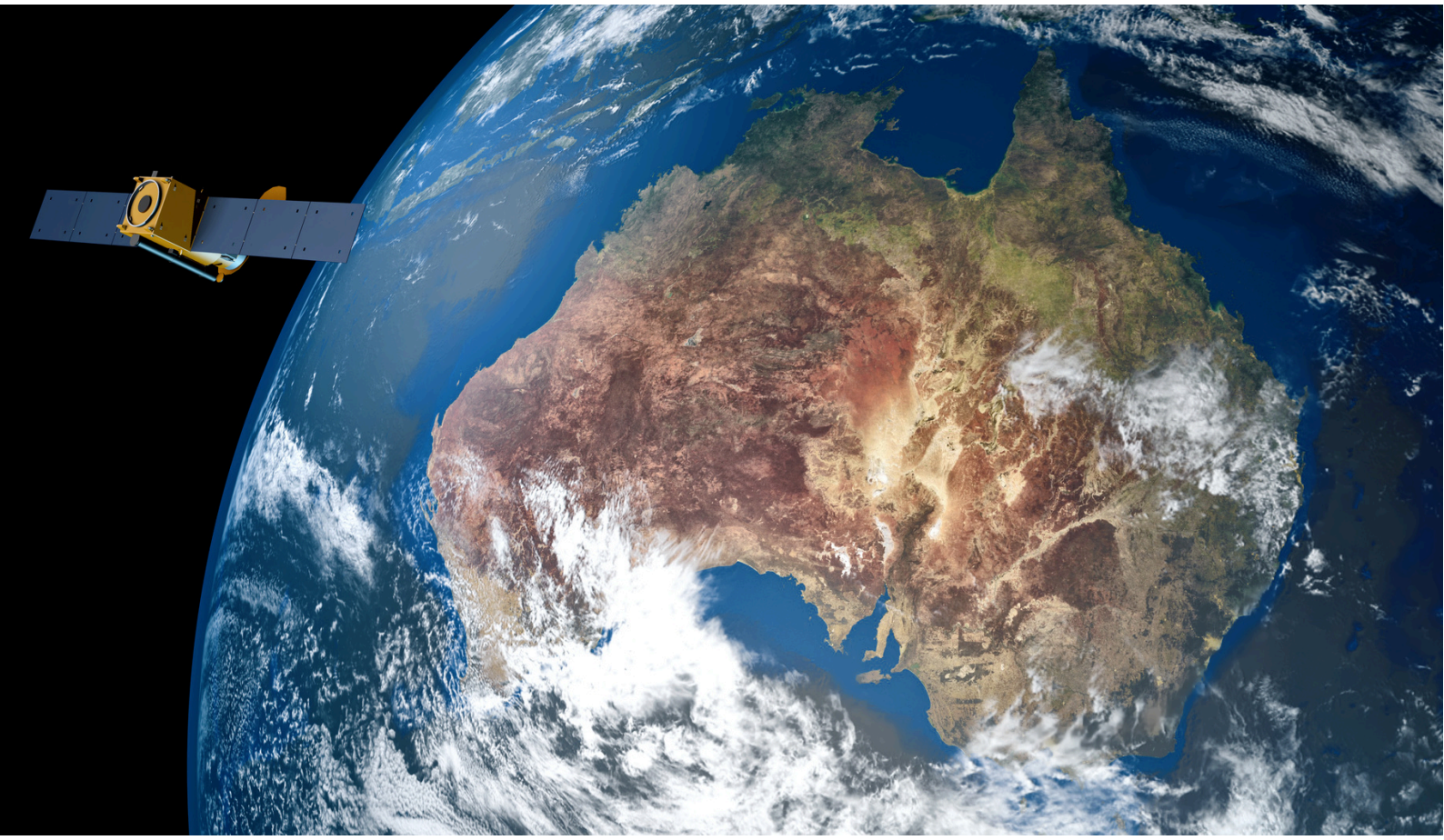
SECURING AUSTRALIA THROUGH SPACE: SPACE TECHNOLOGY AS CRITICAL INFRASTRUCTURE

STACEY HENDERSON AND JOEL LISK



ACSG Policy Paper Series
December 2024
www.spacegovcentre.org

ACSG
AUSTRALIAN CENTRE FOR SPACE GOVERNANCE

About the Authors

Dr Stacey Henderson is a Senior Research Fellow in Law and the Defence, Security & Space Lead with the Jeff Bleich Centre for Democracy and Disruptive Technology in the College of Business, Government and Law, Flinders University.

Joel Lisk is a Research Associate (Space and Regulation) and the Media & External Engagement Lead with the Jeff Bleich Centre for Democracy and Disruptive Technology in the College of Business, Government and Law, Flinders University.

About the Securing Australia Through Space Policy Papers Series

The Australian Centre for Space Governance hosted a workshop in March 2024 titled “Securing Australia Through Space”, where the question was posed: what does Australia need to secure, and how do space technologies help us to do so?

The workshop was attended by over 90 people, with the vast majority of attendees coming from a range of federal government departments and agencies. Experts from academia, government and industry were invited to give presentations and take part in roundtable discussions. This policy paper series is a result of the workshop.

The papers are authored by those who presented, and edited by Sarah O’Connor, Tristan Moss and Cassandra Steer on behalf of the Australian Centre for Space Governance. The opinions expressed in each paper are those of the authors in their individual capacity, and do not represent the views of any of their employers.

About the Australian Centre for Space Governance

The Australian Centre for Space Governance advocates for Australia’s interests in space in the 21st century and advances the agenda for responsible space governance.

We bring together the nation’s leading experts in fields such as space law, governance, policy, science and technology studies, security, property, history, ethics, political, and social sciences from across six different universities in Australia (Australian National University, Flinders University, RMIT University, University of Adelaide, UNSW Canberra, and Western Sydney University).

The ACSG has received funding from the Department of Defence, Geoscience Australia and the Department of Home Affairs.

Citation

Stacey Henderson and Joel Lisk, ‘Securing Australia Through Space: Space Technology as Critical Infrastructure’, Australian Centre for Space Governance, 2024.

SECURING AUSTRALIA THROUGH SPACE: SPACE TECHNOLOGY AS CRITICAL INFRASTRUCTURE

Stacey Henderson and Joel Lisk

Summary

- Australia is highly dependent on critical infrastructure systems, the destruction or degradation of which, would have a debilitating impact on Australia's defence and national security, a destabilising effect on the population, and cause significant damage to the economy.
- Space-based assets and systems that rely on space-based data are increasingly becoming embedded in critical infrastructure systems in Australia and globally.
- The space technology sector was added to the Australian legal framework designed to secure and protect critical infrastructure in 2022. The inclusion of space technology as critical infrastructure reflects the importance of space technology to everyday life in Australia.
- The security of critical infrastructure regime is primed and ready to be activated by the Australian Government but is not yet fully operational against all parts of the space technology sector.

Policy recommendations

- The Department of Home Affairs should activate the security of critical infrastructure regime in relation to all parts of the space technology sector. There should be no overlap in asset classes between space technology assets and space assets that are included in other critical infrastructure sectors, including the telecommunications sector and the defence sector.
- The Department of Home Affairs should update its guidance materials on the security of the critical infrastructure regime to make it clear which space technology assets are already captured under other critical infrastructure sectors and asset classes.
- The Department of Industry, Science and Resources should develop an educational program for space industry participants to ensure the critical infrastructure systems that their technology feeds into are appropriately hardened.

Australia is highly dependent on complex and critical systems that maintain the 'Australian way of life' as well as the nation's national security and integrity. These key critical systems are collectively referred to as critical infrastructure; systems so vital that their destruction or disruption would have a debilitating impact on Australia's defence and national security, a destabilising effect on the population, and cause significant damage to the economy.

For operators of critical infrastructure assets, the *Security of Critical Infrastructure* ('SOCI') regime imposes significant compliance obligations to ensure the Australian Government can remain confident that those assets are protected and capable of providing services to the wider Australian community. While owners and operators of space technology in Australia got a taste of the SOCI framework following the introduction of 'space technology' to the regime in 2022, application of the full force of the regime is yet to occur.

Eventually, it can be expected that the Australian government will 'activate' the SOCI regime for the space technology sector. This will require a wide range of actors to actively engage with the complex framework of legislation and subsidiary rules that exist to protect Australia.

More work is needed to develop the space technology workforce in Australia to ensure that the workforce has the skills necessary to identify risk and raise awareness among the Australian public about the importance of the space technology sector to Australia in terms of national security and defence, society, and the economy.

Space technologies as critical infrastructure

As society increasingly looks to outer space to support new technologies and augment existing terrestrial systems, space-based assets and systems that rely on space-based data are becoming embedded within critical infrastructure. The increasing reliance on space technology for navigation, communications, and remote sensing makes space technology an attractive target for malicious actors. In 2022, space technology was introduced into the Australian legal framework designed to secure and protect critical infrastructure. This treatment of space technology as critical infrastructure is not a novel approach by Australia, with the United States of America (US) and Europe adopting similar approaches to space technology. The inclusion appropriately reflects the importance of space technology to everyday life in Australia, despite a recent study showing that 64.1% of Australians surveyed were either neutral, disagreed, or strongly disagreed that space technology impacted their daily lives.[1]

The SOCI regime was introduced into Australia in 2018 through the *Security of Critical Infrastructure Act 2018* (Cth) ('SOCI Act'). The regime was originally introduced to 'strengthen the [Australian] Government's capacity to manage the ***national security*** risks of espionage, sabotage and coercion arising from foreign involvement in Australia's critical infrastructure' (emphasis in original).[2] The Australian Government's *2023 Critical Infrastructure Resilience Strategy* defines critical infrastructure as:

> those physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period,

would significantly impact the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security.[3]

In introducing the SOCI regime, the Australian Government acknowledged the importance of critical infrastructure as an essential element of the operation of Australian society and the economy, while also recognising the importance of ensuring that Australia remained an attractive destination for foreign investment, including in sectors designated as critical infrastructure.

How the SOCI regime operates

The object of the *SOCI Act* is to provide a framework for managing risks relating to critical infrastructure, by:

- improving transparency of ownership and operational control of critical infrastructure in Australia in order to better understand risks; and
- facilitating cooperation and collaboration between all levels of government and regulators, owners and operators of critical infrastructure, in order to identify and manage risks; and
- requiring responsible entities for critical infrastructure assets to identify and manage risks relating to those assets; and
- imposing enhanced cyber security obligations on relevant entities for systems of national significance in order to improve their preparedness for, and ability to respond to, cyber security incidents; and
- providing a regime for the Commonwealth to respond to serious cyber security incidents.[4]

The *SOCI Act* primarily works through a series of regulatory mechanisms that define particular 'sectors' where there is critical infrastructure and then critical infrastructure 'assets' within the sectors. The original *SOCI Act* only contained four sectors: electricity, gas, water, and ports. Subsequent amendments substantially expanded the number of critical infrastructure sectors to 11:

- the communications sector;
- the data storage or processing sector;
- the financial services and markets sector;
- the water and sewerage sector;
- the energy sector;
- the health care and medical sector;
- the higher education and research sector;
- the food and grocery sector;
- the transport sector;
- the space technology sector; and,
- the defence industry sector.[5]

During public consultations for the amendments, representatives of the Australian space industry advocated for the inclusion of space technology within the designated categories of critical infrastructure sectors to be protected.

The treatment of critical infrastructure assets is more variable and depends on the sectors. Some sectors have critical infrastructure assets listed in the *SOCI Act* itself. There are also powers contained within the *SOCI Act* for the designation of critical infrastructure assets through rules made under the legislation. Importantly, a critical infrastructure asset can be owned or operated by the Australian Government, the governments of states or territories, or any other entity.

The SOCI regime captures classes of critical infrastructure assets by their relationship with the broader sector. Broadly, the SOCI regime operates by requiring there to be a register of information related to critical infrastructure assets; requiring responsible entities for some of those assets to implement critical infrastructure risk management programs; requiring the notification of cyber security incidents to the Australian Government; and enhanced cyber security obligations on some systems of national significance. The *SOCI Act* also grants power to the Australian Government to direct the entities responsible for some critical infrastructure assets to do certain things or provide certain information.[6] The provisions of the SOCI regime apply to 'responsible entities', those with ultimate operational responsibility for a critical asset, and 'direct interest holders', those with an ownership interest in an asset of more than 10% or that are in a position to influence the control of the asset either directly or indirectly.[7]

Separate statutory rules impact the precise obligations that apply to asset owners and operators.[8] The *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023* require certain critical infrastructure asset owners or operators to prepare risk management programs to mitigate against harms that could arise in connection with their assets. These risk management plans must be developed by reference to specified Australian Standards and guidelines prepared by Government agencies including the Australian Signals Directorate and Australian Energy Market Operator.[9] Operators of declared 'Systems of National Significance' are also subject to enhanced cyber security obligations due to the interconnected, interdependent, and essential nature of those systems.[10]

How the SOCI regime applies to space technology

In recognising the space technology sector as critical infrastructure, the Australian Government sought to encourage better information exchange between industry and government, as well as to build a more comprehensive understanding of threats to national security, society and the economy. Unlike the other critical infrastructure sectors in the SOCI regime, the space technology sector is not comprehensively defined in detail in the *SOCI Act*. The definition is simply as follows: '***space technology sector*** means the sector of the Australian economy that involves the commercial provision of space-related services.' It then lists examples of space-related services: (a) position, navigation and timing services in relation to space objects; (b) space situational awareness services; (c) space weather monitoring and forecasting; (d) communications, tracking, telemetry and control in relation to space objects; (e) remote sensing earth observations from space; (f) facilitating access to space.[11]

In aligning the definition of the space technology sector with the *National Civil Space Priority Areas for Australia*,[12] the SOCI regime is able to accommodate the evolution and future direction of the Australian space technology sector. The *Explanatory Memorandum* accompanying the 2022 amendments made it clear that the space technology sector means 'the sector of the Australian economy that involves the commercial provision of space-related services' and 'reflects those assets and functions that are critical to maintaining the commercial supply and availability of space-related services in Australia.'[13] This includes 'assets, functions and components enabling operation of a space service or activity, including

provision of launch (comprising the assets themselves and the systems that give integrity to those assets)'.[14]

The examples provided in the definition of the space technology sector in the *SOCI Act* reflect Australia's role in the global space services industry. A regulation impact statement produced by the Department of Home Affairs noted that the *SOCI Act* was primarily concerned with ground stations and control centres as critical space technology.[15]

Australia has long been a major player in the global space services industry, with a rich history of involvement in projects as a ground service provider.[16] For example, Australia played an essential role in facilitating communications during the Apollo program, with the Parkes Observatory and Honeysuckle Creek Tracking Station acting as receiving stations.[17] Australia is host to a number of ground stations for satellite systems and science installations, including the Square Kilometre Array Pathfinder in remote Western Australia.[18] And with the recent commitment to Landsat Next, Australia will invest $207 million into expanding its existing ground infrastructure and world-leading data management expertise for Earth observation (EO).[19]

Currently, space communications assets are covered by the *SOCI Act* as critical telecommunications assets, whereas all non-communication space assets will only be covered as part of the broader space technology sector once it has been defined and is fully operational against the sector. The *Explanatory Memorandum* for the 2022 amendments to the *SOCI Act* states that, 'at this time critical space technology sector assets are communications assets and therefore covered under the proposed definition of critical telecommunications assets.'[20] Critical space technology assets such as telecommunications networks (signals and communications) and facilities (towers, equipment, and antennas) will be captured under the *SOCI Act* as 'critical telecommunications assets', and entities responsible for these assets will be captured as carriers or carriage service providers under the *Telecommunications Act*. Carriers and carriage service providers involved in transmitting or receiving radio communications and optical communications to and from space are covered in this way on the basis that these entities are 'best placed to manage the day-to-day operations of the asset and therefore ensure security and resilience of the asset in line with this regime'.[21]

Space technology assets should be defined and included in the security of critical infrastructure regime in a coordinated approach across whole of government and with input from industry and academia. The Department of Home Affairs should update its guidance materials on the SOCI regime to make it clear which space technology assets are already captured under other critical infrastructure sectors and asset classes. There should also be minimal overlap in asset classes between space technology assets and space assets that are included in other critical infrastructure sectors, including the telecommunications sector and the defence sector. While overlap in categorisation may arguably result in the need for certain space assets to be held to a high standard (i.e., the highest standard of any applicable regime), where space assets fall into multiple categories, there are risks of overburdening operators with compliance obligations, incentivising regulatory arbitrage, and disincentivising new participants from entering a sector that already has extremely high cost and technological barriers to entry.

Another key aspect of the 'space technology sector' definition is the focus on '**commercial** provision of space-related services' (emphasis added). This reflects the changing nature of the space sector, with private entities now taking a leading role in developing technologies to provide services from space with customers from the military, civil and private sector. The emphasis on 'commercial' suggests that there is no intention for government-owned assets used exclusively for government purposes to be captured. The definition of space technology could be stressed if an Australian government (federal, state or territory) ever sought to operate a space asset and sell or otherwise commercialise the services it provides. A similar position may arise if a space asset was being used for non-commercial purposes such as research activities undertaken by universities.

Defining the 'space technology sector' in this way risks narrowing the application of the *SOCI Act* with potential adverse consequences for Australia's national security and defence and the economy. The definition should be expanded to bring a broader range of actors and activities within the space technology sector definition. If the intention of the Australian Government was to expressly exclude the governmental space assets from the SOCI regime, such a position should be clearly expressed and justified. Exceptions for research should genuinely be considered given the risk of the SOCI framework acting as a barrier to such activities due to the high cost of compliance.

Another point of weakness is the focus on physical assets. While communications satellites and command and control facilities are essential to some critical infrastructure systems, the data that is derived from space systems can be just as important. For example, if a malicious actor were to interfere with the quality of data passed from an EO satellite to a ground station, this could have severe consequences for those reliant on the data itself. Such considerations appear well outside the bounds of the SOCI regime's current treatment of space technology.

Despite the inclusion of the space technology sector in the SOCI regime, it is not yet currently fully operational against the sector. For the full force of the SOCI regime to apply to a critical infrastructure sector, it needs to cover defined critical infrastructure assets. This leaves the regime as primed and ready, but currently inoperable with respect to the space technology sector. This does not mean that the SOCI regime does not currently apply to space assets at all. As noted, other critical infrastructure sectors can potentially involve space-assets or space-related systems, including the telecommunications sector and the defence industry sector.

To proactively prepare for the *SOCI Act* becoming fully operational against the space technology sector, space industry participants should strengthen their cyber security strategies and ensure the critical infrastructure systems that their technology feeds into are appropriately hardened. In addition, the Department of Industry, Science and Resources should develop an educational program outlining steps that space industry participants can take to comply with obligations under the *SOCI Act*. The Australian space technology sector will need to be ready to respond.

Notes

[1] Tristan Moss, Katheryn Robison Hasani and Aleks Deejay, *Looking Up from Down Under: Australian attitudes to national space activities*, Australian Centre for Space Governance, 8 December 2023, accessed 2 December 2024, https://doi.org/10.26190/unsworks/28684
[2] Explanatory Memorandum, *Security of Critical Infrastructure Bill 2017*.
[3] Department of Home Affairs, *Critical infrastructure Resilience Strategy*, Commonwealth of Australia, February 2023, accessed 2 December 2024, https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-resilience-strategy-2023.pdf
[4] *Security of Critical Infrastructure Act 2018* (Cth) s 3.
[5] Ibid s 8D.
[6] Ibid s 4.
[7] Ibid ss 6, 12L.
[8] See *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023*.
[9] *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023* reg 8(4).
[10] *Security of Critical Infrastructure Act 2018* (Cth) pt 2C, s 52B.
[11] *Security of Critical Infrastructure Act 2018* (Cth), div 2, s 5.
[12] Australian Space Agency, *Advancing Space: Australian Civil Space Strategy 2019-2028*, Commonwealth of Australia, May 2022, accessed 2 December 2024, https://www.industry.gov.au/publications/australian-civil-space-strategy-2019-2028, 12-13.
[13] Explanatory Memorandum, Security of Critical Infrastructure Bill 2017, 38-39, para 234.
[14] Ibid.
[15] Department of Home Affairs, *Critical Infrastructure, Systems of National Significance*, Regulatory Impact Statement, Commonwealth of Australia, Office Best Practice Regulation ID: 25902, 4.
[16] Joel Lisk, and Melissa de Zwart, 'Watch This Space: The Development of Commercial Space Law in Australia and New Zealand', *Federal Law Review*, 2019, 47(3), https://doi.org/10.1177/0067205X19856, 1-25.
[17] M L James, 'Into Space From Australia – the Early Days', Paper presented at the Fifth National Conference on Engineering Heritage, Perth, Australia, 3-5 December 1990, https://catalogue.nla.gov.au/catalog/424343, 55.
[18] CSIRO, *The ASKAP Radio Telescope*, 2016, accessed 2 December 2024, https://www.atnf.csiro.au/projects/askap/index.html; Leah MacLennan, 'Skynet satellite ground station opens in Adelaide to aid UK military communications', *ABC News* (online), 16 May 2016, accessed 2 December 2024, https://www.abc.net.au/news/2016-05-16/skynet-satellite-ground-station-opens-in-adelaide/7419042; Department of Industry, Innovation and Science, *2016 State of Space Report*, 1 March 2017, accessed 2 December 2024, https://www.space.gov.au/about-agency/publications/state-space-2016, 28, 42.
[19] Cassandra Steer, 'Australia just committed $207 million to a major satellite program. What is it, and why do we need it?', *The Conversation*, 27 March 2024, accessed 2 December 2024, https://theconversation.com/australia-just-committed-207-million-to-a-major-satellite-program-what-is-it-and-why-do-we-need-it-226621#:~:text=The%20commitment%20means%20we%20will,Landsat%20satellites%20–%20a%20major%20role.
[20] Explanatory Memorandum, *Security of Critical Infrastructure Bill 2017*, para 238.
[21] Ibid para 239.

Australian Centre for Space Governance

E contact@spacegovcentre.org
W www.spacegovcentre.org
linkedin.com/company/spacegovcentre

ACSG
AUSTRALIAN CENTRE FOR SPACE GOVERNANCE