisation against a satellite's sensor is determined by being within the field of view, which

[146] Secure World Foundation, "Global Counterspace Capabilities Report 2025, pp. 75-76.

[147] Ibid.

[148] Ibid.

[149] Ibid.

[150] Ibid.

[151] Ibid.

allows for possible attribution of the attack as well as to an approximate geographic location.[152] However, it is also significant that the ability to determine if an attack was successful is lowered, due to the lack of visibility.[153]

The potential for military counterspace applications of DEWs contributes to their attractiveness for States. With the ability to interfere with or disable a satellite without generating debris, DEW technology would enable States to affect EO satellites, and possibly most satellites in LEO.[154] The significant financial burden to develop Space-based DEW is higher, which has contributed to stalled developments or planning in that area.[155] It is not limited to the power requirement, but the mass of the weapon, consumables and disturbance torques (chemical lasers), electrical power generation (solid-state and fibre lasers, particle beams), target acquisition and tracking, and the potential required large size of a constellation.[156] Furthermore, being able to assess the effectiveness of ground- and Space-based non-destructive DEW counterspace capabilities is limited. Determining if a target has experienced temporary dazzling or blinding, compared to long-term damage, relies on assessments of internal designs or protective measures.[157]

Directed Energy			
Types of Attack	Laser Dazzling or Blinding	High-Powered Laser	High-Powered Microwave
Attribution	Clear attribution of the laser's location at the time of attack	Limited attribution	Limited attribution
Reversibility	Reversible or irreversible; attacker may or may not be able to control	Irreversible	Reversible or irreversible; attacker may or may not be able to control
Awareness	Only satellite operator will be aware	Only satellite operator will be aware	Only satellite operator will be aware
Attacker Damage Assessment	No confirmation of success	Limited confirmation of success if satellite begins to drift uncontrolled	Limited confirmation of success if satellite begins to drift uncontrolled
Collateral Damage	None	Could leave target satellite disabled and uncontrollable	Could leave target satellite disabled and uncontrollable

[152] Ibid.

[153] Ibid.

[154] Ibid. pp. 80-81.

[155] Ibid.

[156] Ibid.

[157] Ibid.

Table 9: Effects of different Directed Energy Space threats. CSIS Space Threat Assessment 2023 Report, p. 6)

Ongoing and operational projects in major spacefaring nations

The following assessment is based on publicly available information of current DEW capabilities for specific States.

The United States is reported to possess the capability to dazzle, and possibly blind, Earth Observation (EO) imaging satellites from ground-based locations. Since the 1980s, there has been significant research and development of DEW by the United States. The intent was to develop high-power lasers to intercept ballistic missiles and nuclear warheads or against satellites.[158] Three projects produced publicly available information on U.S. DEW capabilities:

- The Mid-Infrared Advanced Chemical Laser (MIRACL) program was the most publicised counterspace laser weapon project by the U.S., with a test performed against an orbiting satellite in 1997. Test results were not made public.[159]
- The Low-Power Atmospheric Compensation Experiment (LACE) satellite was launched in 1990 with the capability to read and understand ground-based laser beams.
- A combined United States Air Force and Missile Defence Agency project was the Airborne Laser (ABL), started in 1996.[160]

The projects and testing have likely been repurposed into other use, following cancellations from budget restructures, or cessation after project completion.[161] Operations of potential high- or low-powered lasers has not been witnessed or reported since the cancellation of the last of these projects in 2011. There is no public evidence suggesting space-based DEW is in development.[162] There has been no further advisement on whether the plans have generated any research or development since a statement made in 2019, so it is an assumption that the U.S. possesses DEW counterspace capabilities based on previous testing from the 1980's.[163]

Russia has had significant technological developments for different laser systems as early as the 1970's. A Space-based high-power laser was developed and experienced a failed launch in 1987.[164] The product, Skif-DM (or Polyus), was built for the purpose of ASAT missions and was using a carbon dioxide laser. There have been no further attempts for a similar mission by Russia since 1991, and it is assumed that it is not being pursued currently.

[158] White Sands Missile Range, "High Energy Laser Systems Test Facility," October 26, 2018, https://home.army.mil/wsmr/about.

[159] William Broad, "U.S. to Fire Laser Weapon at a Satellite," New York Times, October 3, 1997, https://www.nytimes.com/1997/10/03/us/us-to-fire-laser-weapon-at-a-satellite.html.

[160] Secure World Foundation, "Global Counterspace Capabilities Report 2025, p. 77.

[161] Ibid.

[162] Ibid. 20-21.

[163] Patrick Tucker, "Pentagon Wants to Test a Space-Based Weapon in 2023," Defense One, April 13, 2021, https://www.defenseone.com/technology/2019/03/pentagon-wants-test-space-based-weapon-2023/155581/.

[164] "Polyus/Skif-DM", n.d., https://www.buran-energia.com/polious/polious-desc.php

Two air-based systems have been reported on in the last decade. The Beriev A-60 reportedly had test flights in the 2010's, able to detect and track satellites with laser technology to be utilised for targeting purposes. The Sokol-Echelon system was an air-based laser equipped in 2017.[165] This was fitted on a modified transport aircraft, however there was no confirmation of progression to a testing phase.[166]

A mobile laser dazzling system, known as Peresvet, has been in public development for some time. Since the initial statement of development by Russian President Vladimir Putin in 2018, the Peresvet system has been reported to be in an experimental combat operation. It is believed to be capable of dazzling aerial and Space reconnaissance systems that are tracking, attempting to detect, or image military deployments.[167] In 2022, Russian officials claimed that Peresvet – and a more advanced version referred to as Zadira – were in operation during the conflict in Ukraine. There has been no publicly available information to support this claim.

In terms of ground-based laser development, it is believed that Kalina, a code-name for the ground-based laser project, is for the purpose of upgrading the Krona optical Space surveillance systems to incorporate laser dazzling or blinding capabilities.[168] Development of this project is currently unknown.

China has been likely developing DEW for counterspace use. Information on their operational status and current military use is not publicly available.[169] In 2006, it was reported by anonymous U.S. defence officials that ground-based lasers originating from China had dazzled U.S. optical satellites. The previous year, a Beijing University scientific journal made reports of a successful vehicle mounted laser system tested in Xinjiang.[170] U.S. sources published findings from this journal between 2018 and 2022 discuss propositions of:

- Development of reversible and non-reversible counterspace DEW.
- An expectation that ground-based laser weaponry will be operational in China by 2020.
- The Korla/Bohu complex is primarily developing vehicle-mounted dazzling or destructive lasers.
- Space-capable laser systems in development by a research team from Zhejiang University.[171]

[165] Patrick Tucker, "Russia Claims It Now Has Lasers to Shoot Satellites," Defense One, April 12, 2021, https://www.defenseone.com/technology/2018/02/russia-claims-it-now-has-lasers-shoot-satellites/146243/.

[166] Secure World Foundation, "Global Counterspace Capabilities Report 2025, p. 131.

[167] Bart Hendrickx, "Peresvet: A Russian Mobile Laser System to Dazzle Enemy Satellites," The Space Review, June 2020, https://www.thespacereview.com/article/3967/1.

[168] Bart Hendrickx, "Kalina: A Russian Ground-based Laser to Dazzle Imaging Satellites," The Space Review, July 2022, https://www.thespacereview.com/article/4416/1.

[169] Secure World Foundation, "Global Counterspace Capabilities Report 2025, pp. 162-163.

[170] Ibid.

[171] National Air and Space Intelligence Center, "Competing in Space", December 2018, p. 21, https://www.nasic.af.mil/About-Us/Fact-Sheets/Article/1738710/competing-in-space/.

Public and open-source information confirms the research China has conducted. However, the assumed uses of these systems is based on speculation. This does not diminish the likelihood of China developing DEW for counterspace use, or if the country was already in possession of these capabilities.

India reported in 2019 that development of DEWs was in the early stages. The Head of India's Defence Research and Development Organisation (DRDO), G. Satheesh Reddy, stated in 2019 that there was intent to develop 10kW and 20kW laser weapons.[172] However, there is no clear indication if it will be a counterspace capability, or for strict military operations on Earth. At the time of statement, there was no indication if the weapons were primarily targeting aerial or electronic capabilities as well.[173] There has not been an update on the current state of the project, with only news reports advising in 2023 that it is still in development.

France

In 2019, French Minister of Defence expressed support for the placement of lasers on satellites. The lasers would be used to "dazzle those who would be tempted to approach too close," with Parly issuing a statement that the first series of capabilities should be ready by 2025, and an anticipated completion by 2030.[174] Whether the use of the laser weapons would be destructive and/or primarily utilised for countermeasures against offensive targeting systems is unclear. The YODA satellites, currently in development but stated to have significant surveillance capabilities as a form of aggression deterrence, may have DEW capabilities on board.[175] Whilst this would make the satellites capable of dazzling or interfering with other Space objects, there has been no indication of this capability as of this yet.[176]

Case study

In September 2006, the U.S. Department of Defence confirmed that one of their satellites had been illuminated by a ground-based laser from China. There was no publicly reported information on whether the satellite had sustained damage from the event, but the U.S. National Reconnaissance Office (NRO) determined the laser use was for testing purposes.[177] The use of the laser system was supported by Chinese research journals published in 2007, which confirmed targeting of multiple U.S. satellites, not limited to the

[172] Rajeswari Pillai Rajagopalan, "What Are India's Plans for Directed Energy Weapons?", The Diplomat, September 24, 2020, https://thediplomat.com/2020/09/what-are-indias-plans-for-directed-energy-weapons/.

[173] Rajat Pandit, "DRDO Plans Star Wars-style Weapons for Battles of Future," The Times of India, September 14, 2020, https://timesofindia.indiatimes.com/india/drdo-plans-star-wars-style-weapons-for-battles-of-future/articleshow/78096712.cms.

[174] Taylor Mahlandt, "France Wants to Use Lasers to Protect Its Satellites," Slate Magazine, August 1, 2019, https://slate.com/technology/2019/08/france-space-command-plan-satellites-lasers.html.

[175] Chris Flaherty, "The War Satellite Cometh – New Technology Definition Research Note," Space & Defence, December 7, 2021, https://spaceanddefense.io/the-war-satellite-cometh-new-technology-definition-research-note/.

[176] Ibid.

[177] SpaceNews Editor, "NRO Confirms Chinese Laser Test Illuminated U.S. Spacecraft," SpaceNews, October 3, 2006, https://spacenews.com/nro-confirms-chinese-laser-test-illuminated-us-spacecraft/.

impacted satellite from September 2006.[178] Whilst the use of the laser system to dazzle the satellite was debated by officials as concerning and there were calls for further regulation from the U.S., these claims backfired as the United States had fired a chemical laser in the 1990's without regulation. The outcome of the test by China and further actions by the U.S. were not released publicly, except for reports stating the incapacity to discuss the incident with the Chinese Embassy.[179]

What is Australia's takeaway from the first publicised DEW test?

- In the 2020 Force Update, there has been three mentions of developing a framework for DEW capabilities. Since then, Australia has not made an official or publicly available statement for any current development, or if DEW capabilities would be targeted at Space systems.
- Prior to the Force Update, an independent company – Electro Optics Systems – was contracted in 2018 for the development of a laser system for the express purpose of removal of Space debris. However, due to the dual-use of such technology, this could give latent DEW capabilities to Australia. Stationed at Mt Stromlo, Canberra, the joint project between the U.S., Japan, and Australia has not had an update since 2021.

3.1.3 Electronic Measures

Taxonomy and categorisation

Electronic Warfare (EW) is defined as a military action, due to the use of electromagnetic spectrum to disrupt services.[180] Due to the flexibility of EW, it has been a long-term favoured option for counterspace capabilities. Temporary interference to communication streams to or from satellites is possible, with effects also being largely reversible. There is also consideration for its capacity to avoid production of debris in orbit, and with the ability to singly target capabilities of a satellite, only one function could be impacted, such as transponders or frequencies.[181] Required technology is commercially available and considered inexpensive, which has eased accessibility for State and non-State actors.[182]

There are two main forms of EW:

Jamming – Noise that is generated on the same Radio Frequency (RF) band to or from a satellite that causes interference in the data stream. Jammers can target the uplink – or orbital – from Earth-to-satellite, such as the Command-and-Control (C2) orders. Uplink interference can originate anywhere within the satellite antenna receiver. Downlink jammers interfere with satellite-to-Earth communication,

[178] Glenn Kessler, "Bachmann's Claim That China 'Blinded' U.S. Satellites," Washington Post, October 4, 2011, https://www.washingtonpost.com/blogs/fact-checker/post/bachmanns-claim-that-china-blinded-us-satellites/2011/10/03/gIQAHvm7IL_blog.html.

[179] SpaceNews Editor, "NRO Confirms Chinese Laser Test Illuminated U.S. Spacecraft."

[180] Joint Chiefs of Staff, "USG Compendium of Interagency and Associated Terms," p. 299.

[181] Secure World Foundation, "Global Counterspace Capabilities Report 2025, pp. 127-130.

[182] Ibid.

meaning the information received can be impacted. By targeting the ground user of satellite services, a broadcasted RF signal can overpower intended satellite signals for users in a specific area.

Spoofing – When false information is injected into a data stream. This can have false commands issued uplink to disrupt operations. These commands could be in the form of convincing systems that a destination has been reached, when a commercial freight ship or Spacecraft has not moved, or by altering military locations to hide operations. Meaconing is a form of spoofing. By rebroadcasting a time-delayed copy of the original signal, without alterations, it allows this information to be read or delayed. Military GPS systems (P(Y) radio frequency) are often targeted by this EW capability, according to U.S. publications.

Presentation of the threat and potential consequences

Electronic counterspace weapons primarily target communication to and from Earth. By targeting the electromagnetic spectrum that Space systems utilise, the disruption to this can interfere with or jam RF energy. Principle areas of concern for counterspace capabilities that can be affected by EW counterspace are Global Navigation Satellite Services (GNSS), Satellite Communications (SATCOMs), and Synthetic Aperture Radar (SAR) imaging.[183] Whilst communications can generally be restored once the interference stops, the perceived threat of jamming or spoofing communications is a cause of concern for States. The ability for a State to operate navigation services with increased precision, whilst simultaneously denying the same to another, would be advantageous across most sectors. As has been seen thus far, EW has been used to degrade the accuracy of GPS-guided systems in tactical scenarios.

Omnidirectional antennas that are present in devices such as GPS receivers and satellite phones provide a wider angle on the ground, making these systems more susceptible to downlink jamming and spoofing. Combined with the fact that electronic attacks are more difficult to detect or distinguish from accidental interference, it becomes significantly harder to attribute an attack to a State or individual – or determine if there was an actual attack. With reduced awareness about a potential culprit, there is a possibility of increased miscalculation and miscommunication.

Due to its flexibility, low cost, and availability, EW is a highly sought-after military capability. With the expectation that growth of future military systems will incorporate higher cases of autonomy, and increased reliance on satellite systems, having EW capabilities (offensive and defensive) has become significant. Modern militaries provide little public information about EW capabilities and vulnerabilities, as the information is considered highly sensitive. Military Space capabilities, such as military signals of GNSS, are considered more resilient to EW than civilian GNSS signals. As has been stated, EW counterspace capabilities are generally reversible. For military Space capabilities, it is more likely to have a degradation in use, than full denial of access, by operational jamming devices.

Types of Attack	Jamming	Spoofing

[183] Secure World Foundation, "Global Counterspace Capabilities Report 2025, pp. 161

Origin to Destination	Ground-to-Ground; Ground-to-Space; Space-to-Space	Ground-to-Ground; Ground-to-Space; Space-to-Space
Permanence of Attack	Not Permanent	Not Permanent
Scale of Attack Effects	Limited and Regional, dependent on mode of attack	Limited and Regional, dependent on mode of attack
Attributability of Attack	Modest Attribution depending on model of attack	Modest Attribution depending on model of attack
Requires Space Launch Capability	No	No
Requires Space Domain Awareness	No	No

Table 10: Effects of different Electronic Weapons. (CSIS Space Threat Assessment 2025 Report, p. 5)

Ongoing and operational projects in major spacefaring nations

The following assessment is based on publicly available information of current EW capabilities for specific States.

The United States has operational EW offensive counterspace systems. These are deployed globally, able to provide uplink jamming against geostationary Communications Satellites (COMSATs), as part of the Counter Communications System (CCS) programme.[184] Initiated in 2003, the CCS programme was part of a broader counterspace capability development plan. The technical characteristics of the CCS, such as frequency ranges, power levels, and waveforms, are not available to assess nor compare, which is in line with the military secrecy on EW capabilities. It has been believed that the CCS' effectiveness in denying geostationary Satellite Communications Capabilities (SCC) has contributed to a lack of public information. The CCS is a high-priority program for the U.S. military and offers the possibility of COMSAT jamming capabilities.[185] In 2020, the United States Air Force initiated a program to upgrade the CCS. This program would lighten the CCS system load, provide capability to jam at a wider and broader range of frequencies, and use open architecture software to ease the ability to update the programme.[186] It is likely that it is capable of jamming most of the major commercial frequencies (such as C and Ku), the most common military frequencies (X-band), with a possibility of also affecting the Ka-band.[187]

The U.S. Space Force has additionally undertaken EW training sessions. In September 2022, "Black Skies" was initiated, to allow Space Force personnel the opportunity to practice jamming capabilities, especially against commercial satellites. However, there is no confirmed public information on the U.S. military's technical capabilities for offensive jamming

[184] Secure World Foundation, "Global Counterspace Capabilities Report 2025, pp. 20-21.

[185] Ibid, pp. 70-74

[186] Ibid.

[187] Ibid.

(or spoofing) of Positioning, Navigation and Timing (PNT) capabilities following this exercise. The training event is part of a larger series, as "Red Skies" in 2023 had a focus on orbital warfare, and a future "Blue Skies" event wasplanned for 2024 to focus on cyber operations. Additionally, other sectors of the U.S. military have performed EW specific exercises that have taken place in recent years. It can be assumed from previous tests that the United States has effective capabilities for jamming and spoofing of additional GNSS receivers, including the Global Positioning System (GPS), Globalnaya Navigazionnaya Sputnikovaya Sistema (GLONASS), and BeiDou.[188]

Russia's military EW capabilities have been reported on for several decades. Operational experience with the use of counterspace EW capabilities has often been used within Russia to protect strategic locations and VIPs.[189] With a high priority of EW integration into military operations, Russian forces have focused on upgrades for multifunction tactical systems.[190] Their mobile systems can jam specific SATCOM user terminals within tactical range, with an assumed ability of fixed ground stations being capable of interfering with COMSAT uplinks over a wider area.[191]

Reports emerged prior to the Ukraine conflict, that jamming was experienced by ESA's Sentinel-1 radar imaging satellite near the Russian-Ukraine border in 2021. Earlier reports emerged as early as 2015, indicating that Russia had been deploying and testing current EW systems in Syria with the use of the mobile EW system, Krashukha.[192] However, public information on the full scope of Russian capabilities is limited, and most evidence of EW counterspace capabilities has stemmed from recent military operations. With a specific proficiency in downlink jamming, Russia is capable of interfering with guidance systems of Unmanned Aerial Vehicles (UAVs) and Precision-Guided Munitions (PGMs).[193] It is likely to assume Russia does possess the capability to cause uplink interference to GPS satellites, due to developments complementing ground-based stations.[194] As of 2024, there has been no evidence of Russia possessing Space-based EW capabilities.

Russia has developed dedicated systems to protect critical infrastructure. To protect fixed facilities, 250,000 GPS jammers were installed across the country.[195] Mobile EW systems are integrated within military units, such as the R-330Zh "Zhitel" and the "Borisoglebsk-2."[196] These units are reported to be capable of impacting UAVs, cruise missiles, and PGMs. The

[188] Ibid.

[189] Secure World Foundation, "Global Counterspace Capabilities Report 2025, p. 123.

[190] Ibid. pp. 22-23.

[191] Secure World Foundation, "Global Counterspace Capabilities Report 2025, pp. 123-124.

[192] Anna Varfolomeeva, "Signaling Strength: Russia's Real Syria Success Is Electronic Warfare Against the US," The Defense Post, April 30, 2019, https://www.thedefensepost.com/2018/05/01/russia-syria-electronic-warfare/.

[193] Secure World Foundation, "Global Counterspace Capabilities Report 2025, pp. 123-124.

[194] Secure World Foundation, "Global Counterspace Capabilities Report 2025, pp. 123-124.

[195] Brian Wang, "Russia Will Place GPS Jammers on 250,000 Cellphone Towers to Reduce Enemy Cruise Missile and Drone Accuracy," NextBigFuture.Com, April 7, 2017, https://www.nextbigfuture.com/2016/10/russia-will-place-gps-jammers-on-250000.html.

[196] "Sky's the Limit: Russia's Unique Jamming System Getting Upgrade," Sputnik International, December 5, 2016, https://sputnikglobe.com/20161205/russia-electronic-warfare-system-1048187517.html.

Zhitel mobile jammer has been reported to be able to jam commercial Inmarsat and Iridium receivers, with action also seen in recent military conflicts.[197]

Several programs have been in development by Russia, with the intent for more advanced EW capabilities:

System	Deployed	Key Target	Possible Capability
Krashukha-4	2014	Uplink jamming of SAR satellites	Able to counter Airborne Warning And Control Systems (AWACS) and airborne radar systems, reported range of 300km
Tirada-2	2019	Uplink jamming of COMSATs	Able to cause permanent damage to structure and integrity of satellite systems
Bylina-MM	In development	Uplink jamming of COMSATs	Specifically able to target Milstar, GBS, Skynet, Sicral, Italsat, and Sakura satellites
Divnomorye	In development	Integrated EW system	Replacing Krashukha system, able to target air, space, and ground capabilities

Table 11: Examples of Russian Electronic Space warfare capabilities.

It was suggested in late 2019 that Russia might be developing a new generation of nuclear reactors. With the intent to power on-orbit jammers, the program was called Ekipazh, and utilised a Russian company, KB Arsenal, who have experience in developing nuclear reactors for satellites. KB Arsenal was reported to state that jammers would be supported from the nuclear reactors on a wider range of frequencies than had been previously seen. The power of the reactors would enable the jammers to also affect a greater area from highly elliptical or geostationary orbits. Whilst it was not until 2021 that further information on Ekipazh became public, it has not seen any further progress or plans for operational deployment.

China's EW counterspace capabilities and their full scope is difficult to assess through open sources. It is presumed that capabilities against GNSS and SATCOMs are significant, due to a heavy military doctrine on EW as part of broader information warfare.[198] Following a restructuring of Space and counterspace forces in 2015, Space was designated as a part of the military domain, with control over EW and cyber capabilities assigned to the Strategic Support Force (SSF).[199] According to the U.S. Department of Defence (DoD), in 2018, the SSF conducted a series of training exercises, referred to as LUOYANG, with a focus on an EW environment. The full extent of the exercises, including how much involvement Space capabilities had, is uncertain. At most, China is assessed to have proficiency in GNSS jamming capabilities, with both fixed and mobile systems developed and operational. The U.S. Defence Intelligence Agency (DIA) Space and Counterspace Report from January 2019 advised China was in the process of development for two forms of jammers. The first would be able to target SATCOM over a greater range of RF bands, including protected military frequency communications.[200] The second form would be dedicated to SAR targeting,

[197] David Axe, "Russia's Jamming Force Could Isolate Ukrainian Troops—So Artillery Can Destroy Them," Forbes, November 23, 2021, https://www.forbes.com/sites/davidaxe/2021/11/23/russias-jamming-force-could-isolate-ukrainian-troops-so-artillery-can-destroy-them/.

[198] Secure World Foundation, "Global Counterspace Capabilities Report 2025, pp. 24-25.

[199] Ibid.

[200] Ibid, pp. 161-163.

specifically onboard military reconnaissance platforms, including Low Earth Orbit (LEO) satellites.[201] This information is based on non-official material.

The U.S. DIA have also produced reports on China's deployment of EW military capabilities. It is estimated that between April 2018 and November 2019, China had made significant efforts in deploying military EW efforts. Mobile jamming trucks, capable of interfering with GPS or other GNSS signals, were positioned along the disputed Spratly Islands in the South China Sea.[202] In November 2019, multiple incidents of GNSS jamming and spoofing near the Port of Shanghai were reported by civilian populations were reported. Deployment of the capability was clearly monitored and considered unique to previous demonstrations of EW capabilities. Over several weeks, multiple ships were reported to have jumped in position every few minutes in a controlled ring pattern.[203] The uniqueness of the spoofing capability was due to the significant number of ships and GPS systems that were impacted, and with each vessel moved to a different location. Regular experiences of spoofing involve fake signals advising the receiver it is in the same location. The capability has not been seen to such an individual level, which would require significant control and precision.

Iran has demonstrated EW capabilities over the last two decades. Persistent interference with broadcasts from commercial satellites had been noted as early as 2003, with Telstar 12's broadcast of Persian-language experiencing persistent content jamming.[204] Instances of continued jamming of TV channels continued into the early 2010's. The continued jamming escalated to a review by the International Telecommunications Union (ITU), with an order to prevent jamming within Iranian territory.[205] It is unclear how successful this intervention was. Iran has more recently demonstrated EW counterspace capabilities in 2022, with the coordinated jamming of French commercial satellites.[206]

In 2019, public warnings were issued to commercial shipping operators by the U.S. government regarding potential Iranian jamming and spoofing concerns. The warning was limited to GPS interference, bridge-to-bridge communications spoofing, alongside other forms of communications jamming.[207] Speculation on Iran possessing more advanced EW capabilities has been a concern for some time, with a possibility to interfere with satellite-

[201] Ibid.

[202] Michael R. Gordon and Jeremy Page, "China Installed Military Jamming Equipment on Spratly Islands, U.S. Says," The Wall Street Journal, April 9, 2018, https://www.wsj.com/articles/china-installed-military-jamming-equipment-on-spratly-islands-u-s-says-1523266320/.

[203] Mark Harris, "Ghost Ships, Crop Circles, and Soft Gold: A GPS Mystery in Shanghai," MIT Technology Review, June 17, 2020, https://www.technologyreview.com/2019/11/15/131940/ghost-ships-crop-circles-and-soft-gold-a-gps-mystery-in-shanghai/.

[204] Robert Windrem, "U.S. Satellite Feeds to Iran Jammed.", NBC News, October 2003, https://www.nbcnews.com/id/wbna3340692

[205] Peter B. De Selding, "ITU Implores Iran to Help Stop Jamming," SpaceNews, January 19, 2023, https://spacenews.com/itu-implores-iran-help-stop-jamming/.

[206] Jason Rainbow, "Eutelsat Says Satellite Jammers within Iran Are Disrupting Foreign Channels," SpaceNews, March 3, 2023, https://spacenews.com/eutelsat-says-satellite-jammers-within-iran-are-disrupting-foreign-channels/.

[207] Ryan Browne and Barbara Starr, "US government warns of Iranian threats to commercial shipping, including GPS interference," CNN, August 7, 2019, https://edition.cnn.com/2019/08/07/politics/us-warns-of-iranian-threats-to-shipping/index.html.

based C2 signals or GPS signals relying on uplink RF interference. There has been no evidence to suggest that Iran possesses this technology.[208]

North Korea: Despite long-term exhibited capacity to jam civilian GPS signals, the full extent of military EW capabilities from North Korea is unknown.[209] Within limited geographical areas, North Korea has demonstrated downlink interference with civilian GPS navigation as used by passenger aircraft, automobiles, and ship systems, particularly in the area surrounding the South-North border and along coastal areas.[210] Areas affected by the interference are dependent on the power emitted by the jammer and local topography, with some incidents estimated to be in a range of nearly 100kms. There has been no reported effect on GPS satellites directly, nor for the service provided to users outside the range of the downlink jammers, which has contributed to the uncertainty of uplink jammer development from North Korea.[211] Further, the limitation on available information of developing jamming devices against military GPS signals and/or satellite communications has prevented any reporting on possible development, testing, or use.[212] There is one report about North Korea possibly jamming military communications from a South Korean satellite from 2012, however development since then is unknown.[213]

Other: For countries that have stated intention to develop EW capabilities, please see the table below:

Country	Current Status
India	• Developed indigenous offensive EW systems, including Samyukta and Himshakti. • Demonstrated capabilities against Pakistani radars and communications.[214]
France	• Possesses terrestrial-based EW capabilities, full capabilities are unknown and no information if has been deployed offensively.[215]

[208] John Hudson, "Nobody Knows if Iran's Drone Hack Was a Hoax," The Atlantic, October 30, 2013, https://www.theatlantic.com/international/archive/2012/04/nobody-knows-if-irans-drone-hack-was-hoax/328944/.

[209] Secure World Foundation, "Global Counterspace Capabilities Report 2025, p. 222.

[210] Choe Sang-Hun, "North Korea Tried to Jam GPS Signals Across Border, South Korea Says," The New York Times, April 1, 2016, https://www.nytimes.com/2016/04/02/world/asia/north-korea-jams-gps-signals.html.

[211] Ibid.

[212] Julian Ryall, "North Korea 'Aggressively' Jamming BBC'S New Korean-language Service," The Telegraph, September 27, 2017, https://www.telegraph.co.uk/news/2017/09/27/north-korea-aggressively-jamming-new-bbc-broadcasts/.

[213] Martyn Williams, "Report: DPRK Jams South Korean Satellite Comms," North Korea Tech - 노스코리아테크, November 17, 2012, https://www.northkoreatech.org/2012/11/17/report-dprk-jams-south-korean-satellite-comms/.

[214] Lt Gen R S Panwar, "Future WarsIndia's Space Programme: Organisations and Warfighting Potential," Future Wars, November 18, 2021, https://futurewars.rspanwar.net/indias-space-programme-organisations-and-warfighting-potential/.

[215] Secure World Foundation, "Global Counterspace Capabilities Report 2025, p. 194.

Japan	• In FY2020, a ¥4.0 billion (AUD $41 million) programme was submitted to develop offensive EW capabilities, goal of completion slated for mid-2020's.[216]
South Korea	• Was included as an area of development in the Space Odyssey 2050 program, released in 2020. No further update available.[217]
United Kingdom	• No publicly available information to advise if developing or considering development of EW capabilities.

Table 12: Electronic Space warfare capabilities for other States.

Case study

Between October and November 2018, a large-scale miliary exercise was hosted in Norway. The Trident Juncture exercise included military personnel from 31 different countries: 29 North Atlantic Treaty Organisation (NATO) members, plus Finland and Sweden, were in attendance.[218] Air, land, and maritime operations were incorporated, for the purpose of ensuring NATO's strength, credibility, and commitment to a unified membership.[219] Located along the west coast of Norway, the Bodø Air Base was used during the exercise, hosting aircraft and tankers from countries including France, Greece, and Spain.[220]

Why is the Trident Juncture Incident relevant for Australia?

- The range of the jamming, 730km, is nearly equivalent distance between a boat stationed off the coast of Port Moresby, Papua New Guina, to Port Douglas, Queensland, Australia
- Along the northern coast of Australia, allies are hosted for training exercises (i.e. U.S. in 2022), which could be exposed to EW jamming
- EW jamming capabilities can be mobile, including air- and sea-based, and per above case study, can operate for an unprecedented timeframe affecting military and civil operations

Due to population density in coastal areas, there is a high risk to civilian operations and infrastructure, including airport traffic and emergency services, as seen in this case study

GPS signal loss was reported by military personnel within hours. Alternate routes were taken by air forces from representative countries or were grounded entirely during the exercise. Civilian reports surfaced during the military exercise that GPS signal jamming had occurred

[216] "Japan Requests Record $50 Billion Defense Budget in Eighth Straight Increase," The Defense Post, July 26, 2020, https://www.thedefensepost.com/2019/08/30/japan-record-defense-budget-50-billion/.

[217] Andy Hong, "South Korea's Space Program Is a Big Deal," The Diplomat, July 1, 2022, https://thediplomat.com/2022/07/south-koreas-space-program-is-a-big-deal/.

[218] Leigh Hartman, "31 Countries Come Together for NATO's Trident Juncture," ShareAmerica, November 2, 2018, https://share.america.gov/31-countries-come-together-for-natos-trident-juncture.

[219] Jonathan Masters, "NATO's Trident Juncture Exercises: What to Know," Council on Foreign Relations, October 23, 2018, https://www.cfr.org/article/natos-trident-juncture-exercises-what-know.

[220] "Bodø Air Base – Backbone of Trident Juncture's Air Component," Allied Air Command, November 4, 2018, https://ac.nato.int/archive/2018/bodo-air-base.

a week prior to the arrival of personnel, in Tromso and Lyngen.[221] There were no reports of incidents during the exercise due to the loss of signals, and civilian reports stemmed from loss of mobile phone functionality to delays and divergences at airports from emergency services.[222] However, Russia operated missile tests off the same coast towards the end of the NATO exercise. It was reported that Russian forces were operating at the Pechenga military base, an estimated 730km away from the Bodø Air Base, when the GPS jamming occurred, prior to their own missile tests, however this was officially outside of military operations.[223]

hat is Australia's position on EW measures?

- In 2021, Australia announced Defence Project 9358. With the intent to explore and expand options for ground-based EW counterspace capabilities, Australia's position aligns more with protecting satellites.[224]
- There is a primary focus on non-kinetic counterspace options, with EW being a part of that, however, there has been no information on where the project currently is. The last update was in 2023 with then-Defence Space Commander Catherine Roberts, who did not provide a timeline on when Australia would have those specific EW capabilities.[225]
- Significant policy changes with goals of developing national security Space capabilities does not give a specific timeframe, however it does suggest Australia will have initial EW counterspace capabilities.

It does appear that there is serious interest in having the option to use nascent EW counterspace capabilities, so having minimally operational systems would support this.

3.1.4 Cyber Measures

Taxonomy and categorisation

Cybersecurity is a popular term used in today's age of modern technology, but what is cybersecurity really and what does it mean for Space? The cyber domain and Outer Space share many commonalities. They are both open, shared, limitless, cross-border, and unregulated domains. Cyberspace is often described by having three layers and an attack on one can affect the others. The physical layer is the equipment and infrastructure – hardware, data centres, satellites. A logical/software layer – the lines of code, binary information. And a cognitive or social layer – the actual information, digital content and data exchanges in cyberspace, as well as end users. This means that outer Space can be attacked

[221] Kjell Persen, "- Det Er Som å Bli Blind Uten Forvarsel, Og Da Er Det for Sent," TV 2, February 11, 2019, https://www.tv2.no/nyheter/10395618/.

[222] Kjell Persen and Roy-Arne Salater, "Ambulansefly Kunne Ikke Lande Etter GPS-utfall," TV 2, February 11, 2019, https://www.tv2.no/nyheter/10397144/.

[223] Gerard O'Dwyer, "Finland, Norway Press Russia on Suspected GPS Jamming during NATO Drill," Defense News, November 16, 2018, https://www.defensenews.com/global/europe/2018/11/16/finland-norway-press-russia-on-suspected-gps-jamming-during-nato-drill/.

[224] "Defence explores options for Space Electronic Warfare", Australian Department of Defence, n.d., https://www.minister.defence.gov.au/media-releases/2021-07-29/defence-explores-options-space-electronic-warfare

[225] Colin Clark, "Aussie Space Command Looks to Electronic Warfare, Other Tech to Deter Attacks on Satellites," Breaking Defense, March 2, 2023, https://breakingdefense.com/2023/03/aussie-space-command-looks-to-electronic-warfare-other-tech-to-deter-attacks-on-satellites/.

not just physically, but also through the technology which is used to monitor, protect, and advance modern society.

According to the Secure World Foundation, four categories of cyberattacks on space systems exists: the first category relates to security breach in the supply chain. This is where faulty or counterfeit microelectronics or material produced internationally have deliberate installations of hidden backdoors. A second category involves attacks directed against the links joining satellites and ground control. Most often these are man-in-the-middle (MITM) involving the attacker inserting themselves between sender and receiver. This MITM type of attack allows information passing between satellite and ground control to be read, interrupted, destroyed, gathered, encrypted, or changed. The third category is made of attacks on terrestrial C2 or data relay stations. Fly-overs with manned aircrafts, unmanned aerial systems (UAS), or weather ballons which can cause signal disruptions or hijackings through proximate positioning of the broadcasting equipment, gaining access to the structural internet or ethernet cables, or piggybacking off the stations data relays. Finally, other attacks target the user of a Space system, either the terminal, the device, or the satellite signal. These attacks are often similar to cyberattacks against computers, which exploit hardware and software vulnerabilities.

The Centre for Strategic & International Studies's (CSIS) 2025 report the Space Threat Assessment understands a cyberattack on Space systems can result in the loss of data or services which are provided by satellites. The disruptions caused by cyberattacks can have widespread systematic effects if used against GPS, energy and telecommunications companies. An attacker could shut down communications and permanently damage satellites by issuing commands which could cause damage to the electronics propellant or sensors. Cyberattacks can become difficult to attribute as complex methods of concealing their identity can be used such as concealing the IP address, leaving small traces of activity, or making no public announcements in the aftermath. According to North Atlantic Treaty Organisation (NATO) Joint Air Power Competence Centre (JAPCC), cyber threats on Space systems are growing with attacks from criminal, terrorist groups, foreign nations, insiders, and more. When new technology, pieces of equipment, or software updates are introduced to the system, there are new vulnerabilities which can be exploited in a cyberattack. Attacks on Space systems can be categorised by the points of entry on the attacks surface, distinguishing between various segments: Ground segments, which consist of all ground elements of Space systems including command, control, and mangement of the satellite itself and the data arriving from the payload and being delivered to the user. Link segments, which consist of the signal transmission between the satellite and the ground sation, as well as between satellites.

The SmartSat Cooperative Research Centre (CRC) released a Satellite Cyber Resilience Whitepaper in 2022 which illustrates the importance of monitoring and protecting Critical Space infrastructure. SmartSat CRC have two space related taxonomies. The first is Critical Space Infrastructure, defined as any infrastructure on which society has a critical dependency on, and if disturbed, could cause significant and potentially catastrophic

consequences to the safety or security of that society.[226] Examples of such infrastructure include systems which rely on satellites for vital functions like time, location, guidance, communications, and sensory data. Air traffic control, banking, and emergency services are all institutions which rely of critical infrastructure that could be affected in the event of a cyberattack.

The second is Space Resilience Taxonomy. Plotnek and Slay explain (2022)[227] this taxonomy as follow:

- Anticipate refers to the satellite system's resilience-enhancing mechanisms in place to prevent, detect and avoid HILF cyber events;
- Survive refers to the satellite system's resilience-enhancing mechanisms in place to mitigate, absorb and withstand the impacts of the HILF cyber event;
- Sustain refers to the satellite system's resilience-enhancing mechanisms in place to contain any impacts and preserve core functions during a HILF cyber event;
- Recover refers to the satellite system's resilience-enhancing mechanisms in place to respond, restore operations and 'bounce back' from a HILF cyber event;
- Adapt refers to the processes and procedures in place to reflect on lessons learned and adopt new mechanisms to increase resilience for any similar cyber events in the future.

Presentation of the threat and potential consequences

There are only a few cyberattacks against satellites publicly known. This is often because making a public announcement that a cyberattack has occurred installs a sentiment of mistrust from the public. Companies often avoid publicising such an attack to keep their customer base.

Cyberattacks can be used to target a diversified set of stakeholders, such as civilian or military satellites, satellite manufacturers, parts suppliers, software brokers, or launch service providers.[228] Any such cyberattack could include theft, alteration, or denial of information, as well as control or destruction of satellites, their subcomponents, or supporting infrastructure.[229] Cyber-attacks are often man-in-the-middle (MITM) attacks,[230] an umbrella term that involves an attacker inserting themselves between the sender and receiver, thus able to interfere with information either before a transmission is sent to the satellite or after the satellite has responded. It is also possible - although often very difficult - to use a cyberattack against the command-and-control (C2) link to gain access to the satellite bus or the payloads.[231] Cyberattacks on Space assets are increasingly of concern with the exploitation of satellite links having become more prominent to facilitate the hacking of an adversary's

[226] Smartsat CRC, "Satellite Cyber Resilience White Paper – Technical Repoprt", 2022, https://smartsatcrc.lbcdn.io/uploads/Satellite-Cyber-Resilience-Whitepaper-FINAL.pdf

[227] Ibid.

[228] Ibid, p 195.

[229] Ibid, p 179.

[230] Ibid, p 195.

[231] Ibid, p 182.

Space system.[232] To launch a cyberattack in this modern era does not require a complex knowledge of the technology or know-how and because of this there is an increase in attempts of cyberattacks.[233] The equipment needed to conduct cyberattacks is readily available at a local hardware store and the instigator does not require advanced technical skills.

Cyber			
Types of Attack	Data Intercept or Monitoring	Data Corruption	Seizure of Control
Attribution	Limited or uncertain attribution	Limited or uncertain attribution	Limited or uncertain attribution
Reversibility	Reversible	Reversible	Irreversible or reversible, depending on mode of attack
Awareness	May or may not be known to the public	Satellite operator will be aware; may or may not be known to the public	Satellite operator will be aware; may or may not be known to the public
Attacker Damage Assessment	Near real-time confirmation of success	Near real-time confirmation of success	Near real-time confirmation of success
Collateral Damage	None	None	Could leave target satellite disabled and uncontrollable

Table 13: Effects of different types of Space cyber attacks (CSIS Space Threat Assessment 2023 Report, p. 7)

Ongoing and operational projects in major spacefaring nations

In the table below are simplified case studies of cyberattacks that have occurred. Each have a specific reference to the type of attack – e.g. an attack on a ground system, stolen data, or data leaks - which can be used as exemplars to understand where the attacker was able to infiltrate and deliver the attack, what occurred in said event, and who was affected.

Case study

On the 24th of February 2022, a planned cyberattack on ViaSat's KA-SAT took place. ViaSat is a high-speed satellite internet provider who operates out of Europe, with services provided worldwide[i]. The attack affected tens of thousands of customers across Europe, with 40,000 to 45,000 modems going silent, and some modems unable to be reset remotely. Around 9,000 subscribers of NordNet – a French telecommunication company – were without service. A third of British broadbands provider BigBlu users – a subsidiary of Eutelsat – where affected in France, Hungary, Greece, Italy, Poland, and Germany. The German energy company Enercon experienced a loss of connection with their fleet of 5,800 wind turbines, however the only issue experienced was the ability to monitor the turbines remotely – there was no loss of energy to the turbines or any reports of power outages in relation to the Viasat cyberattack.

[232] Ibid, p 184

[233] Ibid, p 185.

This loss of remote connectivity was because SCADA, the system who Enercon relied on, was managed by the KA-SAT's network. In addition, the attack led to a mass loss of internet to customers in Ukraine – including the Ukrainian Government, the army, and security services. Directly following the outage, the Ukrainian Government publicly called upon Starlink's owner, Elon Musk, to provide temporary broadband access to aid the defence of Ukraine. Musk then repositioned thousands of Starlink's constellation terminals to assist in restoring connectivity.

Following an analysis of the incident ViaSat stated on March 30, 2022, that they 'believe the purpose of the attack was to interrupt service' rather than taking or destroying data[iii]. The company also stated that 'there is no evidence that any user data was accessed, nor any personal information compromised, or any impairment to the satellite and ground infrastructure'. After a joint investigation with Eutelsat, Skylogic, and allied partners into the attack, ViaSat said that the attackers had gained remote access to the network via the exploitation of a misconfigured VPN device [iv].

In the months following its first statement, ViaSat collaborated with the European Union and the Five Eyes (Australia, Canada, New Zealand, United Kingdoms, and the United States) to investigate who caused the attack. These first statements asserted that the cyberattack on the Viasat communication satellite had traces of AcidRain, a wiper malware, used by the Russian Military Intelligence (GRU) in pervious cyberattacks such as WhisperGate. This led the joint investigation team to attribute the attack to the Russia military. On May 10, 2022, a statement with Viasat, the EU, and supported by international partners condemned the "malicious attack" on the KA-SAT satellite, owned by Viasat conducted by the Russian Federation. Estonia, Denmark, Ireland, the Netherlands, Norway, Austria, Germany, Czechia, Italy, Finland, Romania, Poland, and France released similar statements which aligned with this attribution.

Impact overview of attack on ViaSat's Satellite			
Case-specific	Impact Type	Context	Consequence
	Geographic Impact	• Broadband providers across Europe were impacted	• No connectivity
	Societal impact	• Civilians experienced internet outages • Ukrainian internet took longer than the rest of Europe to restore • Absence of satellite connectivity	• Unable to connect with relatives during a time of war • Civilian population went without reliable access to information, connectivity, access to digital public services during the conflict • Leaving citizens under Russian internet rule

	Operational impact	• Recovery time varied • Wind turbines in Germany lost remote control access • No satellite connectivity in Ukraine	• Some internet access took months to restore, many modems had to be replaced • Not able to control turbines remotely
	Military impact	• Loss of connectivity • No back-up solution in case of destruction of terrestrial systems • Potential difficulty in exchanging between the strategic, operative and tactical levels • Impact on OODA loop	• Delay while waiting for Starlink to be operational • Unable to communicate between military departments during a declaration of war
	Legal impact	• Nothing currently	• No justice for stress and loss of life

Table 14: The ripple effects of the Viasat KA-SAT cyberattack

The Viasat KA-SAT cyberattack demonstrates the widespread impact and ripple effect of a single attack on a Space system. This attack, which targeted military and civilian users in Ukraine, ended up having a wider geographical impact on infrastructures and users across Europe. The attack also led to a social impact, leaving users without internet connection for a long period of time.

How could a cyber-attack of this scale become a reality for Australia?

- A similar attack to the Viasat may happen to an Australian commercial system, such as the dual-use Optus C-1, which provides services to the Australian DoD and civilian customers at any time. Increase in cyberattacks demonstrate the need to have a proactive approach to satellite cybersecurity in Australia to anticipate these types of threats, including an action plan if such an attack occurs.
- As Australia does not have sovereign satellites, civilians are at risk if there were an attack on allied satellite that Australia shares access to.
- Government, military, and other critical infrastructure have already been exposed to a large-scale cyberattack which originated from within Australia - by a private youth citizen.
- Current Government response is to review existing law (critical infrastructure act 2018) with new protocols for commercial actors entered into effect, however military infrastructure, including satellites, has not been publicly addressed.

3.2 Defensive Measures for Space Control

As offensive counterspace capabilities advance, so too do the measures used to prevent and deny them. Different types of defensive measures can be used in prepare for prevent, or mitigate the damage of an attack, or in direct response as an active defence, a retaliation, or a means of recovering operational capabilities post-attack. This section provides an overview of the types of protections which can be deployed against counterspace – from the technical measures involving software or hardware solutions, to the wider operational practices embedded across a system, right up to the use of policy, legal and diplomatic tools which used to deter threats or limit the potential and scale of escalation.

3.2.1 Technical Measures

With the incorporation of technologies to prevent or deny primarily offensive electronic capabilities, the category of technical defences has grown. As defences can be incorporated into satellites, ground stations, and user equipment, the versatility and variety of technologies has helped establish several protective measures.

Defence through Monitoring

Space Domain Awareness (SDA)

SDA is considered the baseline requirement for enabling defence and protective measures. With the ability to identify and track Space objects, and predict where objects will be, this gives States key information for reactivity.[234] It allows for the characterisation of a Space object's capabilities, how it is being used, and can assist with characterisation of accidental and intentional actions in Space.[235] SDA is not limited to identification and tracking, as it also assists with assessing intents of a system. As SDA systems include terrestrial-based optical, infrared, radar systems, and Space-based sensors, the need to develop and update capabilities is high due to the diversity of sensors utilised by States and non-State actors.

To provide an advantage in decision-making to a state, improvement of SDA is a must. There have been recent suggestions of using AI for this purpose. Yet to be publicly tested, it is predicted that AI can enhance SDA capabilities through pattern-based behaviour tracking. In the event of abnormal behaviours being detected that may be missed by human analysts, AI has been able to identify, track, and predict additional Space objects, broadening awareness of the domain.[236] With regards to satellites, AI could allow for better use of operational capabilities, such as manoeuvrability and faster response time to commands.

Space-based Radio Frequency (RF) Mapping

Space-based RF mapping is complimentary to SDA capabilities. By allowing operators to monitor and analyse the RF environment, a more complete understanding of the Space

[234] Sandra Erwin, "Air Force: SSA is no more; it's 'Space Domain Awareness'," Space News, November 14, 2019, https://spacenews.com/air-force-ssa-is-no-more-its-space-domain-awareness/.

[235] Sandra Erwin, "Space Force needs sensors to distinguish weapons from benign objects," Space News, January 6, 2021, https://spacenews.com/space-force-needs-sensors-to-distinguish-weapons-from-benign-objects/.

[236] Mark Dickinson, "A Space Data Association Focus: The current state of Space Situation Awareness (SSA)," Sat Magazine, January 2019, http://www.satmagazine.com/story.php?number=1895054050.

environment is achieved. It provides the capability of distinguishing between intentional and unintentional interference of RF energy and is more exact in detecting and geolocating origins of electronic attacks. With the increased ability to characterise jamming and spoofing attacks from Earth or other satellites, space-based RF mapping has the advantage of allowing defences to be employed quickly and effectively. One of the attractive aspects of this capability is that it is effective for timely responses; the faster a threat can be detected, identified, and characterised, the more valuable and quicker information is utilised to enable defensive capabilities.

The growth in transparency of the space environment is due to contributing commercial non-State actors. Private companies – such as HawkEye360, Spire Global, and Unseenlabs – have utilised constellations of satellites to monitor RF signals in Space, allowing for RF data to be analysed for geolocation capabilities and changes in the Space environment.

Physical Defence

Electromagnetic shielding

The volatile background radiation of the space environment poses a threat to satellites. Degradation of components over time is anticipated, however it can vary between each satellite due to the vulnerabilities, manufacturer, and model. There is also the presented threat of HPM attacks and electromagnetic pulse weapons that could be used offensively also represent a threat. For effective and sustained long-term use of satellites, to also protect core components such as memory chips and internal processors, resistance to radiation has seen development been developed by States. By surrounding electronics and cables within a satellite with shielding and surge protectors, with recent combinations of metals used such as tungsten and tantalum with more traditional aluminium and lead, the density of the metals can deflect low-energy electrons and gamma rays. Other shielding components that have been utilised, often in conjunction with metals, include plastics such as polyethylene and nylon, composites such as carbon fibre reinforced polymer and boron nitride nanotube, and water tank circulations.

However, the additions of protections to satellites can impede operations. Increased weight and complexity with shielding can impact stability and longevity of a satellite in orbit, but also initial launch capability and cost. The effectiveness of shielding is also hindered by high costs for materials, but also requirements for careful processes, testing, and validity validation of outcome.

Antenna nulling and adaptive filtering

The introduction of antennas that ‘null’ or minimise signals, or adaptive filtering of specific RF bands can protect satellite operations. With the protection from Earth-to-satellite or satellite-to-satellite signal receiving, the antennas fitted to satellites reduce the experience of jamming or remove it entirely. Nulling of signals is specifically useful when the origin of a jamming signal is from known geographic locations, such as those generated by States (North Korea, Iran, China). Alternatively, the use of adaptive filtering is not limited to known origins of jamming, as it blocks identified frequencies used for interference. This means that transmissions can continue to and from the satellite, with the additional noise filtered out of the signal.

As with other systems of technical measures, the introduction of antenna nulling and adaptive filtering does come with risks. Nulling does pose the risk of blocking friendly transmissions should they fall within the scope of the antenna. Should a jamming signal be within range of a friendly transmitter, the antenna would not be able to accurately block the jamming signal without blocking legitimate users. Adaptive filtering is also inefficient when a wideband jamming signal is utilised. Should a significant portion of the RF spectrum that is used for filtering out jamming frequencies be used, the operational performance of the filter suffers due to higher-than-anticipated performance. This can pose a risk to the long-term use and degradation of system.

Filtering and shuttering

The implementation of filters and shutters on remote sensing satellites can provide protection from laser dazzling and blinding. By restricting certain amounts of light to reach sensors, filters limit the possible damage that can be experienced from unwanted wavelengths. Shutters in turn react to the detection of threats or anomalies, such as when a threshold of received light is programmed. This allows for the blocking of light – or diversion to a specific sensor – limiting damage received.[237]

These two capabilities do carry similar drawbacks as shielding. Increased weight and complexity of satellites create multi-factor issues as previously stated. With a need for also understanding the technical capabilities of counterspace weaponry, at the very start of the development of a satellite, filters do pose the risk of blocking wavelengths that are intended to be read. This can be due to lasers operating at the wavelength to which the satellite mission is set, which can be a complex and specific offensive procedure, but is still a possibility. The shutter system can also interrupt the collection of data. Whilst temporary, there is a possibility for satellites to not react to the lack of threat quickly, or in the instance of HPM weaponry use, if generated heat is programmed as a threat, the shutter may not deactivate or be impacted and remain closed.

Defence through Algorithms

Jam-resistant waveforms

The ability to utilise a radio wave, or waveform, for the transmission of encoded data affects the outcome of jamming or spoofing. Different types of military or civilian waveforms can be used to improve resistance to EW, such as the commercial C- and Ku-band, and the military Ka-band. There are also two types of actions using RF bands that can assist with protection against EW capabilities. One of these actions, Frequency Hopping Spread Spectrum (FHSS), is when RF transmissions are rapidly changed using a mostly random pattern. This prevents a jammer from matching the RF band of the transmission.

Interleaving is the other form of a protective action using waveforms with the purpose of controlling data errors. The interleaving process applies the controlled errors to the data before it is transmitted, corrects them once the data is received, before applying the correction algorithm. This is to reduce the effect of RF interference, which impacts the data in

[237] David Wright, Laura Grego, and Lisbeth Gronlund, "The Physics of Space Security", American Academy of Arts & Science, 2005. p 128.

a transmission by generating more and irregular errors than a correction algorithm can manage. By overwhelming the correction algorithm with errors, the data becomes corrupted. With the control of errors and what is provided to corrective algorithms, the corruption risk is reduced.

As with all techniques, it does not make a system or operation full proof. By controlling the interactivity of the data stream on the waveform, this helps reduce the likelihood of interference. But if a high-powered wideband jammer was utilised, due to the increased interference across the spectrum of frequencies, FHSS can be ineffective and still have the data experience jamming. Latency issues from interleaving due to the requirement to reassemble data prior to the correction algorithm being utilised can be perceived as an issue and prevent the use or consideration for the technique.

Encryption and air-gapped systems

Encryption of data transmissions is considered standard practice for State actors in Space. Due to the risk posed to command-and-control data streams Earth-to-satellite, as well as any information received satellite-to-Earth, including imaging, the protection of uplink and downlink streams is vital for operations. RF transmissions are inherently exposed despite efforts of encryption, so the addition of previously discussed techniques is likely to assist with further protections. With the threat of cyber-attacks to and from satellites, and with previously seen events of interference such as with the ViaSat incident, consistent and up-to-date encryption is a necessity to protect systems.

Air-gapped systems as an additional form of cybersecurity have the benefit of being separated from the public internet. Unless insider help is provided, air-gapped systems are harder to breach due to the lack of accessibility, and often a combination of encryption and privacy in place. However, Space systems are not always functionally benefited by having an air-gapped system, as the data produced is for the express purpose of public consumption. This data could be produced by weather satellites, imaging satellites by commercialised agencies, or communications to and from satellites. The additional working load of separating data for public consumption and private ownership can make air-gapped systems financially unfeasible.

Encryption standards of State Space actors are not always the standard of commercial operations and international partners. The expectation of quality of security and encryption can be outweighed by the reality of commercial operations having ineffective cybersecurity. Australia's communications provider, Optus, experienced two outages in 2022 and 2023, affecting nearly 10 million people, civilian and government operations, and resulting in private identification material being held ransom. Optus maintains denial that the 2023 outage was due to a cyberattack, despite ongoing investigations into lack of cybersecurity. It is worth noting in this instance that Australia restructured the Security of Critical Infrastructure Act 2018 following the 2022 breach, with the addition of requiring telecommunication providers to report to the Government within 72 hours of an alleged cyberattack.

Encryption algorithms, much like in the Optus Outage 2022, can be exploited due to flaws or breaks in script. With the presence of quantum computing for instance, higher processing speed of these systems can brute-force the gaps in an encryption key. There has been a push for quantum-proof encryption to be developed faster and more effectively, as the

additional benefit is diminishing the threat of cyberattacks by humans as well.[238] The ability to compromise an encryption key through loss experienced by sensitive hardware or software also limits utility. The systems would need to be capable of rapid and secure configuration for encryption rekeying. This also assumes that systems would also allow processing for this purpose, despite any loss.

Should Australia look to invest in industry development for technical measures?

- Essentially most of these defences are high cost, with increasing interference with satellite operations
- As Australia doesn't have sovereign satellites, development of the physical defences like shielding and shuttering do not appear to be necessary
- SDA is a prime area of defence highlighted by the DoD for development and industry growth however it is reliant on satellites and defences
- If a development pathway was put in place for the purpose of SDA capability growth and defensive development, Australia would likely see a return, even if the development of defences was for the purpose of protecting terrestrial operations from DEW and EW offensive capabilities to allow for controlled testing and economic understanding

3.2.2 Operational Measures

Operational measures against counterspace technology are passive ways of preventing the targeting of satellites. These measures prevent targeting abilities through satellite behaviour and operation, with increasing resistance and restorability.

Architectural Defences

Disaggregated Constellations

By separating missions onto different platforms or payloads, the fundamental idea of disaggregated constellations is to reduce complexity. With the benefit of increasing the acquisition of data, satellites that have been separated into individual missions – together making up the whole overarching mission – operate in parallel and have a focused task, as opposed to balancing multiple orders. The separation of the mission between satellites can also contribute to reducing unintended escalation, should the incorrect system (strategic or tactical) have been targeted in a conventional understanding of conflict. By forcing an attacker to be explicit about what capability is being targeted, disaggregated constellations are also done with the express purpose of having a strategic and tactical system operational separately but working in parallel. An unintended side effect of this defence is that an attacker may not trust the information on what is explicitly tactical or strategic and opt to not attack. An example of this defence is the U.S. Space Force's plan for the separation of the current SATCOM system into two entities: the Evolved Strategic SATCOM (ESS) system, working as a strategic support for the Protected Tactical Service (PTS) tactical system.

However, disaggregated systems are costly in comparison to other constellation defences. With the need for development of separate space systems, alongside the capability to launch

[238] William Cummings, "An adaptive nulling antenna for military satellite communications," Lincoln Laboratory Journal 5, no. 2 (1992), 174.

the systems almost simultaneously, this can cause issues with costs, testing, production, and development stagnating.

Distributed Constellations

With the express intent of having multiple satellite nodes working together to perform the same mission, or function, as a single node, distributed constellations benefit the end-user. No single satellite within the constellation is solely responsible for the capability, meaning that the loss of a single or multiple satellites would not end the mission or function. This defence also provides a larger number of targets to attacks, with the outcome of a successful attack requiring a higher number of satellites to be impacted to have the same effect as non-distributed satellites or constellations. An additional benefit of this defence is the possibility to use less complexly made satellites, due to the distribution of a capability between multiple nodes. The current GPS system is an example of a distributed constellation, as the functioning system is not dependent on a single satellite or ground station.

However, a major concern for the existence of distributed constellations is the possibility of increased Space traffic. Due to the significant number of satellites within a constellation – such as the commercial Starlink constellation containing over 4,000 satellites – and the intention of continually growing this form of defence, the concern for lack of Space Traffic Management is apparent.[239] Increasing the size of distributed constellations may cover a greater range and offer the benefit of transferring end-users between nodes without disruption, but the sheer number of those constellations, particularly in LEO, has already seen pushback due to their negative outcomes. Particularly in the cases of degradation of satellites, wherein the removal of those satellites is limited by the lack of complexity within the other satellites of the same constellation, but also the generation of debris if satellites in a distributed constellation were attacked, giving rise to the possibility of a significant debris field that could impact the remainder of the constellation.

Proliferated Constellations

With the distribution of a larger number of the same types of satellites in a similar orbit with the same mission, there is the possibility of a crossover with other defences. However, the concept of a proliferated constellation lies in the intent to gradually build more systems over time to increase the existing size and capacity of a constellation. Additionally, the maintenance of on-orbit spares also contributes to the size and capacity of a proliferated system. The protection provided by a proliferated system is due to the sheer size and necessary attack that must be mounted for an effect on the end-user. The U.S. military Wideband Global SATCOM (WGS) system is an example of this defence, having grown from three satellites to the planned constellation of eleven.

As with other constellation defences, there is a significant cost involved. However, proliferated systems differ depending on the learning curve and experience gained from gradually developing and deploying satellites for the system. Were there singular satellites being developed, there is the possibility of individual costs outweighing the benefits, particularly in

[239] Mike Stone and Joey Roulette, “SpaceX’s Starlink wins Pentagon contract for satellite services to Ukraine”, Reuters, June 2023, https://www.reuters.com/business/aerospace-defense/pentagon-buys-starlink-ukraine-statement-2023-06-01/.

the time between each launch. Understanding the gradual development of technology which can aid and maintain a proliferated system overall can offset that cost, particularly if planned.

Diversified Architecture

By taking a proliferated constellation a step further, diversified architecture also utilises different orbits or domains. The diversification of orbits or domains used by satellites that contribute to the same mission reduces the effect of an adversarial attack. If a loss was experienced in one orbit or domain, a satellite from another orbit can be moved to compensate for that loss. This can effectively be a significant defence by itself, as it would render a waste of resources of an attack, but also presents the possibility of different capabilities being needed depending on the orbital regime of a satellite. Furthermore, the collateral damage from an attack, such as orbital debris, could be a greater threat to all. The Chinese BeiDou system is an example of diversified architecture, with Positioning, Navigation and Timing (PNT) utilising multiple orbits, such as satellites in geo-stationary orbit (GEO) and medium Earth orbit (MEO).

Redundant, Mobile, or Hardened Ground Stations

Ground stations are at risk of an attack due to the operations that they enable, including C2. Rapidly deployable ground stations – alternatively referred to as redundant or mobile – are effective in allowing the station and operations to be moved in event of an attack, or due to the threat of natural disaster. The impact of kinetic or non-kinetic attacks is reduced for the Space system, as it would not be dependent on a singular location or station. Hardening of ground stations and local infrastructure that may be utilised also reduces the effectiveness of potential attacks. Using additional materials or a variety of methods in the development of a permanent structure increases longevity and can also provide protection from offensive EW capabilities (depending on materials used).

To make use of the manoeuvrability offered by mobile stations, a high degree of precise SDA is required. It would be anticipated that effective SDA capabilities would determine if an attack was to occur, to allow for accurate responses. Training of users to make use of mobility and timeframes also impacts the functionality of mobile stations, and high costs for the development of structures would impede deployment. For permanent ground stations, to make full use of specific materials for resistance to kinetic – and possibly non-kinetic – attacks requires development and readily available materials at the building stage. Most structures can be assumed to not be in a position of having accessibility to rebuild areas with hardened materials, and at most, local infrastructure such as wiring and plumbing, may be re-laid with materials – again depending on availably and costs.

Can Australia benefit from any architectural defences?

- Due to a lack of sovereign, autonomous industry development for own satellites for the purpose of communications, Australia utilises WGS and GPS from allied States
- Constellations of satellites and the possible defences as seen above could be beneficial to Australia due to geolocation and spread of payload
- However, due to high costs involved for development, launching and maintenance of satellite constellations

- Hardening of ground stations and redundant/redeployable are not of an immediate benefit to Australia
- High cost and uncertain materials to make effective stations

Missile defence

Missile defence capabilities for Space defence would require extension and upgrades to a country's current missile defence system to intercepting DA ASAT weapons. It is currently unknown how effective missile defence would be in genuine space conflict, but countries are constantly expanding and developing capabilities, in anticipation against disaster.

Other measures

Rapid deployment and replacement

Rapid deployment of satellites would theoretically act as preventative protection, expanding abilities and launch speed to avoid adversary attention and attacks. Frequent launch system updates and limiting outside knowledge, prevents pre-emptive targeting. However, launching satellites in large clusters at high speeds is currently unfeasible, and would require training and testing before utilisation. Current launch speed is 27 hours from command to liftoff, as tested by Millenium Space Systems, Firefly Aerospace and the USSF with the Victus Nox launch from the Vandenberg Base in California in September of 2023.[240] Improving on this feat would require launch vehicle availability, launch preparation, integration, and optimal launch conditions, such as the launch window, weather and limited hazards. Launching satellites into orbit requires these factors to be as favourable as possible, and making sure everything aligns in a short space of time is difficult, and technology requires frequent updating and replacement. Air-launched deployment would allow for better launch ranges and weather standards but would still not resolve development and preparation response time

Reconstitution

Reconstitution, or the quick replacement of capabilities can be utilised to substitute damaged satellites and restore functionality. This would work for replacing satellites in orbit, with copies of the original built concurrently, or providing an updated version, as well as ground stations, where data can be transferred online, and damaged sites replaced. However, it requires the abilities of rapid deployment, to allow the replacement to occur smoothly. Speed is less of a concern than safety, as immediate replacement may still entice threats. Keeping the technology up to date and safe to use is also a concern, as even without use, damage may occur in storage.

Manoeuvre

- Fitted with chemical thrusters to avoid kinetic and DEW ASAT weapons

[240] Eric Berger, "The US Military Just Proved It Can Get Satellites Into Space Super Fast," Ars Technica, September 15, 2023, https://arstechnica.com/space/2023/09/firefly-and-space-force-demonstrate-ability-to-rapidly-launch-a-satellite/.

- Near real time continuous tracking data for incoming warheads required
- Best employed when utilised with other methods

Stealth

Satellites can be made more difficult to detect, either through manufacturing smaller satellites with radar-absorbing coats, through software that can scramble radar signals and spoofing, or through movements that are unexpected and difficult to track. These movements, aided with chemical thrusters and thus avoiding kinetic and directed energy ASAT capabilities, allow the avoidance of projected threats, simply by changing position. However, tracking and orbital weapons have wider detection sensors, and require up-to-date tracking data to avoid. Attempting software-disrupting designs carry the risk of minimising power and increasing weight and size of satellites, and is never foolproof.

Deception and Decoys

False satellites and stations, swappable payloads, and deceptive public statements would allow actors to conceal true intentions and capabilities. Decoy satellites can confuse ASAT weapons sensors and mimic electronic and radar signatures to appear as true. These decoys can be deployed when necessary, but are effective in combination with other strategies. On-orbit servicing vehicles allow satellite payloads to be swapped while in orbit. When not publicly announced, this obstructs the capability of the satellite and if switching payloads between satellites, disorient potential threats about current position. By not publicly stating true intentions or abilities of missions, actors can limit information that may contribute to threats against satellite missions. While deceptive, it is legal, as long as the satellite itself is catalogued by the UN. None of these measures have been tested publicly so far, however, they draw from established Cold War and World War II tactics.

Most operational measures covered are theoretical. Building preventative measures into satellites to ensure it cannot be targeted by counterspace threats poses a concern that the satellite becomes weighty and difficult to manoeuvre. Given Australia has proficiency for creating CubeSats which are inherently stealthy due to size, the country may find it unnecessary to implement further operational measures. Australia does not currently possess ballistic missile abilities, and therefore could not utilise this against ASAT weapons.

How could Australia utilise operational measures to protect its space assets?

- Due to the specifications of CubeSats, they are the easiest to replace due to size and cost effectiveness for rapid deployment and replacement. However, that would require permanent operational launch bases that undertake sovereign operations
- Building satellites to be easily fixed requires technical knowledge and testing prior to operation
- Australia would benefit from operational defences because it would have more satellites watching natural disasters, military operations, emergency satellites – if they were damaged, could be easily replaced
- Australia does not have ABM abilities and could therefore not use missile defences against ASATs

- Stealth is beneficial for spying or in active conflict – would be beneficial to have satellites that are moveable to avoid primarily debris in orbit
- In the event of satellites not being used/not necessary for replacement or redeployment, they still require replacement due to technology degradation. This is wasteful if development is for the sole purpose of replacement, undercuts longevity, expensive overall, time consuming, unsure of effectiveness due to no publicly made sovereign tests

3.2.3 Policy, Legal and Diplomatic Measures

Policy, legal and diplomatic tools create a vital framework and context for the management of space activities and diplomatic relations between states. The primary international space law treaty, the Outer Space Treaty 1967, has been fundamental in keeping peace in space for over fifty years.[241] That Treaty establishes core space law principles such as:

Space as the "province of all mankind": Article I of the Outer Space Treaty provides that:

> *The exploration and use of outer space, including the Moon and other celestial bodies, shall be carried out for the benefit and in the interests of all countries, irrespective of their degree of economic or scientific development, and shall be the province of all mankind.*

Clearly, the concept of space as the province of all humanity raises questions regarding the nature of access and use, as well as matters of benefit sharing which may lead to disagreement amongst states.

Freedom of exploration and use: Article I also makes it clear that outer space, including the Moon "shall be free for exploration and use by all States" meaning that no space actor may claim a monopoly of use or exclude other users.

Non-Appropriation: Article II of the Outer Space Treaty provides that:

> *Outer space, including the moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means.*

This important concept means no State (or commercial operator) may claim exclusive ownership of space, including a specific point or orbit, or a celestial body.

Application of International Law: Article III of the Outer Space Treaty confirms that activities in the exploration and use of space must be carried out "in accordance with international law, including the Charter of the United Nations, in the interest of maintaining international peace

[241] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, January 27 1967, 610 U.N.T.S. 205, 18 U.S.T 2410 (entered into force 10 October 1967).

and security and promoting international cooperation and understanding." This provision ensures that international law (including International Humanitarian Law) applies in outer space.[242]

Peaceful purposes: this term appears in both the Preamble and Article IV of the Outer Space Treaty. The Preamble articulates the desire 'to contribute to broad international cooperation in the scientific as well as the legal aspects of the exploration and use of outer space for peaceful purposes'. Article IV contains the prohibition on the placement of nuclear weapons and other weapons of mass destruction in orbit around the Earth, on celestial bodies and in outer space.

Further, it states:

> *The Moon and other celestial bodies shall be used by all States Parties to the Treaty exclusively for peaceful purposes. The establishment of military bases, installations and fortifications, the testing of any type of weapons and the conduct of military manoeuvres on celestial bodies shall be forbidden.*

However, Article IV confirms that:

> *The use of military personnel for scientific research or for any other peaceful purposes shall not be prohibited. The use of any equipment of facility necessary for peaceful exploration of the Moon and other celestial bodies shall also not be prohibited.*

The content, intent and scope of the concept of 'peaceful purposes' in the Outer Space Treaty remains unclear, although space has been used by militaries since the beginning of the space age. Military uses have included nuclear warning systems, communication, position, navigation and timing, reconnaissance and observation, weather monitoring and even the transit of weapons through (although not to or from) space.[243]

International Responsibility: Article VI of the Outer Space Treaty provides that States must 'bear international responsibility for national activities in outer space…whether such activities are carried on by governmental agencies or by non-governmental entities, and for assuring that national activities are carried out' in accordance with the provisions of the Outer Space Treaty. Space activities of non-governmental entities 'shall require authorisation and continuing supervision by the appropriate State Party to the Treaty.' This provision attributes responsibility to States for actions by their nationals and from their territory. It does not designate how States must exercise authorisation and continuing supervision. In Australia,

[242] Jack Beard and Dale Stephens "The Woomera Manual on the International Law of Military Space Operations", Oxford University Press, 2024, pp 12 -15.

[243] Taunton Paine "Bombs in orbit? Verification and violation under the Outer Space Treaty", The Space Review 19 March 2018, https://www.thespacereview.com/article/3454/1.

this is done through the licensing provisions of the Space Activities (Launches and Returns) Act 2018. Hence States are obliged to ensure that space activities of their jurisdiction comply with international space law.

Due Regard and Harmful Interference: Article IX requires States to 'conduct all their activities in outer space, including the moon and other celestial bodies, with due regard to the corresponding interests of all other States Parties to the Treaty.' States are also obliged to conduct operations in space in such a way as to avoid 'harmful contamination and also adverse changes in the environment of the Earth resulting from the introduction of extraterrestrial matter'. Arguably, these provisions may be applied to the creation of space debris and other harmful effects created by counterspace activities.

Subsequent to the Outer Space Treaty, four other UN Space Treaties have been concluded. Three of these seek to expand upon key principles articulated in the Outer Space Treaty, dealing respectively with rescue and return of astronauts and space objects (Rescue and Return Agreement),[244] liability for damage (the Liability Convention),[245] and registration of space objects (the Registration Convention).[246]

The Moon Agreement, which provides additional requirements regarding space resource activities, attracted only 18 parties, with Saudi Arabia's withdrawal from the Agreement effective 5 January 2024 leaving 17.[247] Australia is a party to the Moon Agreement and must comply with its provisions.

Whilst the UN Space Treaties are managed by the UN Committee on the Peaceful Uses of Outer Space, discussions relating to military uses of outer space are reserved for the First Committee on Disarmament, which has made it difficult to progress discussions regarding disarmament and the prevention of the placement of weapons in outer space. Progress on a Ban on Destructive ASAT Testing in the UN stalled after the UN adopted Resolution A/RES/77/41 on 7 December 2022, calling upon States 'to commit not to conduct destructive direct-ascent anti-satellite missile tests'.[248] Whilst this Resolution received overwhelming support, it is non-binding and there were some significant spacefaring states who voted against (Russia, China) and states who abstained from voting (India). Any further progress on this agenda is unlikely in the context of the Russia-Ukraine War.

Ambiguities in the legal framework create opportunities for misunderstandings and tension, further they also may involve grey zone activities, which fall below the threshold of conflict. This is particularly the case with activities such as Rendezvous and Proximity operations

[244] Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space, opened for signature 22 April 1968, 672 UNTS 119 (entered into force 3 December 1968).

[245] Convention on International Liability for Damage Caused by Space Objects, opened for signature 29 March 1972, 961 UNTS 187 (entered into force 1 September 1972).

[246] Convention on the Registration of Objects Launched into Outer Space, opened for signature 14 January 1975, 1023 UNTS 15 (entered into force 15 September 1976).

[247] Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, opened for signature 18 December 1979, 1363 UNTS 3 (entered into force 11 July 1984).

[248] Ching Wei Sooi, "Direct-Ascent Anti-Satellite Missile Tests: State Positions on the Moratorium, UNGA Resolution, and Lessons for the Future", Secure World Foundation, October 2023, https://swfound.org/media/207711/direct-ascent-antisatellite-missile-tests_state-positions-on-the-moratorium-unga-resolution-and-lessons-for-the-future.pdf

which have opaque motivations and effects. In 2021, China lodged a Note Verbale to the United Nations Committee on the Peaceful Uses of Outer Space alleging that two Starlink satellites, launched by SpaceX (a US company), had created 'dangers to the life and health of astronauts aboard the China Space Station'.[249] The Note claimed that the China Space Station had to execute two preventative collision avoidance manoeuvres on 1 July and 21 October 2021, respectively, in response to behaviours of two Starlink satellites. Detailing two 'close encounters' between the China Space Station and Starlink satellites, stating the dates of the incidents and identifiers of the Starlink spacecraft, the Note claimed that the China Space Station had to take evasive manoeuvres to avoid potential collision with Starlink satellites. The first incident occurred when a Starlink satellite moved to an orbit close to the space station, and in the second case it claimed that the satellite was 'continuously manoeuvring, the manoeuvre strategy was unknown and orbital errors were hard to be assessed' and this was deemed to be a collision risk. This Note was expressed to be provided under Article V of the Outer Space Treaty, which provides that States should inform the UN 'of any phenomena they discover in outer space (...) which could constitute a danger to the life or health of astronauts.' The Note did not make any explicit claim regarding a violation of the Outer Space Treaty, but included a reminder regarding state responsibility under Article VI. The exchange between Chinese and US diplomats continued over some months and remained unresolved. This is a clear example of the difficulties of the ambiguities of actions in space and the ongoing responsibility of States for actions by their commercial, civil and military space assets.Hence, the legal and policy framework creates both opportunities and ambiguities for space security. Space remains a domain where actions and motivations remain unclear. Discussion in international and regional forums and participation in transparency and confidence building measures, including information sharing, remain very important for the future of space security.

3.3 Matrix of Offensive and Defensive Measures

The matrix below matches offensive space control measures (physical, energy, electronic and cyber) with possible defensive measures of technical, operational, policy and diplomatic nature.

		Technical	Operational	Policy & Diplomatic
Physical (Kinetic and Non-Kinetic)	DA-ASAT	Enhanced Space Domain Awareness (SDA) Ready-to-deploy replacements Onboard defences	Enhanced architectural design Stealth Deception Decoys SDA early warning operations Rapid deployment and replacement Rapid reconstitution Manoeuvre Missile defence systems	Participation within International fora Deterrence through effective national policy and strategy International SDA coalitions Access agreements with international partners

[249] United Nations Committee on the Peaceful Uses of Outer Space, Note Verbale dated 3 December 2021 from the Permanent Mission of China to the United Nations (Vienna) addressed to the Secretary-General, UN Doc A/AC.105/1262 (6 December 2021).

		Technical	Operational	Policy & Diplomatic
	Co-Orbital ASAT	Enhanced Space Domain Awareness (SDA) Ready-to-deploy replacements Onboard defences	Enhanced architectural design Stealth Deception Decoys SDA early warning operations Rapid deployment and replacement Rapid reconstitution Manoeuvre Missile defence systems	Participation within International fora Deterrence through effective national policy and strategy Dialogue and transparency International SDA coalitions Access agreements with international partners
	Ground Station Attacks	Redundant, Mobile, or Hardened Ground Stations Redundant Control Centres		
	Nuclear Detonation	Radiation-hard satellite materials and components Electromagnetic Shielding Enhanced Space Domain Awareness (SDA)	Enhanced Architectural Design Rapid deployment and replacement Rapid Reconstitution Manoeuvre (avoiding high radiation zone)	Defensive Alliances Access to replacement services through Partnership
Directed Energy	Co-Orbital Chemical Attacks	Resistant materials and components SDA infrastructure Ready-to-deploy replacements. Enhanced Space Domain Awareness (SDA) Servicing and repair capabilities Onboard defences	Stealth Deception Decoys Rapid deployment and replacement Rapid reconstitution	Participation within International Fora Access to replacement services through Partnership
	Dazzling & Blinding	Filtering Electromagnetic shielding Shuttering	Stealth Deception Decoys Enhanced Architectural Design	Rapid Reconstitution Access to replacement services through Partnership
	High-Powered Laser	Electromagnetic shielding	Stealth Deception Decoys Enhanced Architectural Design	

		Technical	Operational	Policy & Diplomatic
Electronic	High-Powered Microwave	Electromagnetic shielding Shuttering Filtering	Stealth Deception Decoys Rapid Deployment and Replacement Rapid Reconstitution	Access to replacement services through Partnership
	Jamming	Jam-resistant waveforms Electromagnetic shielding Enhanced Space Domain Awareness (SDA)	Stealth Deception Decoys Enhanced Architectural Design Antenna nulling and adaptive filtering	
	Spoofing	Jam-resistant waveforms Enhanced Space Domain Awareness (SDA),	Stealth Deception Decoys Enhanced Architectural Design	
Cyber	Ground-Satellite Link Attacks			
	Hardware Backdoors			Regulation of public procurement processes to avoid unknown components. High security vetting for public-private procurement

4 SCENARIOS FOR AUSTRALIAN DEFENCE

In order to evaluate the options available to space stakeholders and gain deeper insight into the application of existing security mechanisms across various scenarios, the study team developed four hypothetical use cases. These use cases are intentionally designed to be open-ended, aiming to stimulate discussion regarding the most effective responses and the potential utility of current security mechanisms in addressing these challenges.

Each of the use cases presented below was crafted to identify potential gaps in policy, legal frameworks, technical solutions, governance structures, and behavioural practices within the Australian space ecosystem. Although some of the use cases are inspired by real-world events and reflect vulnerabilities within space systems for the purpose of a realistic and comparative analysis, it is important to note that none are intended to target or implicate any specific company or country. While the scenarios are designed to be realistic, the specific events, locations, capabilities, and nations involved are largely fictional and only intended to represent plausible scenarios in which conflict could begin or extend to space.

4.1 SCENARIO 1 – Cyber Attack on Ground Infrastructure

4.1.1 Context

As part of its national space strategy, Kangaroo nation in 2023 decided to sign a Technology Safeguards Agreement (TSA) with Eagle nation, its main strategic partner in the region. The Agreement would enable space launches from Kangaroo while safeguarding sensitive Eagle technology and sets standards for its use in satellite and rocket launches conducted from Kangaroo.

Recognising the growing strategic need and aiming to capture increasing commercial demand for launch capacity in the region, Southern Aerospace, a private company, opened a new launch facility in an ideal launch location within Kangaroo nation. This facility is part of a broader strategy to enhance Kangaroo's space capabilities and support allied operations.

Enabled by the new TSA, and with this launch facility now operational, Kangaroo and Eagle have formalised arrangements to launch an Eagle military satellite from Kangaroo. Eagle plans to strategically place this satellite in polar orbit, leveraging the geographical location of Kangaroo's new launch facility, which is ideal for such launches. The satellite will be launched on a SpaceY Hawk Heavy rocket. SpaceY has significantly invested in the new launch site, additionally building its own launchpad infrastructure to facilitate its operations. After the launch, this infrastructure is expected to be transferred to Kangaroo and become the initial point of joint space facilities, involving private-academic and governmental entities from both states. Likewise, it has emerged in the international press that this infrastructure is a key element of Eagle's space defence system for projecting its force in the South Pacific.

Kangaroo, however, has full responsibility for the construction and operation of all other infrastructure at the site, including the hardware and software used for centralised control. With limited experience in such activities and inadequate in-house production of all necessary components and software, commercial off-the-shelf (COTS) products were procured from Australian companies. Despite strict procurement rules and vetting, particularly under the TSA, it appears that some elements of these COTS products did not originate entirely from

Kangaroo. The TSA rules prohibited the use of COTS originated from the Dragon nation, however, a small fraction originated from Lizard, a neighbour country of Dragon, and it is highly likely that the supply chain for these specific components was actually initially developed in Dragon. Manufacturing, however, was entirely carried out in the friendly nation of Lizard.

4.1.2 Nature of the attack

On 26 May 2026, one week before the first launch from the new Kangaroo-Eagle facility, an anonymous account on social media 'X' revealed that the launch facility had been compromised in a cyber-attack. The account is recent and has claimed responsibility for the attack, but without indicating its affiliation with any specific institution or government. The Kangaroo Secret Intelligence Service has clear suspects about the origin of the attack and recommended elevating the national alarm due to the unknown consequences of the attack.

The compromised hardware allowed a disgruntled Kangaroo employee of Southern Aerospace with security clearance to exploit a backdoor. The employee was bribed and coerced by a rogue hacker group believed to be affiliated with and sponsored by North Duck nation, a non-democratic country led by an autocratic leader and allied with the Dragon nation. A sophisticated cyber infiltration attack was successfully carried out. The extent of the attack is not fully known, but sensitive data was relayed to IP addresses in both Dragon and North Duck nations. Kangaroo officials publicly acknowledged the attack but did not disclose details on the type of data stolen. At this time, it is not yet known how long the individual and hacker group had access to the launch facility networks, how many subnetworks were exposed, or what other sensitive information might have been stolen.

The duration of the hacker group's access to the launch facility networks, the number of subnetworks exposed, and the additional sensitive information that may have been stolen remain unknown. The facility has been completely shut down while investigations are underway. The Eagle's Department of Defence expressed its anger publicly and recalled its satellite and all other Eagle technology on site.

Attacker	North Duck state-sponsored hacker group (not verified)
Attack purpose	Reconnaissance and data exfiltration
Type of attack	Cyberattack through compromised technologies and insider threat
Attack surface	Launch facility hardware, leading to software backdoor
Infrastructure involved	Launch Infrastructure present at Kangaroo
Attack effect	Exposed sensitive information on Kangaroo launch infrastructure and Eagle launch vehicles

4.1.3 Implications

Ceased Launch Operations: Upon discovery of the attack, all operations from the launch site have been halted indefinitely, impacting planned launches over the next year.

Damaged Relations with Launch Partners: Ceased launch operations have affected bilateral relations with international launch partners. Other International and commercial partners are concerned about the compromise of sensitive data, with some retrieving their own launch vehicles and satellites, and others terminating existing contracts.

Economic Repercussions for the Australian Space Sector: Future contracts for the launch facility appear unlikely, resulting in a reduction of investment in Kangaroo's space sector and wider economic repercussions. Kangaroo is now missing out on opportunities to explore new space capabilities in the short-term. Damaged relationship with Eagle.

Implications for International Technology Procurement: Western nations are approaching COTS hardware and software cautiously, auditing their supply chains and strengthening policies to protect national security interests.

4.1.4 Questions for Participants

Scenario Specific Questions:

1. How could enhanced polices for vetting and verification processes for COTS products have prevented the compromise of launch facility hardware and software?
    a. Policy: Implementing rigorous supply chain audits to trace the origin of all components.
    b. Policy: Establishing stricter cybersecurity standards for all suppliers and conducting compliance checks.
    c. Policy and Operational: Conducting vulnerability assessments on all COTS products before deployment.
2. What immediate response measures should be taken to mitigate the effects of the data breach?
    a. Operational: Isolating compromised networks and systems to prevent further data exfiltration.
    b. Operational: Conducting a comprehensive forensic investigation to identify the extent of the breach.
    c. Policy & Diplomatic: Coordinating with Eagle's partners to implement joint containment and remediation strategies.
3. What immediate response measures should be taken from the diplomatic and political sides to mitigate the effects of the attack on the space infrastructure?
    a. Operational: To deliver accurate information from official governmental accounts to manage the rising crisis and bring serenity to the civilian population (preventing the spread of fake news).
    b. Policy & Diplomatic: To initiate consultation processes through the assistance of Eagle's ambassador.
    c. Policy and Diplomatic: Notifying UNOOSA about the nature of the attack and its implications for the 1967 Outer Space Treaty.

4. How can future satellite launch facilities be designed to better detect and prevent insider threats and cyber infiltration?
    a. Technical and Operational: Integrating advanced user behaviour analytics to detect anomalies indicative of insider threats.
    b. Technical and Operational: Enhancing access controls with e.g. multi-factor authentication and biometric verification.
    c. Technical and Policy: Regularly updating and patching all systems to mitigate known vulnerabilities and threats.

General Questions:

1. What actions could have been taken to prepare for and prevent this situation?
    a. Operational: Conducting regular cybersecurity risk assessments and updating security protocols.
    b. Operational: Implementing a comprehensive insider threat detection programme.
    c. Policy: Establishing robust supply chain security measures to prevent the introduction of compromised components.
2. What counter measures are already at your disposal?
    a. Operational: Immediate mission shutdown to evaluate the extent of exfiltrated data.
    b. Operational: Update of internal cybersecurity protocols and endurance of the vetting system for professionals involved in key missions.
    c. Policy and Diplomatic: Initiate negotiations with Eagle's partners to secure the maintenance of the relationship.
3. What capabilities or measures are currently lacking that would enhance your response to this situation?
    a. Advanced threat detection and response systems.
    b. Secure communication channels and encrypted data transmission.
    c. Enhanced cyber incident response teams with specialised training.
    d. Network segmentation and isolation protocols.
    e. Real-time monitoring and intrusion detection systems.
    f. Established incident response procedures and recovery plans.
4. What are the pros and cons of different responses?
    a. Immediate shutdown of compromised systems:
        i. Pros – Prevents further data exfiltration.
        ii. Cons – Disrupts ongoing operations.
    b. Deployment of cyber counter-offensive measures:
        i. Pros – Deters further attacks.
        ii. Cons – Risk of escalation.
    c. Public disclosure of the attack:
        i. Pros – Increases transparency and stakeholder trust.
        ii. Cons – May cause panic and reputational damage.

4.2 SCENARIO 2 – Bear Co-orbital RPO Activity

4.2.1 Context

It is now over three years since Bear nation, the largest country in the Ganymede continent, initially invaded Deer nation, the second largest country on the continent, through their shared border. Although there was a period when the allies of Ganymede's main military alliance, particularly the Eagle nation, seemed to waver in their indirect support for Deer, a series of events and increased Bear aggression led to a significant pivot in allied support.

Kangaroo nation has promised Deer several of its newly produced AS9 Redback self-propelled howitzers. Although it was formally agreed with Deer that these weapons were for defensive purposes – to be used only to prevent Bear advances in Deer territory – Bear now publicly claims Kangaroo weapons are being used to attack targets within Bear's territory.

Deer denies these allegations, and there is no hard evidence to support Bear's claims. Nevertheless, Bear uses this situation to incentivise retaliation on Kangaroo's hybrid commercial and military satellite, Optical D1. This satellite is a component of Kangaroo's Defence Satellite Communication System (KDSS) and serves both defence and civilian purposes in areas such as SAR operations, which are believed to have been used to support Deer military operations.

4.2.2 Nature of the attack

Two weeks after Bear's public claim that Kangaroo weapons have been used to attack Bear's territory, the KDDS was supporting a SAR operation over Antarctic continent, where a vessel with 12 tourists wrecked. The accident caused a fuel spill in the ocean and resulted in the deaths of all those aboard. The KDDS is providing strategic communication for rescue and emergency response efforts to both military and civilian organisations involved. The SAR tasks are estimated to last for two weeks. During the development of the SAR tasks, a Kangaroo's military satellite ground control operator informs senior officials of Kangaroo's Department of Defence that the satellite is off course and unresponsive.

Unknown to Kangaroo at the time, Bear had successfully completed a rendezvous and Proximity Operation (RPO) on Kangaroo's satellite through a non-registered technology demonstrator satellite. Specifically, the activity was carried out by a co-orbital Bear satellite designed specifically for a variety of purposes. This satellite was deployed in orbit by Bear several months prior, launched together with a separate but much larger military satellite as a ruse. The larger satellite's launch was made public and officially registered through the UN registry, while the smaller satellite, with unknown capabilities, was deployed in secrecy.

When Bear decided to initiate its RPO, its military satellite operators used on-board propulsion to alter its trajectory. Over several weeks, the trajectory was aligned with Kangaroo's satellite. Once in position, Bear's operators initiated a secretive attack from a close distance, causing physical damage to the targeted satellite, without any physical contact. The impact altered the target's trajectory, making initial tracking efforts difficult.

Kangaroo's Department of Defence, suspecting Bear's involvement, relayed the incident to Eagle's defence officials, its main strategic partner in the region. Within two days, Eagle's officials tracked down the astray satellite and informed Kangaroo's Department of Defence

that physical damage had been caused to its satellite. Given the satellite's role in supporting Deer and recent Bear claims, it was relatively clear this was an attack from Bear. However, without solid evidence, Bear continued to deny the accusations. Instead Bear invited Kangaroo to join efforts for the signature of a treaty restricting the placement of weapons and use of force in space, a long-standing initiative sponsored by the Bear and Dragon nations at the United Nations.

Attacker	Bear (neither claimed nor verified)
Attack purpose	Denial of service
Type of attack	Unknown, physical (possibly chemical)
Attack surface	Kangaroo military satellite in orbit
Infrastructure involved	Optical D1 Commercial and Military satellite
Attack effect	Permanent destruction of satellite functionality

4.2.3 Implications

Denial of Military Satellite Service: The damage to the satellite results in a loss of critical SATCOM capabilities for Kangaroo's Defence Force.

Increased Vulnerability of Military Satellites to Physical Attacks: The attack reveals the vulnerability of military satellites to unconventional methods, necessitating a review of protective measures. It also highlights the need for continual review of technical specifications when Kangaroo's government is contracting private companies to construct military infrastructure.

Heightened Surveillance of Bear's Satellite Launches: Future Bear satellite launches are subjected to increased scrutiny and surveillance by international monitoring agencies.

4.2.4 Questions for Participants

Scenario Specific Questions:

1. What pre-emptive measures could have identified the threat posed by the co-orbital satellite before it conducted the physical unknown attack?
    a. Operational: Conducting permanent counterspace intelligence analysis over potential hazards to national space systems.
    b. Technical and Operational: Enhanced Space Domain Awareness (SDA) to detect unusual satellite manoeuvres.

   c. Technical and Operational: Developing and deploying on-orbit inspection satellites to monitor suspicious objects.
   d. Policy & Diplomatic: Collaborating with international partners to share real-time space situational data.
2. How should Kangaroo and its allies respond to the loss of SATCOM capabilities due to this physical attack to maintain operational readiness?
   a. Operational: Deploying backup satellites or utilising allied satellite services to fill the communication gap.
   b. Policy and Operational: Diversifying SATCOM capabilities from thirds platforms serving in LEO and GEO. Initiating a consultation process within the OST and ATS regarding the nature of operations affected by the lack of SATCOM capabilities due to a hostile act in outer space, and the environmental and humanitarian impact on territories considered under the ATS.
   c. Technical and Operational: Enhancing cyber defences to protect remaining space assets from further attacks. Activating international alarm considered under UN General Assembly resolution 58/199 on the Creation of a global culture of cybersecurity and the protection of critical information infrastructures (30 Jan. 2004).
3. What long-term strategies should be implemented to protect Kangaroo's military satellites from unconventional threats enabled by RPO?
   a. Developing satellite hardening techniques.
   b. Implementing redundant systems and rapid satellite deployment capabilities.
   c. Establishing international norms and agreements to deter the use of unconventional attacks in space.
   d. Establishing international norms under the ATS to deter the use of counterspace capabilities over task being conducted at Antarctic territory.

General Questions:

1. What actions could have been taken to prepare for and prevent this situation?
   a. Policy & Diplomatic and Operational: Conducting joint military exercises to simulate and prepare for such attacks.
   b. Operational: Enhancing intelligence gathering and analysis on potential threats.
   c. Technical and Operational: Implementing advanced early warning systems for satellite anomalies.
   d. Operational: Implementing a redundant system with third platforms serving in LEO and GEO, avoiding the lack of communications.
2. What actions must be followed at multilateral level?
   a. Sending a diplomatic note to UNOOSA alerting to the loss of operability of the SATCOM system and noting that the system was being used during SAR tasks, with considerations for human security and environmental protection.
   b. Sending a diplomatic note to the Secretariat of the Antarctic Treaty, alerting to the lack of capabilities to continue with tasks according to the environmental protocol.

   c. Activating a consulate alarm, requesting SATCOM services support due to the conduct of SAR operations.
   d. Activating the International Charter for Major Disasters to continue tasks related to SAR and environmental protection, as well as to enhance the acquisition of ISR data.
3. What counter measures are already at your disposal?
   a. Policy and Diplomatic: Improve international collaboration amongst state partners to improve SSA and SDA capabilities.
   b. Policy and Diplomatic: Improve collaboration with international partners to provide continuous support to the Antarctic mission.
   c. Diplomatic: Notify UNOOSA about a possible breach of the Liability Convention.
4. What capabilities or measures are currently lacking that would enhance your response to this situation?
   a. On-orbit servicing and repair capabilities for damaged satellites.
   b. Rapid deployment mechanisms for replacement satellites.
   c. Advanced chemical detection and neutralisation technologies.
   d. Backup SATCOM satellites and allied satellite service sharing agreements.
5. What are the pros and cons of different responses?
   a. Diplomatic efforts and appeals to international governance bodies:
      i. Pros – Raises awareness and international condemnation.
      ii. Cons – Limited immediate effect.
   b. Accelerated deployment of replacement satellites:
      i. Pros – Restores capabilities quickly.
      ii. Cons – High cost and resource-intensive.
   c. Development of anti-satellite defence systems:
      i. Pros – Deterrence against future attacks.
      ii. Cons – Potential arms race and escalation.

4.3 Scenario 3 – Dragon's Direct Energy Weapon Test

4.3.1 Context

Dragon nation's ambitions to assert control over Snake Island, a small country south of Dragon, are becoming increasingly clear. Its aggressive rhetoric and direct statements of intent, paired with visible military preparations, spread out by official media press, have raised significant concerns among Western allies. Eagle nation has abandoned its strategic ambiguity on the issue as an attempt to openly confront Dragon's interest, and a growing number of Eagle's allies, including Kangaroo, have pledged support for Snake Island should Dragon's threats materialise into an invasion.

Despite significant economic ties with Dragon, Kangaroo is increasingly concerned that an invasion of Snake Island is imminent, fearing both the regional repercussions of Dragon's dominance and its global implications. With rising tensions, public support for intervention becomes almost universal among Kangaroo citizens. Under pressure from military strategists and public sentiment, Kangaroo quietly sends arms to Snake Island, including advanced anti-aircraft systems and naval support equipment, it would also be supportive to Snake Island by providing communication technologies, ISR capabilities, and information field technologies, in accordance with a Science and Technology Pact signed between both nations.

Dragon perceives this as an act of aggression and decides to send a clear warning, but without escalating to direct conflict. Dragon tests an experimental directed energy weapon (DEW) prototype on an Earth observation satellite serving to Kangaroo entities (private and governmental), suspected of dual-use military functionality. The targeted platform has been the DeltaSAR-1 satellite. It is operated by Kangaroo's Government agency responsible for scientific research, The Scientific and Industrial Research Administration (SIRA), from Kangaroo's Centre for Appropriate Technology (CfAT) ground station, Kangaroo's first and only First nations-owned and operated ground segment service provider[250]. Due to its Synthetic Aperture Radar (SAR) capabilities, Dragon suspects that the platform is being used for military intelligence support over the Strait between Dragon and Snake Island.

4.3.2 Nature of the attack

The DEW attack involves a high-powered laser. Two initial low-powered tests dazzle the satellite for a few seconds, noticed by the operator but dismissed as anomalies. The third test involves a more powerful and continuous laser directed at the satellite's optical sensors, permanently damaging them. The satellite remains operational but loses partial functionality.

The attackers use advanced targeting algorithms and precision control mechanisms to ensure the laser impacts the satellite's most vulnerable components. The laser's intensity and duration are carefully calibrated to cause maximum damage without immediate detection. The satellite's compromised functionality includes reduced imaging capability and intermittent communication issues.

To maintain plausible deniability, Dragon conducted the test, not from its national territory, but from one of its scientific research bases located in the Antarctic South Pole Circle.

[250] Commonwealth Scientific and Industrial Research Organisation (CSIRO), "NovaSAR-1", n.d., https://research.csiro.au/cceo/novasar/

Although Dragon officially adheres to the 1959 Antarctic Treaty and is a member of the Antarctic Treaty System (ATS), which prohibits any military use and emplacement of weapons in Antarctica, it has long been suspected that some activities have dual purposes, exploiting the fact that the base never had been inspected by third member states of the treaty according to normal procedures. The geographical location of this base is ideal for targeting satellites serving Kangaroo, given the range and accuracy of the experimental weapon. Dragon, however, denies all allegations related to its test, and Kangaroo finds difficulty in officially tying Dragon to this activity.

Attacker	Dragon (neither claimed nor verified)
Attack purpose	Strategic warning, experimental weapon test, disruption of commercial/dual-use satellite service
Type of attack	Directed Energy Weapon
Attack surface	Optical sensors of the satellite
Infrastructure involved	Commercial earth observation satellite suspected of dual-use
Attack effect	Permanent damage to functionality, non-destructive

4.3.3 Implications

Partial Loss of Satellite Functionality: The satellite's diminished capabilities affect both commercial and potential military operations.

Escalation of Hostilities: The attack is a clear message from Dragon and increases regional tensions in the region. It necessitates strategic responses from Kangaroo and its allies, including ATS members who are growing concerned that the principle of peaceful uses of the Antarctic has been violated and could be jeopardised even further.

Exposure of Directed Energy Weapon Capabilities: The incident highlights Dragon's advancement in DEW technology, prompting other nations to reassess their own satellite defence measures.

Humanitarian and First Nations Considerations: The attack involved actively the capabilities of the CfAT and their First Nations community, promoting the arise of tension surrounding the need to protect the safety and equal access to space benefits from First Nation´s people.

Impacts on Critical Research: Access to DeltaSAR-1 data is free to researchers from institutions across the globe. Following the attack, hundreds of scientific research projects conducted by the SIRA that were reliant on DeltaSAR-1 data are interrupted or devastated.

The impacts on domestic and international partnerships are difficult to quantify and, in some cases, irreversible.

4.3.4 Questions for Participants

Scenario Specific Questions:

1. What specific technological upgrades could enhance the resilience of satellites against directed energy weapon (DEW) attacks?
    a. Technical: Incorporating advanced shielding and reflective materials on satellites.
    b. Technical: Developing adaptive optics to mitigate the effects of laser attacks.
    c. Technical and Operational: Enhancing onboard satellite AI capabilities to detect and respond to DEW attacks in real-time.
2. How should Kangaroo coordinate with its allies to develop a unified response to Dragon's use of DEWs in space?
    a. Establishing joint task forces to monitor and respond to DEW threats.
    b. Sharing intelligence and technology related to DEW defence measures.
    c. Conducting joint exercises to improve coordination and readiness against DEW attacks.
    d. Promoting awareness on counterspace capabilities and its potential impacts, on the consultive meetings at the ATS.
3. What measures can be taken to improve the detection and attribution of DEW attacks on satellites?
    a. Deploying space-based sensors to detect high-energy laser emissions.
    b. Utilising ground-based observatories to monitor and track DEW activities.
    c. Enhancing methods to better identify and attribute DEW sources.

General Questions:

1. What actions could have been taken to prepare for and prevent this situation?
    a. Policy and Technical: Increasing investment in DEW detection and mitigation technologies.
    b. Operational: Conducting threat assessments and scenario planning for DEW attacks.
    c. Policy & Diplomatic: Enhancing international collaboration on space security initiatives.
2. What counter measures are already at your disposal?
    a. Policy and Diplomatic: Develop a new satellite defence paradigm with a focus on hardening to improve space assets' resilience to DEW
    b. Diplomatic: Request the inspection of Dragon's base in Antarctica by third member states in accordance with the 1959 Antarctic Treaty
    c. Diplomatic: Establish, along with allies in the region, a combined response to the use of DEW
3. What capabilities or measures are currently lacking that would enhance your response to this situation?

   a. Advanced DEW detection systems.
   b. Satellite hardening and shielding technologies.
   c. Real-time monitoring and response capabilities.
   d. Ground-based DEW detection and monitoring systems.
4. What are the pros and cons of different responses?
   a. Diplomatic engagement efforts:
      i. Pros – Builds international consensus.
      ii. Cons – Slow and potentially ineffective.
   b. Development and deployment of DEW countermeasures:
      i. Pros – Enhances deterrence.
      ii. Cons – High cost and technical challenges.
   c. Retaliatory DEW testing:
      i. Pros – Demonstrates capability and resolve.
      ii. Cons – Risks escalation and potential conflict.

4.4 Scenario 4 – Downlink Jamming of Warship in Purple Sea

4.4.1 Context

In response to recent rebel attacks on shipping freights in the Purple Sea supported by the Ibex nation, Kangaroo nation has deployed a warship to the region to support its allies, including the Eagle nation. Kangaroo's warship, equipped with advanced military satellite communications systems, plays a critical role in ensuring the safety and security of commercial and military vessels navigating these strategic waters.

With escalating tensions in the region, the Kangaroo warship is deployed to the Purple Sea as part of a multinational task force. This task force is charged with protecting shipping lanes and deterring further attacks. The attacks are being conducted by the political, religious, and military organisation named the Stone Rebels. The warship relies heavily on satellite communications for real-time intelligence sharing, command and control operations, and coordination with allied forces.

Intelligence reports indicate that Ibex-backed stone rebels are planning more aggressive actions against international shipping. In a calculated move to disrupt the operations of the multinational task force, Ibex leverages its cyber capabilities to compromise the satellite communications of Kangaroo's warship. The objective is to impair the warship's operational effectiveness and create confusion among its allied forces.

4.4.2 Nature of the attack

Ibex state-sponsored hacking groups target the satellite communication systems of the warship, aiming to disrupt the communication links between the warship and its command structure. This sophisticated attack involves downlink jamming and spoofing, exploiting known vulnerabilities in encryption and signal integrity protocols.

The attackers utilise commercially available technology, provided by Ibex, to intercept and disrupt communications. Using a commercial satellite dish, a DVB board, and COTS software, the attackers intercept signals from the warship's Very Small Aperture Terminals (VSAT). These components, costing merely a few hundred dollars, allow the hackers to search for satellite signals and capture critical data packets. The adversaries exploit open-source intelligence (OSINT) to gather information on the spectrum and radiofrequency bands used by Kangaroo's communication satellites, their payloads, and precise orbital positions.

By understanding the standardised protocols used for VSAT, such as DVB-S and GSE, the hackers write algorithms to locate and intercept IP data packets. Due to insufficient encryption on the communication satellites, the intercepted data includes unencrypted critical information, which can then be used to disrupt operations and gather intelligence.

The impact of the jamming and spoofing is immediate and severe. The warship experiences significant delays in receiving critical intelligence and commands, which affects its ability to coordinate effectively with allied forces and respond promptly to threats. The spoofed positioning data results in navigational errors, increasing the risk of the warship straying into hostile waters or areas with known rebel activity. Furthermore, the interception and potential decryption of secure communications could expose sensitive operational details to the adversary, jeopardising the mission.

Attacker	Ibex (not verified)
Attack purpose	Disruption of communication to hinder military operations
Type of attack	Downlink jamming and spoofing of satellite signals
Attack surface	Satellite communication downlinks, exploiting vulnerabilities in the encryption and signal integrity protocols.
Infrastructure involved	Warship satellite communication systems
Attack effect	Intermittent loss of communication, incorrect positioning data, and compromised transmission of commands and intelligence.

4.4.3 Implications

Operational Disruption: The disruption of satellite communications leads to delays in receiving critical intelligence and commands, affecting the warship's ability to coordinate with allied forces and respond to threats in a timely manner and diminishing the safety of the operation.

Navigation Issues: Spoofed positioning data causes navigational errors, increasing the risk of the warship straying into hostile waters. This could be exploited as a violation of the territorial waters of Ibex or involve other areas with known rebel activity.

Security Breach: The interception and potential decryption of secure communications could expose sensitive operational details to the adversary, compromising the overall mission.

Escalation of Tensions: The attack signifies a direct escalation in hostilities by Ibex, necessitating a strategic response from Kangaroo and its allies to safeguard their assets and assert control over the region and avoiding the exploitation of the conflict under an asymmetrical perspective.

4.4.4 Questions for Participants

Scenario Specific Questions:

1. What pre-emptive measures could have improved the overall resilience of the warship systems?
    a. Improving the robustness of encryption protocols to protect the confidentiality of information.
    b. Enhancing signal integrity protocols for ensuring reliable data transmission and minimising errors in communication systems across increasingly complex electronic environments.

   c. Strengthening cybersecurity to protect systems and data from malicious attacks and ensure digital resilience.
2. How should Kangaroo coordinate with its allies to respond to Ibex's attacks in the Purple Sea region?
   a. Establishing a nexus between the hacker group and the Ibex nation.
   b. Conducting joint exercises to improve coordination and readiness against electronic and cyber attacks.
   c. Sharing intelligence and technology related to electronic and cyber defence measures.
3. What measures can be taken to improve the detection and attribution of electronic and cyber attacks?
   a. Technical: Implementing electromagnetic shielding to protect critical components.
   b. Operational: Conducting regular system audits and vulnerability assessments.
   c. Technical and Operational: Integrating redundant systems to maintain functionality under attack.

General Questions:

1. What actions could have been taken to prepare for and prevent this situation?
   a. Policy and Technical: Increasing investment in cybersecurity and electronic defences.
   b. Policy and Operational: Conducting threat assessments and scenario planning for cyber and electronic attacks.
   c. Policy & Diplomatic: Enhancing international collaboration on GNSS for accurate positioning and validation.
2. What counter measures are already at your disposal?
   a. Technical: Integrate multi-constellation and multi-frequency GNSS receivers to improve redundancy and resilience against spoofing or jamming.
   b. Operational: Implement GNSS signal authentication techniques to verify the legitimacy of received signals.
   c. Technical and Operational: Use inertial navigation systems as a backup to maintain navigation capability during GNSS disruptions.
3. What are the pros and cons of different responses?
   a. Hardening of critical infrastructure against GNSS disruption:
      iii. Pros – Improves system resilience and continuity of operations.
      iv. Cons – Requires significant investment and complex integration.
   b. Diplomatic efforts:
      v. Pros – Builds international consensus.
      vi. Cons – Difficulty in proving attribution.
   c. Retaliatory cyber and electronic testing:
      vii. Pros – Serves as a deterrent by showcasing operational capability.
      viii. Cons – Unknown results. May provoke adversaries and escalate tensions in the region.

5 Considerations for Australian Defence

As space transitions from a niche area to a pervasive asset affecting all domains of everyday life and industries, nations must urgently rethink their view of space security. In this setting, counterspace technologies, once only a concern for major powers, now pose clear threats to Australia's national interests, especially amid rising geopolitical tensions and increased militarisation and weaponisation of space.

This report highlights a significant change in the global counterspace environment. While space was once seen as a sanctuary for peaceful activities and accessible to every nation, it has now become congested, contested, and competitive. Countries like China and Russia are developing and demonstrating counterspace capabilities, including co-orbital and direct-ascent anti-satellite weapons, which could threaten Australia's access to and use of vital space-based services. Electronic warfare and cyberattacks, although less discussed in mainstream channels, pose an equal or greater threat to space assets and must also be considered and incorporated into national defence strategies.

The ADF already anticipates that future conflicts could extend into the space domain, and therefore incorporates operations in degraded, denied, or deceptive space environments into its more recent space strategies. By doing so, it seeks to ensure reliance on space-based capabilities for command, control, communications, intelligence, surveillance, and reconnaissance, which are vital to Australia's operations.

Given that Australia's space assets are mainly dual-use, supporting both civilian and military purposes, Defence must establish protocols to work with civilian and commercial partners on threat detection, response, and resilience. This includes clear attribution frameworks for when national interests are at risk in the space domain. The mixture of commercial, scientific, and defence space activities, while economical, broadens the attack surface for adversaries. The report stresses the danger of adversaries exploiting these grey zones, especially through non-kinetic or reversible attacks that fall below traditional thresholds for armed conflict.

Furthermore, while Australia chose to focus on becoming a global leader in ground-based operations and data services rather than investing in sovereign space capabilities, it now needs to assess the reliability of its main international partners amid the current highly volatile international landscape. Australia is heavily reliant on allied space services, especially those of the United States. Although these partnerships are essential, the report highlights the risks tied to this dependence, particularly in situations where geopolitical shifts or operational priorities could delay allied support. Consequently, options to increase autonomy and decrease the strategic risk linked to overreliance on external actors must be considered, especially in sovereign SSA capabilities, resilient satellite communications, and alternative PNT systems.

5.1 Findings

The following are the core findings derived from the report's analysis:

1. Counterspace threats present a global growing danger: Several nations with different strategic postures are actively developing counterspace weapons and doctrines against the peaceful uses of outer space. These pose direct risks to Australia's and its allies' national security.
2. Australia lacks a clear and robust deterrence posture in space: Currently, despite asserting the importance of the space domain in documents such as the Space Power E-manual 2022, Australia has no clear framework for how it would respond to acts of aggression in the space domain, which undermines its reaction time and overall ability to deter coercive or grey-zone activities. In this sense, all four scenarios highlight significant grey areas concerning how to prevent, endure, respond and reconstitute from potential space threats.
3. Civil-military integration creates vulnerabilities: Australia's model of dual-use infrastructure, while resource-efficient, lacks comprehensive security frameworks across the entire domain, also allowing varying acceptable security levels and creating new opportunities for hostile exploitation. This fragmented approach can lead to inconsistent threat assessments and response capabilities where private sector entities are involved. Moreover, adversaries may exploit gaps between civilian and military oversight, targeting weaker links to compromise broader national security objectives.
4. Policy and legal frameworks are insufficient: Australia's current space policy framework and national security strategies do not sufficiently address counterspace threats or contingencies related to space conflict. Moreover, its legal framework lacks mechanisms adequately applicable to space security. Instead of focusing cybersecurity responsibilities solely within the Space (Launches and Returns) Act 2018, the protection of space infrastructure from cyber threats is mainly supported indirectly through broader legislative instruments. These are primarily found within laws governing telecommunications and critical infrastructure. However, applying these frameworks to the space sector may pose challenges for space operators, as adapting such obligations can be complex and time-consuming.
5. National space resilience is underdeveloped: Despite recognising the growing danger posed by counterspace threats, redundancy, rapid reconstitution, and hardened satellite systems remain significantly underdeveloped in Australia's national space posture. This lack of resilience leaves critical space-based assets vulnerable to disruption or destruction in a contested environment. Without substantial investment in protective and responsive capabilities, Australia risks strategic paralysis in the face of even limited counterspace operations.

5.2 Key Takeaways and Recommendations

1. Space is now increasingly becoming a warfighting domain.
   Recommendation: Develop a National Counterspace Strategy

Develop a cross-agency strategy that outlines Australia's Defence position on space conflict, response thresholds, and coordination across civil, commercial, and military sectors. This should include a deterrence plan for counterspace threats, planned investments, and swift attribution procedures.

2. Resilience and redundancy are critical.
   Recommendation: Increased investments in space defensive measures

Introduce policy guidelines that require all space systems supporting Defence, including civil, to meet minimum resilience benchmarks, including electronic shielding, anti-jamming measures, and backup communications. Australia must assume contested space environments and plan and invest accordingly, including satellite hardening, proliferated LEO constellations, and responsive launch capabilities.

3. Australia must define its thresholds.
   Recommendation: Develop and publicise what it considers responsible and irresponsible space behaviour

Transparent strategic signalling is necessary to define what counts as an unacceptable attack on space infrastructure and how Australia would respond. While this position can be perceived as potentially escalatory, it can have a positive impact on the space sector by enhancing predictability, legal clarity, and international consistency, as well as reducing the risk of escalation by preventing unilateral state interpretations that could exacerbate conflicts.

4. Alliances matter, but autonomy matters more.
   Recommendation: Invest in Sovereign Space Infrastructure

While the Five Eyes and AUKUS partnerships are vital, Australia's capacity to independently understand, evaluate, and operate within the space environment is equally important. Australia needs to increase investment in sovereign SSA, resilient SATCOMs, and rapid-launch satellite capabilities. Special focus should be on developing autonomous PNT capabilities to lessen reliance on GPS.

5. International engagement for norm creation is essential
   Recommendation: Foster norm-building through cooperation in international forums

While Australia must prioritise the development of sovereign space capabilities, it should also remain actively engaged in international efforts to shape emerging norms and rules governing counterspace activities. This includes supporting multilateral transparency and confidence-building measures and working collaboratively with partners to promote frameworks for responsible space behaviour, not only among strategic allies, but also within OEWGs and broader multilateral forums such as the Conference on Disarmament. Furthermore, Australia should contribute to discussions within COPUOS on safety measures, particularly where such measures intersect with security concerns, to ensure that technical guidelines do not inadvertently introduce vulnerabilities or exacerbate strategic tensions.

ANNEXES

Annex A – List of Abbreviations

Abbreviations			
ABL	Airborne Laser	COPUOS	Committee On the Peaceful Uses of Outer Space
ADF	Australian Defence Force	CSIRO	Commonwealth Scientific and Industrial Research Organisation
ABM	Anti-Ballistic Missile	CSpO	Combined Space Operations Initiative
AEHF	Advanced Extremely High Frequency	DA-ASAT	Direct-Ascent Anti-Satellite
AI	Artificial Intelligence	DASA	Defence Aviation Safety Authority
AIS	Automatic Identification System	DEW	Directed Energy Weaponry
ASA	Australian Space Agency	DFAT	Department of Foreign Affairs and Trade
ASAT	Anti-Satellite	DIA	Defence Intelligence Agency
ASPC	Australian Public Service Commission	DISR	Department of Industry, Science and Resources
AUKUS	Australia United Kingdom United States	DoD	Department of Defence
AUSSpOC	Australian Space Operations Centre	DRDO	Defence Research Development Organisation
AWACS	Airborne Warning And Control Systems	DSpC	Defence Space Command
C2	Command-and-Control	EMP	Electromagnetic Pulse
CCS	Counter Communications Systems	EO	Earth Observation
CFSCC	Combined Force Space Component Command	EW	Electronic Warfare
CJOPS	Commander Joint Operations Command	FHSS	Frequency Hopping Spread Spectrum
GLONASS	Globalnaya Navigazionnaya Sputnikovaya	NZSA	New Zealand Space Agency
GNSS	Global Navigation Satellite Services	OEWG	Open-Ended Working Group
GPS	Global Positioning System	PGM	Precision-Guided Munitions

Abbreviations			
GWEO	Guided Weapons and Explosive Ordnance	PNT	Positioning, Navigation and Timing
HAD	High Altitude Density	QUAD	Quadrilateral Security Dialogue
HPM	High-Power Microwave	RAAF	Royal Australian Air Force
IIP	Instantaneous Impact Point	RAN	Royal Australian Navy
ISR	Intelligence, Surveillance and Reconnaissance	RF	Radio Frequency
ITU	International Telecommunications Union	SAR	Synthetic Aperture Radar
JOPS	Joint Operations Command	SATCOM	Satellite Communications
LACE	Low-power Atmospheric Compensation Experiment	SCC	Satellite Communications Capabilities
LEO	Low Earth Orbit	SDA	Space Domain Awareness
LOE	Lines of Effort	SKAO	Square Kilometre Array Observatory
MDA	Missile Defence Agency	SLR	Satellite Laser Ranging
MIRACL	Mid-Infrared Advanced Chemical Laser	SSA	Space Situational Awareness
MITM	Man-In-The-Middle	SSF	Strategic Support Force
MoU	Memorandum of Understanding	STM	Space Traffic Management
NASA	National Aeronautics and Space Administration	UAS	Unmanned Aerial Systems
NATO	North Atlantic Treaty Organisation	UAV	Unmanned Aerial Vehicle
NRO	National Reconnaissance Office	UNOOSA	United Nations Office for Outer Space Affairs
NSSIDC	National Security Space Interdepartmental Committee	WGS	Wideband Global Satellite Communications

Annex B – Tables and Figures

Part 1: Kinetic physical ASAT tests by country in chronological order.

Country	Type	Title	Status
USA	Direct Ascent	Bold Orion High Virgo	Tested in 1950s-60s, deemed feasible
		NOTSNIK	Successful tests in 1961-62
		Nike Zeus	Successful intercept in 1963, replaced by 437
		ASM135	Successful tests in 1974, cut in 1988
		Program 437	Tested multiple times, terminated in 1975
		Aegis	Tested in 2008
		Ground Based Interceptors	Potential use
	Co-orbital	SAINT	Cancelled before test in 1962
		Delta 180	Successful launch in 1986
		DART	Unplanned collision, undamaged
		X37B	Successful launch and rendezvous
		Prowler	Successful launch in 1990, decommissioned in 1998
		MsTE	Successful flybys in 2009
		Pan	Successful launch and in 2009, relocations during 2013 and reactivation in 2021
		Hornet	Launched in pairs since 2014, forced into early use
		ANGELS	Decommissioned in 2017
		Mycroft	Successful launch and inspection in 2019, no communication
Russia	Direct Ascent	78M6 Kontakt	Resurrected Soviet tech, supposed test in 90s, resumed in 2009, possibly replaced
		Nudol	Resurrected Soviet tech, tested in 2013, successful in 2020
		S-500 AMB	Tested in 2021
Russia	Co-orbital	IS	Tested in 1963-71, cancelled in 1993

Country	Type	Title	Status
		Almaz	Crewed in 1973-75, weapons tested once, cancelled
		ISM	Tested until 1983, cancelled
		Naryad	Tested from 1990-94, cancelled
		Nivelir/Burevestnik	2011 SSA project
		Rockot	Launched in 2014, rendezvous in 2019, inactive since 2023
China	Direct Ascent	Program 640	Cancelled in 1980
		Program 863	Tested in 1990s and 2003
		SC19	Tested since 2005 Various tests in 2013 and 2014 attributed to it
		DN3	2018 interception test
	Co-orbital	SJ-06F	Launched in 2008
		SJ-12	Launched 2010
		SJ-15	Launched in 2013 and rendezvous in 2014
		SJ-17	Launched in 2016
		TJS-3	Launched in 2018, presumed decommissioned in 2021
		SJ-21	Launched in 2021, rendezvous in 2022, unregistered
		SY-12	Launched in 2021
India	Direct Ascent	Agni	Simulation tests in 2012
		AAD	Successful intercept in 2017
		PVD	Successfully tested in 2018
		Shakti	Successful test in 2019

Part 2: Alleged Space cyber-attacks since 2007

Year	Who was the attacker, (alleged)	Attacked, (alleged)	Alleged or confirmed	Type of Attack	What happened
2007	Tamil Tigers extremist separatist group	U.S. broadcasting satellite	Confirmed	Against ground segment	Hacked ground C2 nodes gaining control of broadcasting satellite
2008	(China)	Landsat 7 and Terra (EOS AM-1 satellites)	Alleged	Man-in-the-Middle Attack	U.S. government satellites on four occasions were attacked via a ground station in Spitsbergen, Norway that NASA uses for data transfers over the open internet.
2011	(Chinese IP address)	Jet Propulsion Laboratory. NASA	Alleged	Stolen data	Hackers took over Jet Propulsion Laboratory (JPL) computers and "compromised the accounts of the most privileged JPL users". Across 18 servers, 87 gigabytes of data were stolen.
2014	(China)	National Oceanic and Atmospheric Administration services (NOAA's) computer network. United States	Alleged	Systems disruption attack	Satellite which provided weather data and products for the National Environmental Satellite, Data, and Information Services and National Earth System Prediction Capability were attacked. Nothing was distributed publicly, however systems were down for two days to be cleaned.

Year	Who was the attacker, (alleged)	Attacked, (alleged)	Alleged or confirmed	Type of Attack	What happened
2018	Thrip (linked to China)	United States satellite companies (nonspecific)	Confirmed	Attempts to take over control	Thrip manually looked for a very specific software program to command and take total control of one satellite companies operational technology.
2021	Ghost Shell – an offshoot of the group, Anonymous	NASA	Confirmed	Data steal and leak	Log-in names, passwords, email addresses and CVs, plus contents of online databases of NASA, FBI, the European Space Agency and other government agencies and contractors were published online.
2022	Russia	Viasat KA-SAT (telecommunications satellite)	Confirmed	Interference	40,000 to 45,000 European customers were without broadband, and a German wind turbine company lost remote connection.

Part 3: Relevant national policy, legal and regulatory frameworks

Part 4: Relevant international policy, legal and regulatory frameworks

Outer Space Treaty (OST), 1967:

Article III:

"States Parties to the Treaty shall carry on activities in the exploration and use of outer space, including the moon and other celestial bodies, in accordance with international law, including the Charter of the United Nations, in the interest of maintaining international peace and security and promoting international co-operation and understanding."

Article VI:

"States Parties to the Treaty shall bear international responsibility for national activities in outer space, including the Moon and other celestial bodies, whether such activities are carried on by governmental agencies or by non-governmental entities, and for assuring that national activities are carried out in conformity with the provisions set forth in the present Treaty. The activities of non-governmental entities in outer space, including the Moon and other celestial bodies, shall require authorization and continuing supervision by the appropriate State Party to the Treaty. When activities are carried on in outer space, including the Moon and other celestial bodies, by an international organization, responsibility for compliance with this Treaty shall be borne both by the international organization and by the States Parties to the Treaty participating in such organization."

Article VII:

"Each State Party to the Treaty that launches or procures the launching of an object into outer space, including the Moon and other celestial bodies, and each State Party from whose territory or facility an object is launched, is internationally liable for damage to another State Party to the Treaty or to its natural or juridical persons by such object or its component parts on the Earth, in air space or in outer space, including the Moon and other celestial bodies."

Article IX:

"In the exploration and use of outer space, including the Moon and other celestial bodies, States Parties to the Treaty shall be guided by the principle of co-operation and mutual assistance and shall conduct all their activities in outer space, including the Moon and other celestial bodies, with due regard to the corresponding interests of all other States Parties to the Treaty. States Parties to the Treaty shall pursue studies of outer space, including the Moon and other celestial bodies, and conduct exploration of them so as to avoid their harmful contamination and also adverse changes in the environment of the Earth resulting from the introduction of extraterrestrial matter and, where necessary, shall adopt appropriate measures for this purpose. If a State Party to the Treaty has reason to believe that an activity or experiment planned by it or its nationals in outer space, including the Moon and other celestial bodies, would cause potentially harmful interference with activities of other States Parties in the peaceful exploration and use of outer space, including the Moon and other celestial bodies, it shall undertake appropriate international consultations before proceeding with any such activity or experiment. A State Party to the Treaty which has reason to believe

that an activity or experiment planned by another State Party in outer space, including the Moon and other celestial bodies, would cause potentially harmful interference with activities in the peaceful exploration and use of outer space, including the Moon and other celestial bodies, may request consultation concerning the activity or experiment."

Antarctic Treaty System (ATS), 1959:

Article I:

"Antarctica shall be used for peaceful purposes only. There shall be prohibited, inter alia, any measures of a military nature, such as the establishment of military bases and fortifications, the carrying out of military maneuvers, as well as the testing of any type of weapons."

Article VI:

"The provisions of the present Treaty shall apply to the area south of 60o South latitude, including all ice shelves, but nothing in the present Treaty shall prejudice or in any way affect the rights, or the exercise of the rights, of any State under international law with regard to the high seas within that area."

Article IX:

"Each of the Contracting Parties undertakes to exert appropriate efforts, consistent with the Charter of the United Nations, to the end that no one engages in any activity in Antarctica contrary to the principles or purposes of the present Treaty."

Article XI:

"If any dispute arises between two or more of the Contracting Parties concerning the interpretation or application of the present Treaty, those Contracting Parties shall consult among themselves with a view to having the dispute resolved by negotiation, inquiry, mediation, conciliation, arbitration, judicial settlement or other peaceful means of their own choice. Any dispute of this character not so resolved shall, with the consent, in each case, of all parties to the dispute, be referred to the International Court of Justice for settlement; but failure to reach agreement on reference to the International Court shall not absolve parties to the dispute from the responsibility of continuing to seek to resolve it by any of the various peaceful means referred to in paragraph 1 of this Article."

Antarctic Search and Rescue (SAR) Workshop 5 Improving SAR Coordination and Response in the Antarctic 2023. Agreement N.37:

"Every large-scale SAR operation requires international cooperation to one extent or another",

United Nations Charter, Chapter VII: Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression

Article 39

"The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security."

Article 40

“In order to prevent an aggravation of the situation, the Security Council may, before making the recommendations or deciding upon the measures provided for in Article 39, call upon the parties concerned to comply with such provisional measures as it deems necessary or desirable. Such provisional measures shall be without prejudice to the rights, claims, or position of the parties concerned. The Security Council shall duly take account of failure to comply with such provisional measures.”

Article 41

“The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations.”

Article 42

“Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security. Such action may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations.”

UN General Assembly resolution 58/199 on the Creation of a global culture of cybersecurity and the protection of critical information infrastructures (30 Jan. 2004):

“Critical infrastructures — such as those used for, inter alia, the generation, transmission and distribution of energy, air and maritime transport, banking and financial services, e-commerce, water supply, food distribution and public health — and the critical information infrastructures that increasingly interconnect and affect their operations.”

Annex C – Bibliography

Abbany, Zulfikar. "Modern Spy Satellites in an Age of Space Wars." Dw.Com, August 26, 2020. https://www.dw.com/en/modern-spy-satellites-in-an-age-of-space-wars/a-54691887.

Aerospace. "Counterspace Timeline, 1959-2022." March 31, 2023, https://aerospace.csis.org/counterspace-timeline/.

Australian Space Agency, "About the Agency." n.d., https://www.space.gov.au/about-agency.

Australian Space Agency. "Advancing Australia's position in the global space economy." n.d. https://www.space.gov.au/moon-mars-initiative.

Australian Space Agency. "Real-time traffic management in space." n.d. https://www.space.gov.au/real-time-traffic-management-space.

Australian Space Agency. "Robotics and Automation on Earth and in Space Roadmap." January 24, 2022. https://www.space.gov.au/about-agency/publications/state-space-2021.

Australian Space Agency. "State of Space 2021." July 1, 2022. https://www.space.gov.au/about-agency/publications/state-space-2021.

Australian Space Agency. "Team Artemis Australia." n.d. https://www.space.gov.au/team-artemis-australia.

Australian Space Agency. "Trans-Tasman collaboration to advance space sector innovation." January 31, 2024, https://www.space.gov.au/news-and-media/trans-tasman-collaboration-advance-space-sector-innovation.

Axe, David. "Russia's Jamming Force Could Isolate Ukrainian Troops—So Artillery Can Destroy Them." Forbes, November 23, 2021. https://www.forbes.com/sites/davidaxe/2021/11/23/russias-jamming-force-could-isolate-ukrainian-troops-so-artillery-can-destroy-them/.

Bardoe, Barrie. "Making Space Safer." Department of Defence News. March 27, 2023. https://www.defence.gov.au/news-events/news/2023-03-27/making-space-safer.

Beale, Jonathan. "Space, the Unseen Frontier in the War in Ukraine." BBC News, October 5, 2022. https://www.bbc.com/news/technology-63109532.

Berger, Eric. "The US Military Just Proved It Can Get Satellites Into Space Super Fast." Ars Technica, September 15, 2023. https://arstechnica.com/space/2023/09/firefly-and-space-force-demonstrate-ability-to-rapidly-launch-a-satellite/.

Bingen, Kari A., Kaitlyn Johnson, Makena Young, and John Raymond. "Space Threat Assessment 2023." July 5, 2023. https://www.csis.org/analysis/space-threat-assessment-2023.

Bowman, Alison. "SmartSat and New Zealand Space Agency Collaborate on Joint R&D Initiatives to Advance Space Sector Innovation." SmartSat CRC, January 30, 2024.

https://smartsatcrc.com/smartsat-and-new-zealand-space-agency-collaborate-on-joint-rd-initiatives-to-advance-space-sector-innovation/.

Broad, William J., and David E. Sanger. "China Tests Anti-Satellite Weapon, Unnerving U.S." The New York Times, January 18, 2007. https://www.nytimes.com/2007/01/18/world/asia/18cnd-china.html.

Browne, Ryan and Barbara Starr. "US government warns of Iranian threats to commercial shipping, including GPS interference," CNN, August 7, 2019. https://edition.cnn.com/2019/08/07/politics/us-warns-of-iranian-threats-to-shipping/index.html.

Brumfiel, Geoff. "Russia Is Working on a Weapon to Destroy Satellites but Has Not Deployed One Yet." NPR, February 15, 2024. https://www.npr.org/2024/02/15/1231594952/russia-national-security-threat-space-nuclear.

Butt, Yousaf. "Effects of Chinese Laser Ranging on Imaging Satellites." Science & Global Security 17, no. 1 (June 26, 2009): 20–35. https://doi.org/10.1080/08929880902864376.

Clark, Colin. "Aussie Space Command Looks to Electronic Warfare, Other Tech to Deter Attacks on Satellites." Breaking Defense, March 2, 2023. https://breakingdefense.com/2023/03/aussie-space-command-looks-to-electronic-warfare-other-tech-to-deter-attacks-on-satellites/.

Cook, Ellie. "What Is FTG-12? Pentagon's Space Missile Interceptor Passes New Test." Newsweek, December 12, 2023. https://www.newsweek.com/pentagon-ballistic-missile-air-defense-system-interceptor-test-ftg12-1851601.

Corera, Gordon. "Russia Hacked Ukrainian Satellite Communications, Officials Believe." BBC News, March 25, 2022. https://www.bbc.com/news/technology-60796079.

Davies, Andrew. "Australia's WGS Communications—what Went Wrong?" The Strategist, September 21, 2015. https://www.aspistrategist.org.au/australias-wgs-communications-what-went-wrong/.

De Selding, Peter B. "ITU Implores Iran to Help Stop Jamming." SpaceNews, January 19, 2023. https://spacenews.com/itu-implores-iran-help-stop-jamming/.

Defence, Science and Technology Group. "Resilient Multi-Mission Space." n.d. https://www.dst.defence.gov.au/strategy/star-shots/resilient-multi-mission-space.

Department of Defence. "2020 Force Structure Plan." 2020. https://www.defence.gov.au/about/strategic-planning/2020-force-structure-plan.

Department of Defence. "Geospatial intelligence services." n.d. https://www.defence.gov.au/defence-activities/products-services/geospatial-intelligence-services.

Department of Defence. "National Defence: Defence Strategic Review 2023." 2023. https://www.defence.gov.au/about/reviews-inquiries/defence-strategic-review.

Department of Defence. "New Defence space capability boosts regional security." December 2, 2023. https://www.minister.defence.gov.au/media-releases/2023-12-02/new-defence-space-capability-boosts-regional-security.

Department of Defence. "Operation Dyurra." n.d. https://www.defence.gov.au/defence-activities/operations/dyurra.

Department of Defence. "Organisation structure." n.d. https://www.defence.gov.au/about/who-we-are/organisation-structure.

Department of Foreign Affairs and Trade. "The Quad." n.d. https://www.dfat.gov.au/international-relations/regional-architecture/quad.

Department of Industry, Science and Resources. "Announcing the 2023-2025 Budget." May 10, 2023. https://www.industry.gov.au/news/announcing-2023-24-budget.

Department of Industry, Science and Resources. "Australian Civil Space Strategy 2019-2028." April 1, 2019, https://www.industry.gov.au/publications/australian-civil-space-strategy-2019-2028.

Dougherty, Kerrie. "Upper Atmospheric Research at Woomera: The Australian-Built Sounding Rockets." Acta Astronautica 59, no. 1 (2006): 54–67. https://doi.org/10.1016/j.actaastro.2006.02.015.

DrasticNews. "The War Satellite Cometh – New Technology Definition Reasearch Note." Space & Defence. December 7, 2021. https://spaceanddefense.io/the-war-satellite-cometh-new-technology-definition-research-note/.

Erwin, Sandra. "Air Force: SSA Is No More; It's 'Space Domain Awareness'." SpaceNews, January 23, 2023. https://spacenews.com/air-force-ssa-is-no-more-its-space-domain-awareness/.

Erwin, Sandra. "Space Force Needs Sensors to Distinguish Weapons From Benign Objects." SpaceNews, January 23, 2023. https://spacenews.com/space-force-needs-sensors-to-distinguish-weapons-from-benign-objects/.

European Space Policy Institute. "Emerging Spacefaring Nations." June 21, 2021. https://www.espi.or.at/reports/emerging-spacefaring-nations/.

Foust, Jeff. "More Countries Encouraged to Commit to Halt Destructive ASAT Tests." SpaceNews, June 15, 2023. https://spacenews.com/more-countries-encouraged-to-commit-to-halt-destructive-asat-tests/.

Foust, Jeff. "U.S. to Introduce U.N. Resolution on ASAT Testing Ban." SpaceNews, January 23, 2023. https://spacenews.com/u-s-to-introduce-u-n-resolution-on-asat-testing-ban/.

Frantzman, Seth. "Israel Launches Ofek 16 Satellite to Complete Intelligence Coverage." Defense News, August 18, 2022. https://www.defensenews.com/space/2020/07/06/israel-launches-ofek-16-satellite-to-complete-intelligence-coverage/.

Garrick, Matt. "NASA Successfully Launches Its First Rocket From Newly Created Arnhem Space Centre." ABC News, June 26, 2022. https://www.abc.net.au/news/2022-06-27/nasa-launch-rocket-arnhem-land-success/101183776.

Gilmour Space. "LAUNCH." n.d. https://www.gspace.com/launch.

Gordon, Michael R., and Jeremy Page. "China Installed Military Jamming Equipment on Spratly Islands, U.S. Says," The Wall Street Journal, April 9, 2018.

https://www.wsj.com/articles/china-installed-military-jamming-equipment-on-spratly-islands-u-s-says-1523266320/.

Greene, Andrew. "RAAF Planning for New Military Space Command as It Celebrates 100th Anniversary." ABC News, March 30, 2021. https://www.abc.net.au/news/2021-03-31/raaf-looks-to-space-as-it-celebrates-100-years/100039914.

Greene, Andrew. "Royal Australian Air Force Air Vice-Marshal Catherine Roberts to Become Australia's First Space Commander." ABC News, May 7, 2021. https://www.abc.net.au/news/2021-05-08/air-force-vice-marshal-catherine-roberts-australia-space-command/100124660.

Grimm, Nick. "Scientists Plan to Use High Powered Lasers to Track and Shoot Away Space Junk." ABC News, March 21, 2018. https://www.abc.net.au/news/2018-03-21/scientists-plan-to-shoot-down-space-junk-with-a-laser/9573066.

Harris, Mark. "Ghost Ships, Crop Circles, and Soft Gold: A GPS Mystery in Shanghai." MIT Technology Review, June 17, 2020. https://www.technologyreview.com/2019/11/15/131940/ghost-ships-crop-circles-and-soft-gold-a-gps-mystery-in-shanghai/.

Harrison, Ruth. "ADF Establishes New Defence Space Command Branch." Space Australia, March 29, 2022. https://spaceaustralia.com/index.php/news/adf-establishes-new-defence-space-command-branch.

Hendrickx, Bart. "Kalina: A Russian Ground-based Laser to Dazzle Imaging Satellites," The Space Review, July 5, 2022. https://www.thespacereview.com/article/4416/1.

Hendrickx, Bart. "Peresvet: A Russian Mobile Laser System to Dazzle Enemy Satellites," The Space Review, June 15, 2020. https://www.thespacereview.com/article/3967/1.

Hong, Andy. "South Korea's Space Program Is a Big Deal." The Diplomat, July 1, 2022. https://thediplomat.com/2022/07/south-koreas-space-program-is-a-big-deal/.

Hoskins, Peter. "Virgin Orbit: Branson's Rocket Dream Ends After Mission Failure." BBC News, May 24, 2023. https://www.bbc.com/news/business-65692302.

Hudson, John. "Nobody Knows if Iran's Drone Hack Was a Hoax." The Atlantic, October 30, 2013. https://www.theatlantic.com/international/archive/2012/04/nobody-knows-if-irans-drone-hack-was-hoax/328944/.

India Times. "NASA Calls India's Mission Shakti 'Terrible', as It Added 400 Dangerous Pieces to Earth's Orbit." April 2, 2019. https://www.indiatimes.com/technology/science-and-future/mission-shakti-created-400-pieces-of-dangerous-debris-that-can-harm-space-station-says-nasa-364702.html.

Iyengar, Rishi. "Starlink Ukraine: Why Elon Musk Is the Go-To Internet Provider." Foreign Policy, January 9, 2023. https://foreignpolicy.com/2022/11/22/ukraine-internet-starlink-elon-musk-russia-war/.

Jennings, Ralph. "China Has Capability to Use Space for Military Purposes, Experts Say." Voice of America, April 2, 2022. https://www.voanews.com/a/china-has-capability-to-use-space-for-military-purposes-experts-say/6512155.html.

Jewett, Rachel. “UN General Assembly Adopts Draft Resolution Against ASAT Tests.” Satellite Today, December 9, 2022. https://www.satellitetoday.com/government-military/2022/12/09/un-general-assembly-adopts-draft-resolution-against-asat-tests/.

Joint Chiefs of Staff, “USG Compendium of Interagency and Associated Terms,” DoD Terminology Program, November, 2019, p. 299, https://www.jcs.mil/Doctrine/DOD-Terminology-Program/

Kessler, Glenn. “Bachmann’s Claim That China ‘Blinded’ U.S. Satellites.” Washington Post, October 4, 2011. https://www.washingtonpost.com/blogs/fact-checker/post/bachmanns-claim-that-china-blinded-us-satellites/2011/10/03/gIQAHvm7IL_blog.html.

Kluth, Andreas. “The World Is Still Better off With US Hegemony.” Washington Post, September 13, 2023. https://www.washingtonpost.com/business/energy/2023/09/13/the-world-is-still-better-off-with-us-hegemony/eb4eaaf6-51ec-11ee-accf-88c266213aac_story.html.

Knapton, Sarah. “Elon Musk's Starlink Satellites Aiding Ukraine May Be Legally Destroyed by Russia, Says Space Expert.” The Telegraph, November 26, 2023. https://www.telegraph.co.uk/world-news/2023/11/26/elon-musk-starlink-ukraine-russia-destroyed-space-law/.

Lockheed Martin. “Lockheed Martin Selected as Preferred Bidder for JP9102.” April 3, 2023, https://news.lockheedmartin.com/2023-04-03-Lockheed-Martin-selected-as-preferred-bidder-for-JP9102.

Mahlandt, Taylor. “France Wants to Use Lasers to Protect Its Satellites.” Slate Magazine, August 1, 2019. https://slate.com/technology/2019/08/france-space-command-plan-satellites-lasers.html.

Masson-Zwaan, Tanja, “New States in Space.” AJIL Unbound 113 (2019): 99. https://doi.org/10.1017/aju.2019.13.

Mcguirk, Rod. “Australia Plans Major Overhaul of Defences as China Rises.” AP News, April 24, 2023. https://apnews.com/article/australia-defense-strategic-review-china-be313bcbd58e6793a8c85b79682c0e34.

McKnight, Patricia. “Google Maps Satellite Images Appear to Show Position of Russian Troops.” Newsweek, April 19, 2022. https://www.newsweek.com/google-maps-satellite-images-appear-show-position-russian-troops-1698766.

McLaughlin, Andrew. “Founding Head of Defence Space Command Hands Over to New Leader.” PS News. December 22, 2023. https://psnews.com.au/founding-head-of-defence-space-command-hands-over-to-new-leader/125008/.

Mearsheimer, John J. “Can China Rise Peacefully?” The National Interest, January 7, 2024. https://nationalinterest.org/commentary/can-china-rise-peacefully-10204.

Moss, Tristan. “The Space Between Alliance and Self-reliance: The Evolution of the Australia-US Defence Space Relationship.” United States Studies Centre, August 28, 2023. https://www.ussc.edu.au/the-evolution-of-the-australia-us-defence-space-relationship.

National Aeronautics and Space Administration. “The Artemis Accords.” February 1, 2024, https://www.nasa.gov/artemis-accords/.

Nuclear Threat Initiative. “PAROS Treaty.” May 31, 2022, https://www.nti.org/education-center/treaties-and-regimes/proposed-prevention-arms-race-space-paros-treaty/.

Optus. “Optus C1 Satellite.” n.d. https://www.optus.com.au/living-network/satellite/fleet/c1.

Osborn, Kris. “Just How Strong Are China’s Air Defenses?” The National Interest, December 6, 2021. https://nationalinterest.org/blog/reboot/just-how-strong-are-china%E2%80%99s-air-defenses-197522.

Pandit, Rajat. “DRDO Plans Star Wars-style Weapons for Battles of Future.” The Times of India, September 14, 2020. https://timesofindia.indiatimes.com/india/drdo-plans-star-wars-style-weapons-for-battles-of-future/articleshow/78096712.cms.

Panwar, Lt Gen R S. “Future WarsIndia’s Space Programme: Organisations and Warfighting Potential.” Future Wars, November 18, 2021. https://futurewars.rspanwar.net/indias-space-programme-organisations-and-warfighting-potential/.

Prime Minister of Australia. “AUKUS Nuclear-Powered Submarine Pathway.” March 14, 2023. https://www.pm.gov.au/media/aukus-nuclear-powered-submarine-pathway.

Prime Minister of Australia. “Joint Leaders Statement on AUKUS.” March 14, 2023. https://www.pm.gov.au/media/joint-leaders-statement-aukus.

Pultarova, Tereza. “SpaceX Starlink Satellites Had to Make 25,000 Collision-avoidance Manoeuvres in Just 6 Months — and It Will Only Get Worse.” Space.Com, July 6, 2023. https://www.space.com/starlink-satellite-conjunction-increase-threatens-space-sustainability.

Rachman, Gideon. “From the US to Ukraine, the Gaza War Will Change the World.” Financial Times, November 6, 2023. https://www.ft.com/content/917a006d-db2c-45ce-a0dd-cd92749fe7b6.

Rainbow, Jason. “Eutelsat Says Satellite Jammers Within Iran Are Disrupting Foreign Channels.” SpaceNews, March 3, 2023. https://spacenews.com/eutelsat-says-satellite-jammers-within-iran-are-disrupting-foreign-channels/.

Rajagopalan, Rajeswari Pillai. “What Are India’s Plans for Directed Energy Weapons?” The Diplomat, September 24, 2020. https://thediplomat.com/2020/09/what-are-indias-plans-for-directed-energy-weapons/.

Royal Australian Air Force. “Defence Space Strategy - Defence Space Power eManual.” 2022. https://www.airforce.gov.au/our-work/strategy/defence-space-strategy.

Royal Australian Air Force. “Defence Space Strategy.” 2022. https://www.airforce.gov.au/our-work/strategy/defence-space-strategy.

Ryall, Julian. “North Korea 'Aggressively' Jamming BBC'S New Korean-language Service.” The Telegraph, September 27, 2017. https://www.telegraph.co.uk/news/2017/09/27/north-korea-aggressively-jamming-new-bbc-broadcasts/.

Sang-Hun, Choe. “North Korea Tried to Jam GPS Signals Across Border, South Korea Says.” The New York Times, April 1, 2016. https://www.nytimes.com/2016/04/02/world/asia/north-korea-jams-gps-signals.html.

Secure World Foundation. “Global Counterspace Capabilities Report 2025.” May 26, 2025. https://swfound.org/counterspace/.

Shrimpton, Bec. “The Time Is Right for Australia to Re-establish Its Reputation as a Global Space Power | the Strategist.” The Strategist, June 7, 2021. https://www.aspistrategist.org.au/the-time-is-right-for-australia-to-re-establish-its-reputation-as-a-global-space-power/.

Silverstein, Benjamin, and Ankit Panda. “Reducing Risks to Space Systems: Recommendations for the UN Secretary-General.” Carnegie Endowment for International Peace, April 30, 2021. https://carnegieendowment.org/2021/04/30/reducing-risks-to-space-systems-recommendations-for-un-secretary-general-pub-84453.

Singh, Mandeep. “Drone Swarms: The Emerging Threat.” Indian Defence Review, September 1, 2019. https://www.indiandefencereview.com/news/drone-swarms-the-emerging-air-threat/

Smith, Belinda. “What Is Australia’s Space Division, and Why Is It in the Military?” ABC News, May 13, 2021. https://www.abc.net.au/news/science/2021-05-13/australia-space-division-military-satellites-air-force-commander/100127978.

Smith, Sheila A. “The Quad in the Indo-Pacific: What to Know.” Council on Foreign Relations, May 27, 2021. https://www.cfr.org/in-brief/quad-indo-pacific-what-know.

Southern Launch. “Whalers Way Orbital Launch Complex.” n.d. https://www.southernlaunch.space/whalers-way-orbital-launch-complex.

SpaceNews Editor. “NRO Confirms Chinese Laser Test Illuminated U.S. Spacecraft,” SpaceNews, October 3, 2006. https://spacenews.com/nro-confirms-chinese-laser-test-illuminated-us-spacecraft/.

Sputnik International. “Sky’s the Limit: Russia’s Unique Jamming System Getting Upgrade,” Sputnik Globe, December 5, 2016. https://sputnikglobe.com/20161205/russia-electronic-warfare-system-1048187517.html.

Staff Writer. “Japan Requests Record $50 Billion Defense Budget in Eighth Straight Increase.” The Defense Post, July 26, 2020. https://www.thedefensepost.com/2019/08/30/japan-record-defense-budget-50-billion/.

Starchak, Maxim. “Where Is Russia’s S-500 Air Defense System?” Defense News, October 5, 2023. https://www.defensenews.com/industry/2023/10/05/where-is-russias-s-500-air-defense-system/.

Su, Jianyong. “The ‘Peaceful Purposes’ Principle in Outer Space And The Russia–China PPWT Proposal.” Space Policy 26, no. 2 (May 1, 2010): 81–90. https://doi.org/10.1016/j.spacepol.2010.02.008.

Swope, Claiton, Kari Bingen, Mekena Young, and Kendra Lafave. “Space Threat Assessment 2025.” May, 2025. https://www.csis.org/analysis/space-threat-assessment-2025

Tellis, Ashley J. "India's ASAT Test: An Incomplete Success." Carnegie Endowment for International Peace, April 15, 2019. https://carnegieendowment.org/2019/04/15/india-s-asat-test-incomplete-success-pub-78884.

The White House. "Implementation of the Australia – United Kingdom – United States Partnership (AUKUS): Fact Sheet" April 5, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/05/fact-sheet-implementation-of-the-australia-united-kingdom-united-states-partnership-aukus/.

Tillett, Andrew, and Tom McIlroy. "AUKUS Will Create 20,000 Jobs and 'Safeguard Economy.'" Australian Financial Review, March 12, 2023. https://www.afr.com/politics/federal/aukus-will-create-20-000-jobs-and-safeguard-economy-20230312-p5crej.

Trevithick, Joseph. "X-37B's Power Beaming Payload a Reminder of Potential Orbital Microwave Anti-Satellite Weapons." The War Zone, May 19, 2020. https://www.twz.com/33531/x-37bs-power-beaming-payload-a-reminder-of-potential-orbital-microwave-anti-satellite-weapons.

Tronchetti, Fabio, and Hao Liu. "Australia Between the Moon Agreement and the Artemis Accords - Australian Institute of International Affairs." Australian Institute of International Affairs, June 3, 2021. https://www.internationalaffairs.org.au/australianoutlook/australia-between-the-moon-agreement-and-the-artemis-accords/.

Tucker, Patrick. "Pentagon Wants to Test a Space-Based Weapon in 2023." Defense One, April 13, 2021. https://www.defenseone.com/technology/2019/03/pentagon-wants-test-space-based-weapon-2023/155581/.

Tucker, Patrick. "Russia Claims It Now Has Lasers to Shoot Satellites." Defense One, April 12, 2021. https://www.defenseone.com/technology/2018/02/russia-claims-it-now-has-lasers-shoot-satellites/146243/.

United Nations Office for Disarmament Affairs. "Open-Ended Working Group on Reducing Space Threats (2022)." 2022. https://meetings.unoda.org/open-ended-working-group-on-reducing-space-threats-2022.

United Nations Office for Outer Space Affairs. "Agreement on the Rescue of Astronauts and the Returning of Space Objects Launched into Outer Space." December, 1968, https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introrescueagreement.html.

United Nations Office for Outer Space Affairs. "Committee on the Peaceful Uses of Outer Space." n.d. https://www.unoosa.org/oosa/en/ourwork/copuos/index.html.

United Nations Office for Outer Space Affairs. "Convention on International Liability for Damage Caused by Space Objects." September, 1972. https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introliability-convention.html.

United Nations Office for Outer Space Affairs. "Convention on Registration of Objects Launched into Outer Space." September 15, 1976.

https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introregistration-convention.html.

United Nations Office for Outer Space Affairs. "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies." October, 1967. https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html.

United Nations. "Speakers Renew Calls for Treaty to Prevent Arms Race in Space as First, Fourth Committees Convene Joint Meeting." October 27, 2022. https://press.un.org/en/2022/gaspd761.doc.htm.

United States Space Force. "Advanced Extremely High Frequency System (AEHF)." August, 2021, https://www.spoc.spaceforce.mil/About-Us/Fact-Sheets/Display/Article/2381348/advanced-extremely-high-frequency-system-aehf.

United States Space Force. "Wideband Global SATCOM Satellite." February, 2023, https://www.spaceforce.mil/About-Us/Fact-Sheets/Article/2197740/wideband-global-satcom-satellite/.

Urrutia, Doris Elin. "India's Anti-Satellite Missile Test Is a Big Deal. Here's Why." Space.Com, August 10, 2022. https://www.space.com/india-anti-satellite-test-significance.html.

Varfolomeeva, Anna. "Signaling Strength: Russia's Real Syria Success Is Electronic Warfare Against the US." The Defense Post, April 30, 2019. https://www.thedefensepost.com/2018/05/01/russia-syria-electronic-warfare/.

Varley, Len. "Toowoomba Airport Selected as Virgin Orbit Space Launch Site." AviationSource News, September 20, 2022. https://aviationsourcenews.com/news/toowoomba-airport-selected-as-virgin-orbit-space-launch-site/.

Wall, Mike. "Kessler Syndrome and the Space Debris Problem." Space.com, July 14, 2022. https://www.space.com/kessler-syndrome-space-debris.

Wang, Brian. "Russia Will Place GPS Jammers on 250,000 Cellphone Towers to Reduce Enemy Cruise Missile and Drone Accuracy." NextBigFuture.Com, April 7, 2017. https://www.nextbigfuture.com/2016/10/russia-will-place-gps-jammers-on-250000.html.

Waterman, Shaun. "Space Lasers Come of Age: Optical Communications for Satellites Are Ready for Prime Time." Via Satellite. February 22, 2022. https://interactive.satellitetoday.com/via/march-2022/space-lasers-come-of-age-optical-communications-for-satellites-are-ready-for-prime-time/.

Williams, Martyn. "Report: DPRK Jams South Korean Satellite Comms." North Korea Tech - 노스코리아테크, November 17, 2012. https://www.northkoreatech.org/2012/11/17/report-dprk-jams-south-korean-satellite-comms/.

Windrem, Robert. "U.S. Satellite Feeds to Iran Jammed," NBC News, October 24, 2003. https://www.nbcnews.com/id/wbna3340692.

Wright, Robin. “Does the U.S.-Russia Crisis Over Ukraine Prove That the Cold War Never Ended?” The New Yorker, February 19, 2022. https://www.newyorker.com/news/daily-comment/does-the-us-russia-crisis-over-ukraine-prove-that-the-cold-war-never-ended.

ACKNOWLEDGMENTS

The authors would like to thank the financial support provided by Defence through a Strategic Policy Grant. All views and shortcomings are responsibility of the authors and do not necessarily reflect Defence’s views and opinions.

The authors would also like to thank the contributions of Marco Aliberti (European Space Policy Institute), Dr Vinicius Guedes Gonçalves de Oliveira (Flinders – JBC), Mathieu Bataille (European Space Policy Institute), Michelle Neumann (University of Adelaide), Camille Bitton (University of Adelaide), and the Jeff Bleich Centre for Democracy and Disruptive Technologies Vienna Space Internship student interns Sailor Tyler, Eloise Clarke and Ellen Feeney for their contribution to this project.

PROJECT COORDINATORS

Professor Rodrigo Praino, Director & Professor of Politics and Public Policy, Jeff Bleich Centre for Democracy and Disruptive Technologies, Flinders University.

Professor Melissa de Zwart, Professor Space Law and Governance, Andy Thomas Centre for Space Resources & Deputy Director, ARC Centre for Excellence in Plants 4 Space, University of Adrelaide.

Sumen Rai, Director, Defence Innovation Partnership.

Flinders University

Jeff Bleich Centre
for Democracy and
Disruptive Technologies

Contact us
jbc@flinders.edu.au