2025 Australia Space Cyber Security Report: Challenges, Anticipated Readiness, and Future Directions

RMIT UNIVERSITY
Centre for Cyber Security Research and Innovation

The RMIT University Centre for Cyber Security Research and Innovation (CCSRI)

The CCSRI is a multidisciplinary research centre that draws researchers from across RMIT's schools and colleges to bring a multidisciplinary approach to the organisational, human, and technical aspects of cyber security.

The Strategic Policy Grants Program, Department of Defence

This research was supported by the Australian Government through a grant by the Department of Defence. The views expressed herein are those of the authors and are not necessarily those of the Australian Government or the Department of Defence.

Acknowledgements

This research has been produced as a result of the collaboration between the RMIT University Centre for Cyber Security Research and Innovation (CCSRI), Wise Law, and the Department of Defence. This research was supported by the Department of Defence as part of the Strategic Policy Grants Program. Special thanks to our research partners: EJ Wise and the RMIT staff involved – Professor Matthew Warren, Dr Shah Khalid Khan, Dr Adam Bartley, Professor Nirajan Shiwakoti, Dr Abebe Diro, and Dr Akanksha Saini, with contributions from Lee-ann Phillips and Amal Varghese, and Professor Aiden Warren. A special thank you to Space ISAC Australia Global Hub for facilitating workshops, and a big thank you to all workshop participants for sharing their time, expertise and imagination to ensure Australia is well placed to meet the evolving challenges of Space Cyber Security.

Disclaimer: RMIT University has undertaken this research activity based on unclassified material. No classified material, discussions or activities have been referenced or consulted in the production of this report.

Acknowledgement of Country

RMIT University acknowledges the people of the Woi wurrung and Boon wurrung language groups of the eastern Kulin Nations on whose unceded lands we conduct the business of the University. RMIT University respectfully acknowledge their Ancestors and Elders, past and present. RMIT also acknowledges the Traditional Custodians and their Ancestors of the lands and waters across Australia where we conduct our business.

Acronyms and Abbreviations

ACMA	Australian Communications and Media Authority
ACSC	Australian Cyber Security Centre
ACSS	2023-2030 Australian Cyber Security Strategy
ADF	Australian Defence Force
AI	Artificial Intelligence
APESA	Association of Professional Engineers and Scientists, Australia
API	Application Programming Interface
APT	Advanced Persistent Threats
ASA	Australian Space Agency
ASD	Australia Signals Directorate
BIS	Bundesamt für Sicherheit in der Informationstechnik (Germany)
CAF	Cyber Assessment Framework
CCSPA	Critical Cyber Systems Protection Act
CISA	Cybersecurity and Infrastructure Security Agency (USA)
CISC	Critical Infrastructure Security Centre
CISO	Chief Information Security Officer
CNES	Centre National D'Études Spatiales (France)
COTS	Commercial Off The Shelf
CSF	NIST Cybersecurity Framework 2.0
CSS	Cyber Security Strategy
CVE	Common Vulnerabilities and Exposures
DoD	Department of Defence (Australia)
DoS	Denial of Service
ENISA	European Union Agency for Cybersecurity
GEO	Geostationary Earth Orbit
GPS	Global Positioning System
GNSS	Global Navigation Satellite System
IoT	Internet of Things
ISAC	Information Sharing and Analysis Center
ISM	Information Security Manual
ISR	Intelligence, Surveillance, and Reconnaissance
ITAR	International Traffic in Arms Regulations
JCDC	Joint Cyber Defense Collaborative
LEO	Low Earth Orbit
MEO	Medium Earth Orbit
NCSC	National Cyber Security Centre (UK)
NIST	National Institute of Standards and Technology (USA)
PNT	Positioning, Navigation, and Timing
PSPF	Protective Security Policy Framework
SCM	Supply Chain Management
SCS	Space Cyber Security
SDA	Space Domain Awareness
SDR	Software-Defined Radio
SLA	Service Level Agreement
SOCI Act	Security of Critical Infrastructure Act 2018 (Cth)
TISN	Trusted Information Sharing Network
TT&CS	Telemetry, Tracking, and Command System

Definitions

Confidentiality	A foundation of information security. A system whereby the information is protected from unauthorised access, disclosure, or viewing.
Cyber incident under SOCI Act 2018	A cyber security incident is an act, event or circumstance where a critical infrastructure asset is involved, and it involves unauthorised impairment of electronic communication to or from a computer.
Cyber resilience	"The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources" (NIST n.d.).
DoS	Denial of Service attack to disrupt a network or systems by overwhelming it with traffic.
Dual-use systems	Technologies used for both civilian and military purposes either simultaneously or alternately, such as communication, navigation, and observation.
Firmware	A control software or hardware device.
Free riding attacks	Where a malicious actor crafts a local model update without using training data to trick a system in return for rewards. This can degrade the accuracy of the model.
Grey-zone threats	Non-traditional threats with unclear attribution and high deniability. Activities that are below the threshold of conflict, but that move strategic interests forward at the expense of others.
Integrity	A foundation of cyber security. Refers to the accuracy and reliability of data.
Malware	Malicious software designed to exploit programmable devices, data, or networks, to disrupt systems, steal information, gain access, or demand ransom.
Network segmentation	The isolation of a larger network into smaller segments to limit impact of security breaches.
Penetration testing	Simulated attack on a system or network to identify vulnerabilities.
Person in the middle	The secret interception of communication, and potential altercation, between two parties directly communicating with one another. Also known as a "man-in-the-middle" attack.
Principle of least privilege	Dictates that the minimum necessary rights be granted to users, applications, and processes only when necessary to perform designated tasks.
Reliability	A foundation of cyber security. Refers to the consistent and dependable performance of the network.
Satellite cyber resilience	The recurring ability of a satellite system, including all sub-components and supporting functions, to anticipate, survive, sustain, recover from, and adapt to high-impact low frequency cyber events.
Security-by-design	A security-focused approach to design, development, and deployment of digital products and services with fewer vulnerabilities and with consumer privacy and data safety in mind.
Sensor attacks	The manipulation of information gathered by sensors.
SOCI Act	Refers to *Security of Critical Infrastructure Act 2018* (Cth) that outlines laws and regulation for the protection of 11 critical infrastructure sectors, including the space sector.
Space Cyber Security	Space cyber security refers specifically to protecting networks, devices, and data associated with space systems from unauthorised access or criminal use. This includes special focus on encryption protocols, secure ground-based infrastructure, and resilience measures to mitigate the impact of cyber attacks and ensure confidentiality, integrity, and availability of information.
Space domain awareness	The ability to detect, track, and identify objects in space and predict threats, operational capabilities, and pathways.
Spoofing	Impersonation of a legitimate entity or individual by disguising the origin of communication or data for gaining access to sensitive information of systems.
Sybil	An attack on a system via the creation of multiple fake identities/accounts to appear as legitimate.
Tunnelling	The process of encapsulating data in another protocol to "tunnel" through a network to bypass security restrictions.
Wormhole attacks	A shortcut created through a wireless ad hoc network to disrupt network routing and communication.
Zero-day attack	Exploitation of a known vulnerability before the developer/vendor is aware.

Executive Summary

Space cyber attacks are rapidly becoming a major threat to national security and particularly space systems. As at May 2025, there are 14,240 satellites in orbit, of which 11,700 are still functioning, and this number is expected to increase exponentially in the future (European Space Agency 2025a).

As a result, we can expect the number of attacks from criminal elements and state-based actors that can exploit vulnerabilities in space-based systems will expand dramatically. Reports by government organisations and private sector actors reveal an expansion of malware trends, insider threats, Advanced Persistent Threats (APT), and other cyber threats, is occurring against space-based systems. Moreover, space-based systems interact increasingly with new technologies such as Machine Learning, Artificial Intelligence (AI), and Internet of Things, particularly using third-party solutions, which introduce additional vulnerabilities of space-based systems (SmartSat CRC 2022).

State-sponsored actors have recently increased their activities against space assets. They are increasingly targeting networks in critical infrastructure areas, often attempting to steal government secrets, disrupt activities, and hold private and government organisations to ransom. In the United States, leading military and scientific figures in the space industry have called for a rethinking of how nations need to defend satellite infrastructure, as well as keep pace with "on-orbit weaponry" being developed by adversaries and the threat vectors that are increasing (Dinner 2025).

Australia's space ecosystem is growing in sophistication and ambition. Its importance is reflected by its inclusion as one of Australia's critical infrastructure sectors, as highlighted by the SOCI Act 2018, and is now one of five warfighting domains within the Australian Defence Force. Despite a relatively small-scale industry, Australia excels at, among other capabilities, ground systems operations, nanosatellites, high performance optics, radio communications systems, and on-board data handling. Government policy and strategy development has encouraged investment in the Australian space sector, with strategic objectives focused on positioning, navigation, and timing; Earth observation; communication technologies; space situational awareness; research and development; robotics; and access to space.

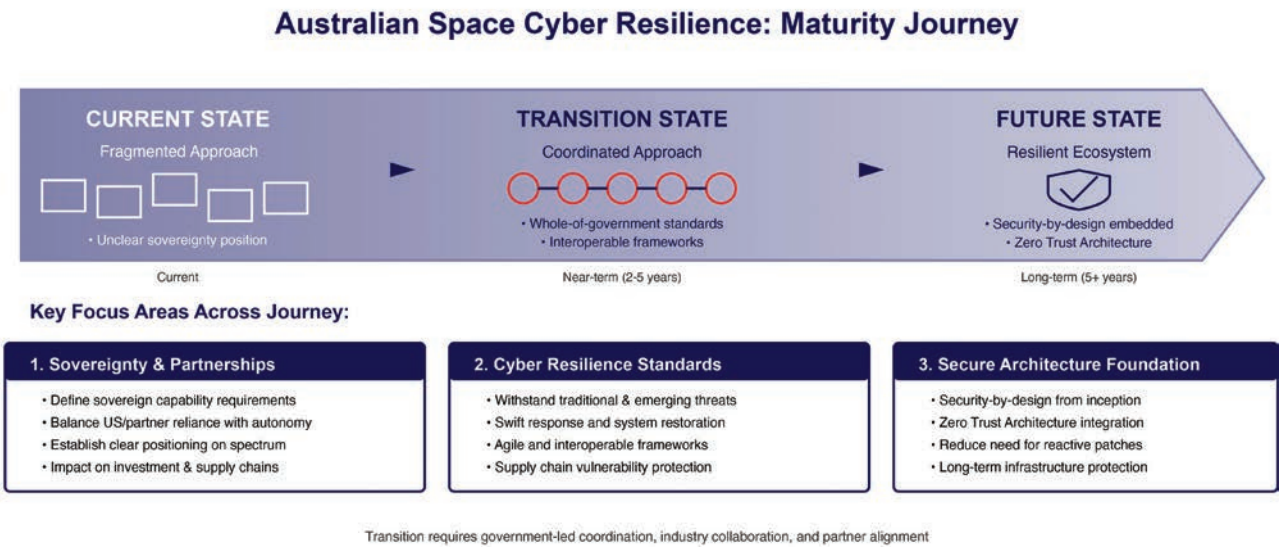
Unmistakably, space has become an enabler for whole of society goods and services for both civilian and defence purposes. From space situational awareness services, space weather monitoring and forecasting, to communications, tracking, telemetry and control in relation to space objects, reliance on space-based infrastructure (inclusive of satellites, supply chains, software) has increased national exposure to new vulnerabilities. This is significant for understanding current roadblocks in the development of a more resilient national space sector. Within Australia there is a narrow education and training base for the Australian space sector; space practitioners are in short supply, especially in cyber security, leaving the sector and the country ill-equipped to take advantage of commercial and non-commercial opportunities. It has also led to a situation where the sector is overly reliant on international partnerships and a global workforce (for whom there is great competition).

Australia's Defence Force began its reliance on space enabled assets, such as satellites, as early as 1981, when it installed its first satellite communications on Royal Australian Navy ships; later that decade, in 1988, Australia began its first trial of the Global Positioning System (Moss 2023). Looking ahead, space-enabled precision strike missiles, autonomous tactical vehicles, and other acquisition priorities underscore a future core space defence dependency. The Department of Defence, additionally, has joined global partners in contributing space situational awareness and has strengthened space-enabled intelligence, surveillance and reconnaissance capabilities. These activities and priorities showcase a necessary strengthening of space capabilities and underscore a capability imperative for a modern warfighting domain. However, funding estimates and strategic acquisitions guidelines currently fail to connect burgeoning dependencies with increasing vulnerabilities. Crisis scenarios showcase that dual-use providers, on which Australian defence is reliant, cannot guarantee services in Australia's national interest if services are disrupted, damaged, or delayed. Clearly, a national discussion about creating a space sovereign capability is required.

Currently, the position of where space systems and assets stand on a spectrum between reliance on the US (and other partners) and sovereignty is unclear in national documents and discussions. Additional understanding about what sovereign capability means for Australian purposes is also necessary. This will have implications for broader civilian and defence space industries, including investment, supply chain management, international framework interoperability, and partnership development. A further consideration for defence space resilience is the cyber protection systems, standards, and training. This means having the ability to withstand traditional and emerging cyber challenges, responding swiftly and methodically, restoring systems and capabilities with minimal disruption, and learning from others to prepare for future experiences.

Meanwhile, the adoption of a broader space cyber resilience posture requires a whole-of-government approach to standards development. The fragmented regulatory framework that currently exists needs to be improved. If Australia is to compete among global actors for space business and technology, including for future-proofing Australian military operations and fleets, a government-led security-by-design approach is necessary. This is necessary to safeguard supply chains from vulnerabilities, particularly at second and third tier levels. Additionally, standards will need to be both agile and interoperable with Australia's key space partners. This means they should be tailored to the Australian model, as well as speak the same language as our partners.

Lastly, in Australia the embedding of secure-by-design and Zero Trust Architecture must be incorporated into processes of space security from their inception. This thinking has been shown to greatly improve the overall resilience of space systems, decrease the need for reactive software patches, and enhance long-term protection of space infrastructure.



Recommendations

Key recommendations include:

1

Develop an Australian sovereign space capability to support Australian military and commercial needs.

A
Conduct risk assessments of dual-use space dependencies. Modern military operations, mobilisation, and intelligence activities require increasing dependencies on dual-use space systems that place too much control on partners and commercial entities to act in Australia's interests. The Australian Government must conduct risk assessments of these dependencies, especially in regard to critical infrastructure and their connection with military systems. This may necessitate expanding export controls to all space related critical technologies.

B
Formally designate critical infrastructure assets in the space technology sector as "critical infrastructure."

i. Noting initiatives such as development of an Australian Earth observation satellite capability, identify critical infrastructure assets in the Space Technology Sector such as coverage of all types of satellites.

ii. Enable the Horizon 2 framework of the ACSS to list and therefore prescribe space sector assets with obligations under the SOCI Act.

iii. Ensure all commercial satellite providers servicing the Australian Government or defence clients implement robust cyber security measures such as data segregation and appropriate encryption.

iv. Establish a formal certification program for commercial satellite providers, assessing their cyber security capability and maturity, including their secure data isolation capabilities.

C
Develop redundancy and substitution to compensate for compromised assets, such as key satellites. Anti-satellite capabilities and other threats are progressing, and Australia may find itself in a scenario where its satellites are targeted. The Australian Government, with commercial input, must begin gaming these scenarios to understand where redundant systems are best placed.

i. Establish contingency plans that include short-term fixes and long-term recovery strategies to address catastrophic failures.

D
There needs to be a **formal threat sharing mechanism** for the space community. This may be an expansion of the existing ASD CTIS (Cyber Threat Intelligence Sharing) to include space domain threat intelligence, or Australia joining a dedicated international space threat intelligence organisation such as the Space ISAC (Space Information Sharing and Analysis Center). This may include information sharing between the Computer Emergency Response Team Australia (CERT Australia) and Australia's partners overseas.

i. For critical infrastructure providers, the Trusted Information Sharing Network (TISN) has been set up for the exchange of information; there is a group for the space sector, and this could also act as a method of sharing threat intelligence in (near) real-time between TISN members.

"Develop redundancy and substitution to compensate for compromised assets, such as key satellites."

2

Promote and expand job opportunities in the Australian space industry and cyber security with a program to connect both.

A
Establish a public outreach program to build more understanding about space cyber security programs, jobs, capabilities, and pathways.

i. Incentivise universities, researchers, and industry to establish a student-industry contact as a criterion for future project funding.

B
Work with universities to develop space-specific undergraduate and postgraduate degrees, underscoring space as a career choice. Non-government organisations like Engineers Australia and the Australian Computer Society, can also play a role through guidance on curricula, standards, skills assessment, and other professional development. This includes investing in specialised training programs for space cyber security.

C
Develop a program with selected universities for space cyber security skills, distinct from standard cyber security or cyber focused courses.

i. Incentivise space industry internship programs with space sector SMEs and space agencies.

D
Broaden the TAFE sector to include space focused skills and trades including space and cyber security. These courses can be integrated with the commercial sector, providing a channel for new people and minds to enter the industry.

E
Expand the AusCheck scheme to include the space sector to ensure background checking services for all security-sensitive critical infrastructure sectors in Australia.

F
As part of the 2023-2030 Australian Cyber Security Strategy, a key action is to **build a framework for the professionalisation of the Australian cyber workforce** to provide employers and businesses with the assurance that the cyber workforce is appropriately skilled, and that workers qualifications and relevant experience are recognised and fit-for-purpose. This framework needs to include the space sector to ensure that the unique cyber and non-cyber skills (e.g. system engineering) are included.

3

All Australian commercial space infrastructure should be considered dual sector and appropriate standards/ definitions understanding need to be developed.

A
Adopt a dual sector understanding for policies and regulatory features to mediate between commercial sector interests and national security interests. Workshop scenarios revealed that potential conflicts in dual-use system priorities may arise. Australia's regulatory framework for space and cyber space systems must account for eventualities where dual-use systems operators may not adhere to national security protocols when these come into conflict with other services they provide.

4

Strengthen Australia's space and cyber supply chain security.

A
Deepen protection for Australia's space critical infrastructure from emerging vulnerabilities in space supply chains. The fastest and largest growing segment of space is in the downstream applications domain of supply chain, transportation, and mobility.

i. Assess Australian space supply chain management (military and civilian) to determine resilience, potential vulnerabilities, and points of weakness.

5

Develop a resilience action plan for Australian space infrastructure.

A
Due to the importance of the space domain, **adopt a clear understanding of what should be considered "critical" in space infrastructure** including cyber components. Current public-facing strategic documents offer a strong start for building space resilience. A resilience action plan must also consider what sovereign capabilities are non-negotiable, and what supply chain vulnerabilities must be adjusted.

B
Clearly articulate principles of resilience to the wider space sector, and embed principles into standards frameworks for security, operation, and supply chains.

C
Customise preparations for space weather events, particularly the events occurring beyond Earth's atmosphere that impact our technology and the near-Earth space environment.

i. Incorporate space weather threats (e.g. coronal mass ejections) into existing all-hazards emergency planning, alongside bushfires, floods, and cyber attacks.

ii. Educate members of parliament and government decision-makers on the real-time, high-impact nature of space weather. This will enable the protocols for decision-making under rapid-response timelines for cross-sector collaboration or between government bodies.

D
Unify warning systems.

i. Clarify roles for Australian government bodies (e.g. Australian Cyber Security Centre (ACSC), ASD, Australian Space Agency) in issuing alerts to critical infrastructure operators relating to cyber security at times of national emergency.

6

Australia to develop comprehensive space-based cyber security standards.

A
Tailor space and space cyber standards to Australia's ecosystem. A sovereign capability development begins with a set of internationally recognised standards for all government space procurement. The options are:

i. Adopt international frameworks such as those offered by ISO and forthcoming IEEE.

ii. Tailored standards to be interoperable with frameworks based on key allies, e.g. USA, basing our standards on NASA, NIST cyber security standards.

iii. Australia to develop our own space cyber security standards and frameworks based upon our prior unique experiences, but also linking to international and ally frameworks.

B
Develop specific protocols for incident response, inclusive of defensive countermeasures, such as network segmentation and encryption (among others).

C
Harmonise the Cyber Security Protection Standards in the *Space (Launches & Returns) Act 2018*, potentially with the *SOCI Act 2018.*

i. Harmonisation of ASA guidance for cyber security standards for the regulated space activities under the *Space (L&R) Act 2018*. Additionally, consider alignment with the more detailed *SOCI Act 2018* approach.

ii. Update the SOCI Act to include space-based software systems and supply chains explicitly.

"Australia to develop tailored, internationally recognised, space-based cyber security standards."

7

Deepen relationships between the Australian military and Australian commercial space operations.

A
Establish key desktop cyber security exercises to build relationships and increase cooperation. The exercises will help improve incident response, and consideration should be given to expanding scenarios to include all management levels and different space segments.

B
Exercises should also include key strategic areas of positioning, navigation, and timing; Earth observation; communication technologies; space situational awareness; research and development; robotics; and, access to space. The Department of Home Affairs has begun this process, and key outcomes are forthcoming. However, a focus must be on including industry partners and expanding government and Defence stakeholders.

C
Exercises are also critical for developing responses to cyber disruptions. These should include testing standards and ensuring that frameworks are working. Other exercises should include crises scenario responses to build resilience in space systems, and across all segments.

8

Australia needs to be part of current and future space consortium and projects (e.g. to remove space debris), which will require international planning and coordination.

A
Join international platforms that advocate for space access, space management, and space regulation.

i. Support domestic research activities and work with international partners to shape standards and rules relating to cyber security for space-related activities and infrastructure through vehicles such as the Artemis Accords, AUKUS, and the UN Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace.

9

Enable Zero Trust Architecture (ZTA) and Secure-by-Design principles as a foundation for all Australian cyber space-based systems.

A
Implement the principles of the recent report by The Australian Signals Directorate (ASD) and Australian Cyber Security Centre (ACSC), "Foundations for modern defensible architecture," fortifying the use of ZTA and secure-by-design principles against current and emerging cyber threats.

"A resilience action plan must also consider what sovereign capabilities are non-negotiable, and what supply chain vulnerabilities must be adjusted."