SMARTSAT
COOPERATIVE RESEARCH CENTRE

TECHNICAL REPORT 11

Cybersecurity of Space Infrastructure: A Multidisciplinary Approach

TECHNICAL REPORT 11

Cybersecurity of Space Infrastructure: A Multidisciplinary Approach

FEBRUARY 2024

Copyright © SmartSat CRC Ltd, 2024

This book is copyright. Except as permitted under the Australian Copyright Act 1968 (Commonwealth) and subsequent amendments, no part of this publication may be reproduced, stored, or transmitted in any form or by any means, electronic or otherwise, without the specific written permission of the copyright owner.

This report should be cited as:
SmartSat 2024, Cybersecurity of Space Infrastructure: A Multidisciplinary Approach, SmartSat Technical Report 11, SmartSat, Adelaide, Australia.

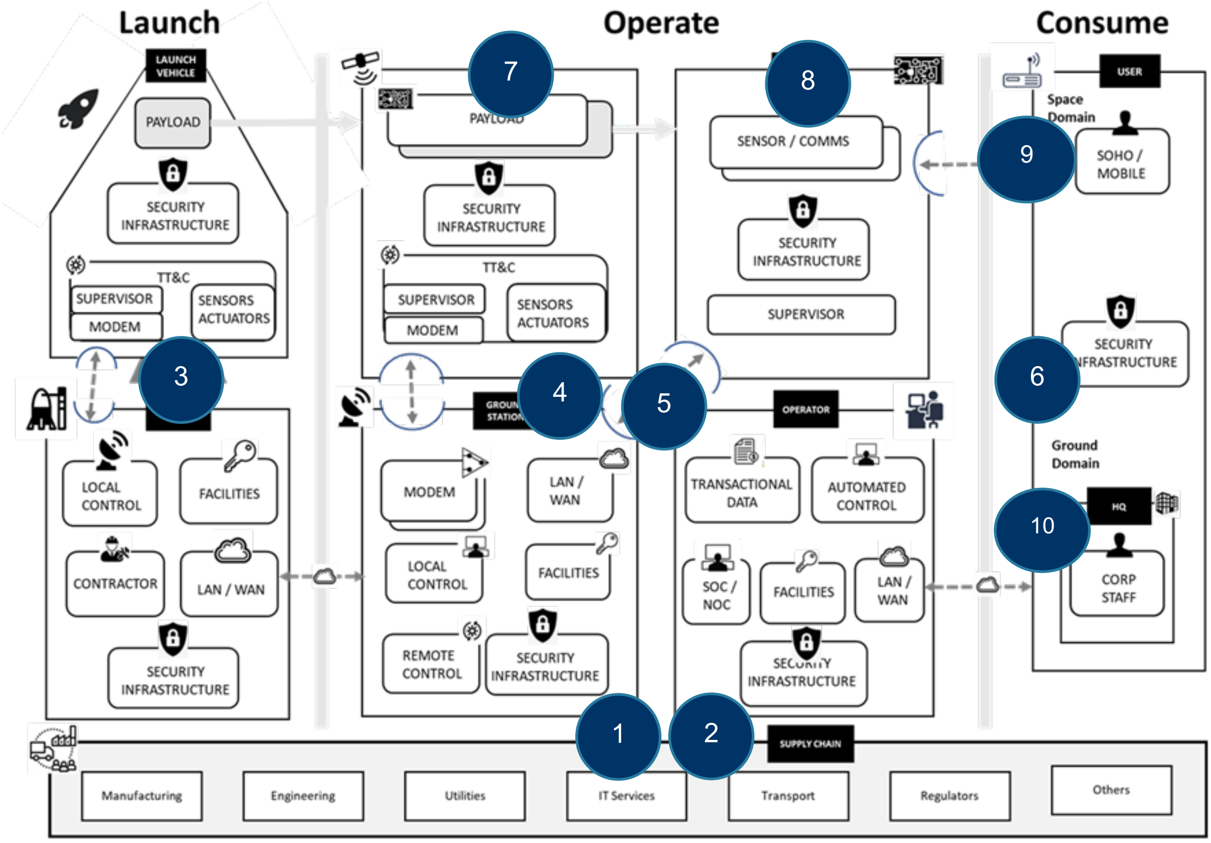
Disclaimer:
This publication is provided for the purpose of disseminating information relating to scientific and technical matters. Participating organisations of SmartSat do not accept liability for any loss and/or damage, including financial loss, resulting from the reliance upon any information, advice or recommendations contained in this publication. The contents of this publication should not necessarily be taken to represent the views of the participating organisations.

Acknowledgement:
SmartSat acknowledges the contribution made by Rodrigo Praino, Clémence Poirier, Vinicius Guedes G. de Oliveira, and Marco Aliberti (Flinders University) and Daniel Floreani (CyberOps) towards the writing and compilation of this technical report.

Executive Summary

The purpose of this project was to identify cyber threats that currently exist within the Australian space sector, shed light on the policy and legal protection available to operators of the space infrastructure in case of cyber incidents, and recommend a set of security controls falling within both the technical and policy dimensions. It did so by enhancing and exploiting a space cyber reference architecture developed by CyberOps[1] through the definition of 10 initial use cases of space cyber threats that exist in satellite missions, an overview of which is provided in Figure 1.

Figure 1: Use Cases Mapped in the Space Cyber Architecture Diagram



These use cases were then used to analyse the policy and legal tools that may apply in case of different types of attacks, conducted by different types of threat actors on different parts of the attack surface. The underlying purpose was to inform specialists about the policy and legal frameworks in which they operate when developing the controls to mitigate the threat vectors. Each use case provided in the report was created in order to highlight potential policy, legal, technical, governance, and behavioural gaps in the Australian space ecosystem. None of the use cases was meant to target or implicate a specific company or country; they simply consist of scenarios that provide an accurate representation of the applicable legal framework based on different threat actors, types of attacks, and consequences.

In this scoping study a variety of legal and policies instruments were found of possible relevance to the cybersecurity of Australia's space infrastructure, as summarised in Table 1 and Table 2.

[1] CyberOps. (2023). Australian Space Cyber Framework. https://www.cyberops.com.au/space-cyber-framework

TABLE 1: OVERVIEW OF GENERAL AND SPACE-SPECIFIC DOMESTIC AND INTERNATIONAL LEGAL TOOLS IN AUSTRALIA WITH DIRECT RELEVANCE TO CYBERSECURITY

Domestic	**General**	• Privacy Act 1988 • The Cybercrime legislation Amendment Act • The Radio Communications Act • Telecommunications and Other Legislation Amendment Act • Security Legislation Amendment (Critical Infrastructure Protection) Act 2021 • Telecommunications and Other Legislation Amendment (Assistance and Access) Act
	Space-Specific	• The Space (Launches and Returns) Act
International	**General**	• Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security • The Constitution and Convention of the International Telecommunication Union • The Council of Europe Convention on Cybercrime • International Humanitarian Law • United Nations Norms of Responsible State Behaviour in Cyberspace • Multiple United Nations Resolutions
	Space-Specific	• The Outer Space Treaty • The Rescue Agreement • The Liability Convention • The Registration Convention

TABLE 2:OVERVIEW OF RELEVANT CYBER-RELATED POLICIES IN AUSTRALIA

Strategic Frameworks	Australia's Cyber Security Strategy 2020
	International Cyber and Critical Technology Engagement Strategy
	2016 Defence White Papers and 2020 Defence Strategic Update
	2021 International Cyber and Critical Technology Engagement Strategy
	Digital Economy Strategy: A Leading Digital Economy and Society by 2030
	2020 Force Structure Plan (FSP20)
	Advancing Space – Australian Civil Space Strategy 2019-2028
	Defence Space Strategy
Implementation Frameworks	Information Security Manual
	Strategies to Mitigate Cyber Security Incidents
	2022 National Plan to Combat Cybercrime
	Risk Assessment Advisory for Critical Infrastructure Space Technology Sector
	Cyber Incidents Response Plan
	Ransomware Action Plan

The analysis shows that Australia's policy and legal framework is not devoid of measures that can be applicable to cyberattacks against space systems, and many efforts were conducted or launched as recently as 2022.

Indeed, it should be noted unlike certain countries like the U.S., which have implemented sector-specific cybersecurity regulations, Australia does not currently possess a specialized cybersecurity law specifically addressing space-related concerns.[2] Australia's approach is marked by fragmentation, with regulations dispersed across various regulatory mechanisms,[3] exemplified by the fact that several Australian legislations can be applied in the case of a cyberattack against an Australian space system (e.g., the Security Legislation Amendment Act, the Cybercrime Legislation Act, the Telecommunication Act, etc).

Additionally, the recognition of space as a critical infrastructure enables better protection and response to space cyber incidents. The reform extends obligations of the Security of Critical Infrastructure Act (2018) to various participants in the space supply chain including 'responsible entities', 'reporting entities', 'direct interest holders', 'managed service providers' and 'operators.' However, many uncertainties remain regarding the concrete positive obligations that the Act entails. Despite the apparent simplicity, assessing the extant applicability to the space infrastructure remains challenging. In addition, the very definition of the space technology sector as *'the sector of the Australian economy that involves the commercial provision of space-related services'* remains rather vague and subject to different legal interpretations.

At the policy level, while Australia does not have a space cybersecurity strategy, cyber threats are acknowledged in the newly released Space Defence Strategy and both space and cyberspace are recognized as warfighting domains by the Department of Defence (DoD). Nonetheless, certain strategic documents have a generalist approach (e.g., Defence White Papers 2016), while others concentrate on either the cyber domain or the space sector. The documents centred on space acknowledge cyberattacks as a threat to Australia's space infrastructure, but only briefly mention the topic without delving into specific strategies (e.g., Advancing Space – Australian Civil Space Strategy 2019-2028, and Defence Space Strategy). On the other hand, documents focused on cyber (e.g., Australia's Cyber Security Strategy 2020, and the 2022 National Plan to Combat Cybercrime) do not address space technology or its distinct characteristics; they typically provide generic guidelines for dealing with cyber threats in a non-specific environment.

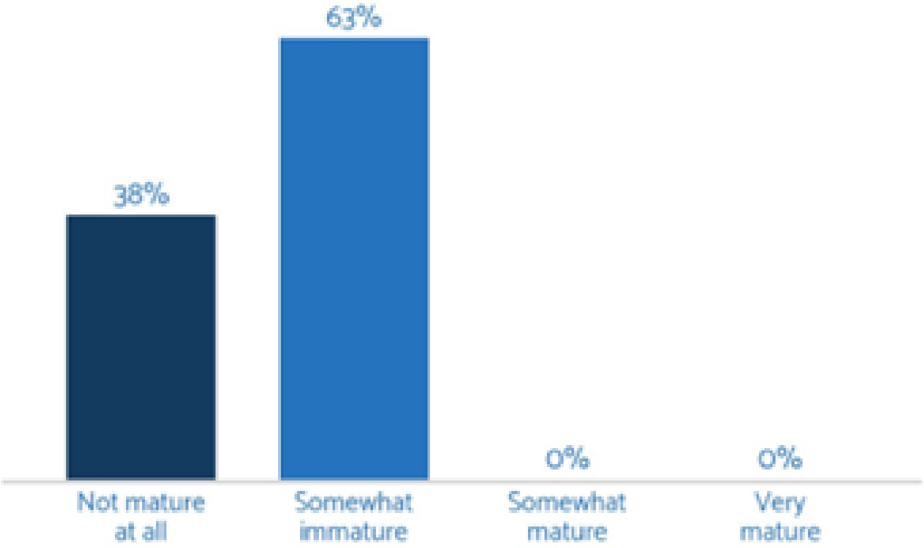
This general assessment was also confirmed by the result of a dedicated consultation workshop organised with Australian policy stakeholders and SmartSat partners. When benchmarking the maturity of the policy and legal framework against specific space cyber threats, several gaps come to the fore.

All consulted stakeholders considered that many gaps exist in Australia's policy and legal framework regarding space cybersecurity. 38% of consulted stakeholders perceived the Australian policy and legal framework regarding space cybersecurity as *not mature at all*, and 63% considered it as *somewhat mature*.

[2] Cybersecurity & Infrastructure Security Agency. (2023). *Cybersecurity Performance Goals: Sector-Specific Goals*. https://www.cisa.gov/news-events/news/cybersecurity-performance-goals-sector-specific-goals

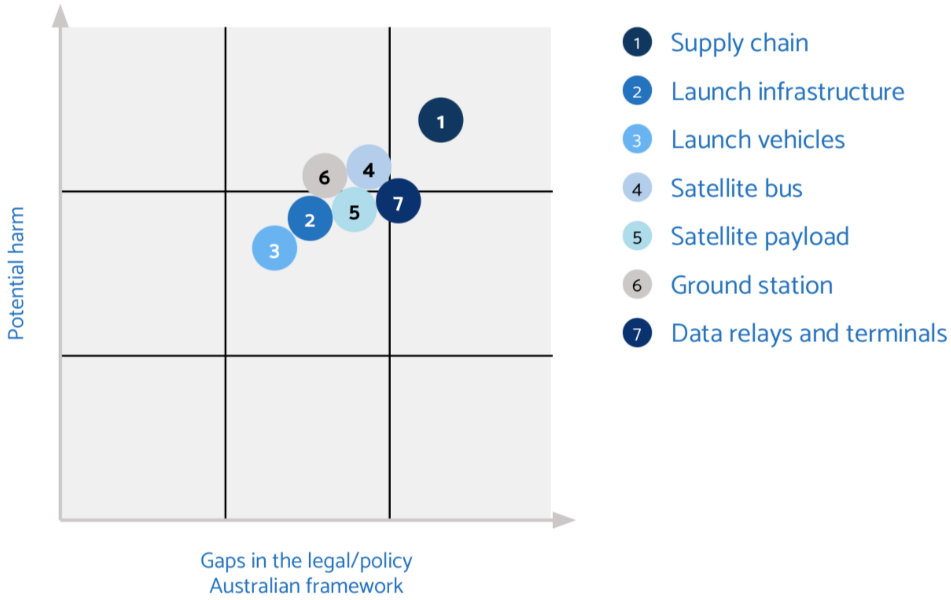
[3] Shah, R. (2023). *Getting regulation right – Approaches to improving Australia's cybersecurity*. ASPI.

Figure 2: Perception of the maturity of the policy and legal framework



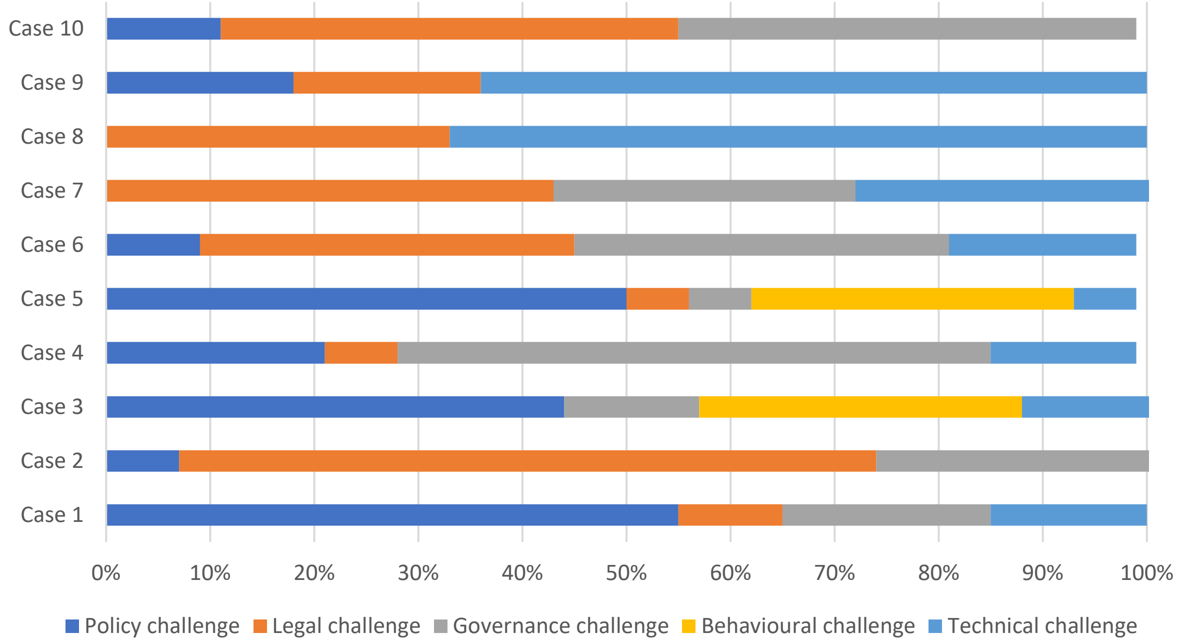
More specifically, consulted stakeholders ranked that the most immature laws and policies pertained to risks regarding the supply chain, data relays and terminals, and satellite buses; which are also the areas where Australia is more at risk. The higher the risk in Australia, the higher the gaps seem to be. This stresses the need to have better policies and awareness measures for supply chain issues in particular.

Figure 3: Assessment of Policy/Legal Gaps vs Potential Harm



Consultations with stakeholders, however, also revealed that the challenges are not only policy or legal in nature, but also behavioural, technical, as well as related to the overall governance of space cyber matters. The table below summarises the types of challenges that the Australian space infrastructure would be confronted with for each of the considered use cases.

Figure 4: Challenges to Case Studies Presented During the Workshop



All the considered cases present governance challenges, in addition to policy and legal ones. 70% of workshop participants considered that organisational aspects and responsibilities are somewhat unclear. This is rather normal as the Australian space program was recently restructured with the establishment of several agencies, as well as some adaptation in the Department of Defence to face new threats and grey zone operations.

As an example, depending on the nature of the intercepted information, different departments are empowered to act. The Telecommunication and Other Legislation Act 2017 provides power to the Secretary of Attorney-General’s Department when there is a breach of information that possesses national security value. Meanwhile, the Security of Critical Infrastructure Act 2018 empowers the Department of Home Affairs if a cyberattack has occurred, is occurring, or is deemed to be imminent and prejudices the social and economic stability or defence of Australia, as represented in Use Case 4.

This lack of clarity would require more interactions between governmental organisations and the industry as well as more awareness raising campaigns to ensure that operators are aware of who to contact and where to report incidents. Based on the policy and legal mapping, the gaps identified in the case studies, and discussions with Australian stakeholders in the course of two dedicated workshops, several recommendations have been outlined to improve the overall cybersecurity of the Australian space sector.

These recommendations have been segmented into three main typologies, as shown in Figure 5 below.

Figure 5: Main Recommendations for the Cybersecurity of the Australian Space Infrastructure

Security Measures Informing Awareness Raising Measures
Conduct awareness-raising campaigns for space cybersecurity
Release a space cybersecurity toolkit for the space industry
Provide space cybersecurity training for professionals and students
Create a recurring space cybersecurity event in Australia
Security Measures Informing Policy and Legal Measures
Update the Space Act of 2018 to integrate cybersecurity
Streamline incident reporting processes
Develop bilateral and multilateral agreements for managing cyberattacks on the space infrastructure
Adapt procurement practices
Security Measures Informing Operational and Implementation Measures
Have a clear information sharing and analysis centre or process for space cyber threats
Further understand the reliance on space applications and services
Further develop domestic space systems and ensure redundancy and substitution
Make cybersecurity tests compulsory before launching a satellite
Encourage the space industry to establish Bug Bounty Programs
Organise cyber exercises and war gaming scenarios to train space operators to better react to cyber incidents

Table of Contents

List of Figures

List of Tables

Introduction

1.1 Project Background and Rationale

Space systems are becoming closely intertwined with, and critical for, an increasing number of economic sectors. Be it remote sensing data used for weather forecast, satcom links for emergency services, or Global Navigation Satellite System (GNSS) signals employed in the energy, transportation, or financial sectors, advanced economies thrive and prosper on these technological advancements.

However, because of this increasing reliance, the strategic and socio-economic consequences of an even partial disruption of the availability or integrity of space data and signals could be dramatic. Any disruption would have the same effect of a power grid blackout, throwing back by decades the functioning of many associated services and economic activities, when not impeding them outrightly.

Awareness of the importance and critical dependence on space has raised the issue of the *safety* and *security* of space activities high in the priorities of decision-makers. Whereas the term safety refers to the set of '*measures precluding inherent malfunction and mitigating the risks of accidental damage that would be caused by or undergone by a space object, including its component parts*,'[4] security can be intended as '*the protection of a space object, including its component parts, against the risk of intentional actions undertaken by external or unauthorized actors*.'[5]

Beyond the many unintentional hazards created by e.g., the growing congestion of key orbits and debris as well as space weather events, space assets have also become potential targets of hostile actors. Comparable to other critical infrastructures, space systems can be strategic targets for a range of actors including governments, military and intelligence agencies, armed groups, terrorists, and individuals such as hackers.

For a variety of motivations, these organisations and individuals can seek to incapacitate, exploit, or take control of space assets with the objective of disrupting space-based services or accessing protected information. These threats are not limited to military space assets in the event of open conflicts and on theatres of operations. Although the threat may vary in intensity according to systems or geopolitical conditions, it remains ubiquitous and inclusive – menacing any system, anywhere, anytime.

Here, civil and military dimensions coexist with concerns over assets protection shared by governmental, military, and commercial stakeholders who may, however, perceive threats differently and pursue different objectives. The overarching objective to protect national space infrastructure remains, nevertheless, with governments as part of national security and defence strategies. From this standpoint, the integration of space infrastructures as assets of interest in defence and security strategies is not new, as space activities have always had strategic implications. However, as space-based capabilities gain in importance for the economy, society, and security, space infrastructure becomes an increasingly central component and its protection a growing concern. This has led to the development of doctrines, capabilities, and technologies around the concept of space control or counterspace, which encompasses both defensive (i.e., capacities to protect space assets) and offensive (i.e., capacities to strike space assets) dimensions with the ultimate objective to gain 'space superiority.'

[4] Zarkan Cesari, L. (2021). *What's in a Word? Notions of 'Security' and 'Safety' in the Space Context*. United Nations Institute for Disarmament Research.

[5] Ibid.

With specific respect to the development of offensive counterspace assets, Secure World Foundation's annual report on global counterspace capabilities highlights that 'the evidence shows significant research and development (R&D) of a broad range of kinetic (i.e., destructive) and non-kinetic counterspace capabilities in multiple countries.[6] Though only four countries have demonstrated kinetic ASAT capabilities in the past – the U.S.A., Russia, China, and India – technically less demanding forms of counterspace capabilities are considered to be available to more actors, including non-state actors.

Among those, particularly pervasive has become the development of cyber counterspace capabilities. Indeed, as space assets continue to move towards the integration of more advanced information technologies such as software-defined radios, all-digital components, on-board processing and machine learning, the entry points for cyberattacks are inevitably bound to increase. Similarly, the globalization of the space supply chain, the proliferation of small satellites using commercial off the shelf (COTS) components and the possibility to operate space mission payloads across networks through public internet connectivity substantially increase the vulnerability of space systems to cyberattacks.

Although cyber threats to space systems are not dissimilar to those faced by other systems relying on information and communication technology (ICT) to operate,[7] manufacturers and operators of space infrastructure have not yet reached the level of cyber resilience of their 'terrestrial' counterparts due to challenges in space operations and environments.[8] In Australia, these risks are exacerbated by the fact that the cybersecurity of space information systems is scantly addressed at the operational and policy levels. Despite the growing efforts of the Australian Cyber Security Centre (ACSC) within the Signal Directorate and the Attorney-General's Department, numerous technology and policy gaps remain, including those pertaining to the definition of roles and responsibilities of the different stakeholders in case of cyberattacks and those pertaining to policy guidance for R&D and procurement activities by public bodies.

This project will contribute to bridging these gaps by identifying cyber threats that exist within the Australian space market today, clarifying the policy and legal protection available to satellite operators in case of cyber incidents, and recommending a set of security controls falling within both the technical and policy dimensions.

1.2 Project Objectives and Approach

This project was designed to identify cyber threats that currently exist within the Australian space market, clarify the policy and legal protection available to satellite operators in case of cyber incidents, and recommend a set of security controls falling within both the technical and policy dimensions. The research hence was designed to cross-pollinate disciplinary boundaries to provide a holistic set of security controls for space missions, thus contributing to making Australia's space companies and public stakeholders at the forefront of the international space community in tackling the cybersecurity issues associated to space operations.

The project was structured in four phases, each corresponding to a specific sub-objective:

Identify threat vector use cases for space systems. In the first phase, the project developed a series of space cyber threats using the Space Cyber Reference Architecture developed as part of a prior Department of Defence (DoD) project By CyberOps. It identified representative threats that Australia's space missions can be subject to throughout their lifecycle, from the manufacturing of satellite systems to their exploitation,

[6] Weeden, B., & Samson , V. (2020). *Global Counterspace Capabilities: An Open Source Assessment*. Secure World Foundation.
[7] Froehlich, A. (2021). *Outer Space and Cyber Space: Similarities, Interrelations and Legal Perspectives (Vol. 33).* Springer International Publishing AG, pg. 62-63.
[8] Oakley, J. G. (2020). *Cybersecurity for Space: Protecting the Final Frontier*. Apress L. P.

passing through their launch and operations. The project team engaged with relevant SmartSat partners (e.g., Nova, Airbus, MDA, BAE, SAAB, DEWC, Sitael, Thales, Leonardo, Solinnov, EOS) to develop the specific cases. The exercise, in turn, enabled the identification and assessment of *vulnerabilities* of the different space systems as well as the identification and assessment of *risks* associated to the identified vulnerabilities. The use cases were chosen based on likelihood and to ensure good coverage in the next phase.

Enhance the threat analysis with an investigation of the policy and legal frameworks that surrounds threats vectors. The project thoroughly examined the applicable policy and legal frameworks to safeguard the security of space infrastructure from cyber menaces. Regarding the policy framework, particular attention was devoted to both strategic documents (e.g., Australia's Cyber Security Strategy 2020, Defence Strategic Update 2020, International Cyber Engagement Strategy) and policy implementation tools (e.g., Australian Government Information Security Manual, Cyber Incident Management Arrangements, Cyber Cooperation Program, etc.). The project likewise examined the extent roles and responsibilities of different stakeholders in response to different types of incidents affecting the cybersecurity of space infrastructure.

Regarding the legal framework, consideration was paid to the applicability of both domestic legislations (e.g., the Cybercrime Legislation Amendment Act of 2012, the Privacy Amendment Act of 2017, the Telecommunications and Other Legislation Amendment Act of 2017, etc.) and international legal regimes (e.g., the UN Charter, the Outer Space Treaty, ITU Convention, the Budapest Convention, etc.).

Identify technical shortcomings and define security controls informing operational countermeasures. Through analysis of use cases relevant to Australia's space activities and the newly defined policy landscape the project examined the specific techniques that can be enacted to counteract identified shortcomings at the operational level and maintain information assurance properties (data availability, integrity, authenticity, and confidentiality). The countermeasures identified are applicable by spacecraft operators to ensure ground-to-space data availability and authenticity or space-to-ground data integrity and confidentiality.

Identify policy and legal gaps and define security controls informing policy making. Through the definition and exploitation of the abovementioned use cases, the project aims offers a set of security controls to offset the identified gaps at the legal and policy level and enhance policy/legal protection available to Australian space operators. Identified policy actions pertain to the enactment of dedicated protocols for efficiently tackling space cyber threats, the definition of contractual requirements for the development and procurement of future Australian space information systems, as well as the development of contingency plans and crisis management scenarios.

This project was designed to be an initial study to guide a future program of study and work. This will eventually lead to the development of a definitive manual on the domain, and capability that can be offered as a commercial service to any Australian companies and SmartSat CRC members operating in the space sector (manufacturers, satellite and ground segment operators, downstream application service provides etc.) and, in the medium term, internationally. Results can also be used to reinforce cyber education programs or be converted into wargame simulations that DoD can use for training purposes.

It is envisioned that once utility has been demonstrated that the Australian Space Agency would be interested in further collaboration in the area of policy development.

1.3 Project Methodology

1.3.1 Process Overview

In terms of approach, the project began by defining 10 initial use cases of space cyber threats that exist in satellite missions. The definition of the use cases was informed by the Space Cyber Architecture (SCArch) developed by CyberOps to provide strategic and operational guidance and demonstrate where interdependencies exist between organisations with differing implementations of the same high-level goals (see Section 1.3.2 for a detailed overview of the SCArch).

Towards this, the project team organised both dedicated interviews and multilateral consultations in the form of two consultation workshops. The first workshop took place on 5 May 2022 while the second took place on 31 October 2022, supplemented by dedicated interviews. The workshops and consultations were held online, under Chatham House Rules, and were specifically intended to collect the space industry stakeholders' views on cyber threats currently confronting the Australian space sector.

The workshops and interviews were organised with the assistance of SmartSat Collaborative Research Centre, and developed with relevant SmartSat partners (e.g., Nova, Airbus, MDA, BAE, SAAB, DEWC, Sitael, Thales, Leonardo, Solinnov, EOS, Australia Space Agency, Australian Space Policy Institute).

In the first workshop, stakeholder engagement was deemed key to ensuring that the selection of the 10 initial use cases of space cyber threats that exist in satellite missions respond to actual threats faced by the Australian space industry, as well as to assess whether the various supply chain organisations were undertaking a journey towards cybersecurity maturity. This workshop focused on identifying the most likely cyber threats that could affect Australia's space missions, considering the entire lifecycle from the supply chain to the manufacturing, and assisting to define ten case studies that best represent such threats.

Pursuant the definition and refinement of the use cases, an investigation into the policy landscape that surrounds these vectors was carried out to inform specialists about the policy and legal frameworks they operate in when developing the controls to mitigate the threat vectors. As part of this exercise, the project team organised the second consultation workshop, which was supplemented by dedicated interviews.

The second workshop aimed to assess preparedness, gaps, and opportunities to enhance the cyber maturity of the Australian space sector and collect inputs on how to achieve a higher security level in the sector. During this workshop, the participants were confronted with the established 10 use cases and asked, among other questions, if they perceived the application of any policy, domestic or international, to it. Considerations included: Preparedness and resilience of Australia's space organisations, perceived gaps in the policy, legal and regulatory domain, and measure to enhance cyber maturity.

The identified threat vectors were then used to recommend a suite of security controls that can guide future decision-making by the government as well as activities by space operators. The project team incorporated feedback received by SmartSat, during the draft circulation stage into final report to SmartSat and other relevant stakeholders, including DoD.

1.3.2 Space Cyber Architecture[9]

Today, space industry organisations need a dedicated security model that effectively adapts to the complexity of the modern environment, embraces the mobile workforce, understands the dynamic nature of

[9] Section based on: CyberOps 2020 Space Cyber Architecture document.

business relationships in a growing ecosystem, and protects people, devices, applications, and data wherever they are located – on the ground or in space.

Towards this, CyberOps developed a Space Cyber Architecture (SCArch) specifically designed and tailored for use during product or services development by the nascent Australian Space ecosystem. Architectures are used to provide strategic and operational guidance, and to demonstrate where interdependencies exist between organisations with differing implementations of the same high-level goals.

The purpose of the SCArch is to achieve the following outcomes:

- Provide systems-wide guidance when developing an end-to-end cybersecurity view of a space mission or project.
- Provide a template for the interaction between different space industry verticals to ensure a seamless approach for a project or operation when multiple industries and contractors are involved.
- Provide tailored advice on security practises best suited to meet the projected demands of the space industry.
- Provide an architectural benchmark where project sponsors can compare different aspects of a common project or operation to identify anomalies.
- Highlight where differing products, services, roles, and responsibilities exist, where security controls, monitoring and governance should be established.
- Provide a reference for organisations when considering contracting with other parties or where internal support reliance exists.

The SCArch was developed as part of a Defence Innovation Hub project and is based on domestic and international reference architectures. The architecture is also segmented into the industry verticals that make up the space ecosystem. These verticals are described below.

Space Industry Verticals

To better understand the attack surface, it is important to understand space systems in the broad sense of the term. The space infrastructure can be mapped in various ways. Harrison et al. mapped the space infrastructure and related threats by distinguishing the ground segment, comprising the ground station, launchpad, simulators and emulators, the supply chain and personnel; and space platforms, comprising payload, radio link, computing, internal communications, and on-board sensors. [10] Wheeler et al. distinguished the attack surface by inputs, outputs, internal communications, and computing.[11] [12] Georgescu et al. consider the space infrastructure by differentiating between types of space systems, namely remote sensing, communications, meteorological, GNSS; and administrative and legislative frameworks.[13] Housen-Couriel distinguishes between stages of satellite operations, which include pre-launch; at launch; telemetry, tracking, and command (TT&C); transmissions; and end-of-life.[14]

[10] Harrison, T., & Johnson, K. (2020). *Space Threat Assessment 2020*. Center for Strategic and International Studies.
[11] Wheeler et al.
[12] Georgescu, A., et al. (2019). *Critical Space Infrastructures: Risk, Resilience and Complexity*. Springer.
[13] Ibid.
[14] Housen-Couriel, D. (2016). *Cybersecurity threats to satellite communications: Towards a typology of state actor responses*. Acta Astronautica 128. https://www.researchgate.net/publication/305729153_Cybersecurity_threats_to_satellite_communications_Towards_a_typology_of_state_actor_responses

For the purposes of this study, the following industry verticals have been chosen to represent the current Australian space ecosystem within the SCArch. These are defined as:

Supply Chain – an organisation or collective of organisations that provide parts, services, or advice to a company playing an active role in the space ecosystem. Supply chain organisations in the space sector may provide:

- Circuit boards, components, and ancillary items such as glues and shielding,
- Complete assembled systems such as satellite busses or processing payloads,
- Utility services to facilities (power, water, communications),
- Security services,
- Legal, cyber, commercial, regulatory, and technical advisory services.

Operators – organisations that operates satellites and provides services internally to their organisation or externally to a third-party. Operators typically:

- Operate a satellite bus via a TT&C link and operations centre,
- Operate a satellite payload,
- Operate and maintain an end-to-end service between customers and the provider.

1. **Launch Site** – An organisation that provides the facility for launch vehicles to ascend from. This may include facilitating the negotiation of local legal and environmental regulations. The launch site may provide the launch control systems or provide services to a third-party launch control system.

2. **Launch Vehicle** – An organisation that builds vehicles or combinations of vehicles (rockets, balloons, air breathers) that take satellites into space or near space.

3. **Launch Brokerage** – An organisation that brokers a launch service on behalf of the Operator.

4. **Ground Station** – An organisation that owns and operates one or more ground stations for the purpose of communicating with satellites in orbit. The ground station can be for control (TT&C), for payload communications or both.

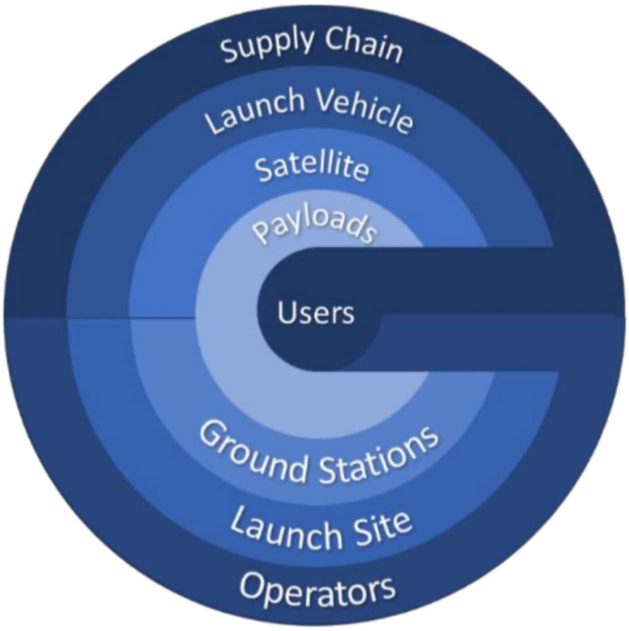
5. **Satellite** (bus/chassis) – An organisation that builds satellite busses or complete missions for their own use or provides them to external parties (operators). Satellites can be custom designed and constructed from a range of components or can be assembled from several pre-built sub-assemblies.

6. **Payload** (of satellite) – An organisation that designs, builds, or configures a payload that is destined to be flown inside a satellite bus. Payloads may be tightly integrated to consume a range of services such as power, shielding, data communications or orientation services from the bus.

7. **Users** – Satellite services can be offered direct to end users, or via third-party relationships. Users are not explicitly considered in this framework but are listed for consistency and to assist in highlighting considerations when using the space industry activity canvas.[15]

[15] CyberOps. (2023). *Australian Space Cyber Framework*. https://www.cyberops.com.au/space-cyber-framework

FIGURE 6: SPACE INDUSTRY VERTICALS (SOURCE: CYBEROPS)



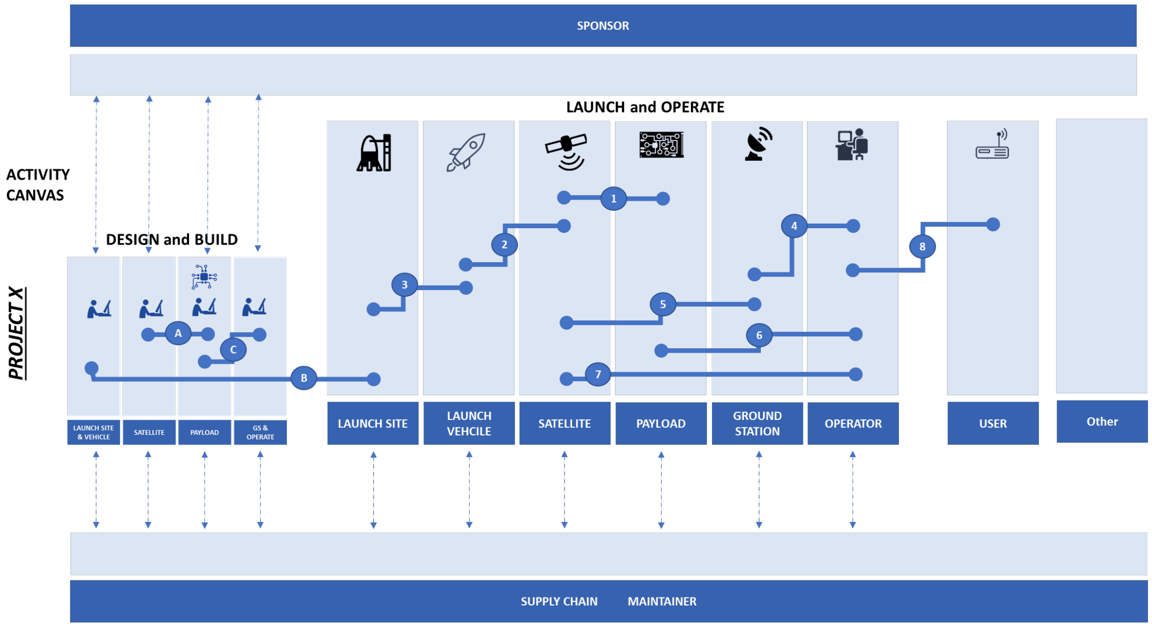
Space Activity Canvas

The space industry activity canvas was developed to provide users of the architecture with a better understanding of the interrelationships and dependencies between products and services required by individual projects or organisational capability. The example canvas shown below highlights the types of interactions between capability segments of the space ecosystem for a particular project or mission.

The canvas has also been used to drive a range of artefacts and views developed for the SCArch. More specifically, the interactions between separate organisations working on common projects or operations helps to drive the security architecture segmentation, policies, user and device identification methodology, end to end encryption models, and more. The activity canvas allows discussions on how these operate and are then captured in the architectural views presented in the SCArch later in this document.

For illustrative purposes of the use of activity canvas created by CyberOps, the diagram below describes the process involved in a representative design, building and operating stages of a satellite project.

Figure 7: Space Activities Canvas (source: CyberOps)



Design and Build Phase

1. The payload designers and satellite bus designers share contractual, regulatory requirements and Interface Control Documents (ICD) to ensure a functional and compliant system.

2. Launch vehicle, launch brokers, and launch site providers establish agreements on the specifications of the launch vehicle and the constraints of the launch site. This includes ensuring the launch control system is tested and operational.

3. The satellite payload designers share contractual, regulatory, and ICDs with satellite operators and in-house or third-party ground station providers to ensure a functional and profitable system is developed and deployed.

Launch and Operate Phase

1. The payload is transported to the satellite bus facility to be integrated into the satellite for the final test and build phase. This may include dry and wet builds and associated testing of the satellite.

2. The combined payload and satellite unit is transported to the launch vehicle for integration and testing phases, and inserted into its payload carrying and release mechanisms.

3. The launch vehicle is transported to the launch site for final tests. Launch procedures are then carried out.

4. Once in orbit, the satellites are released, and contact is attempted by the operator (in this case) via one or more ground stations.

5. Once the satellite is controllable, the ground stations can then establish reliable communications with the satellite.

6. The operators can establish communications with the payload.

7. The operators can control and maintain the satellites orbital characteristics.

8. At this stage, the operators can provide a service to the end customers.

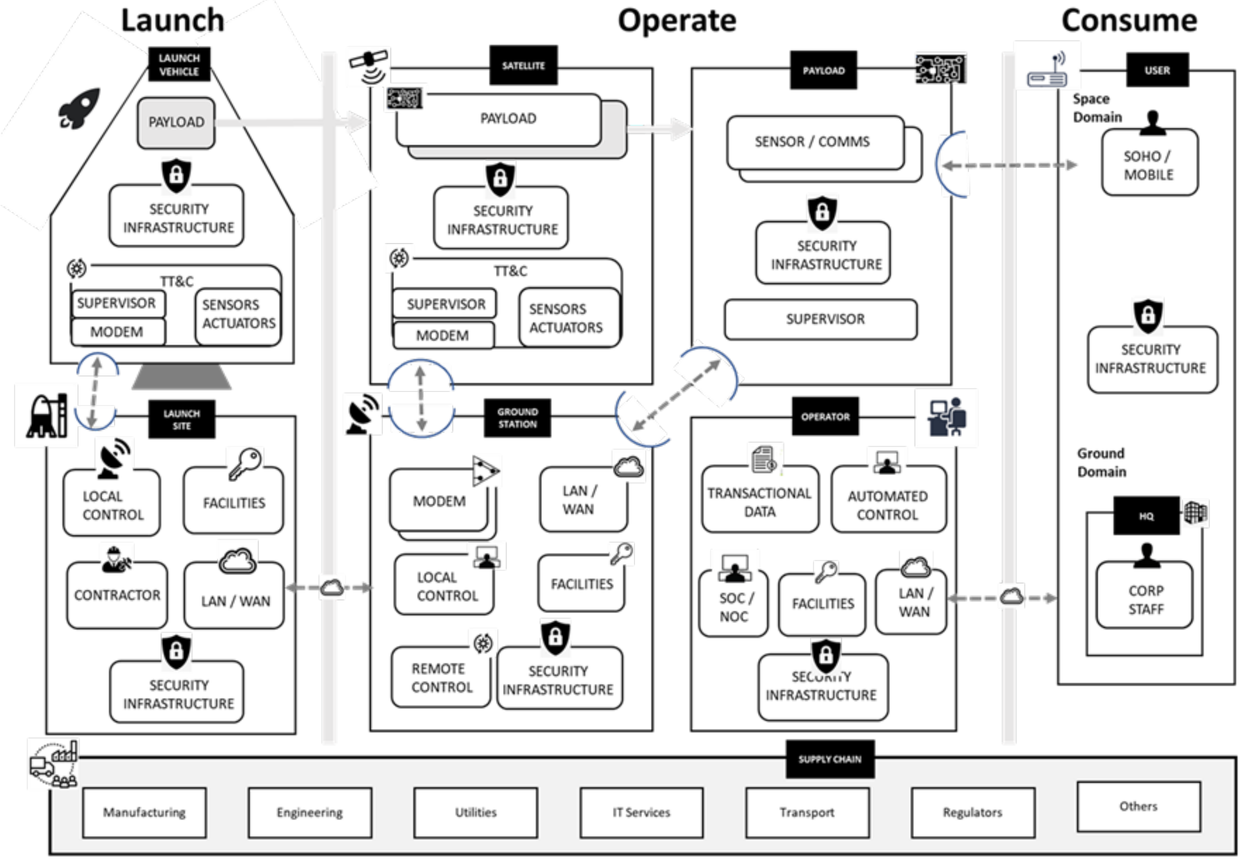
Throughout all stages in the above activity description, a range of organisations are involved in the supply chain. There are likely multiple checks and balances where a project sponsor, product owner, stakeholders or interested parties may be involved in the overall process.

Combined Segmentation View

The space industry activity canvas, described above, provides a mechanism to map relationships between different organisations when they come together for a mission or as part of a single operation.

The combined segmentation view allows security planners to see how segments within the operational security domains of different organisations are related when providing services for a common goal. In many cases it is not necessary for an individual organisation to share all their internal operational security planning or their enterprise security plans to outside groups, however just the relevant operational information is essential to be shared to build trust and provide project owners or mission/operation planners the information they require to ensure a safe cyber environment. Trust in this context is trust in peer organisations, trust in their assessment of the SCArch conditions and controls (identity, assets, applications etc) so that interoperability is possible with peer policy enforcement points.

FIGURE 8: SPACE CYBER ARCHITECTURE DIAGRAM (SOURCE: CYBEROPS)



The diagram is broken into three high level activities:

- Launch – the elements that come together to launch a payload into space.
- Operate – the elements that come together to provide for a project or to operate an ongoing service.
- Consume – the elements that interact when users are consuming space services.

The architecture is structured so that an organisation can take the section associated with their industry vertical and apply the guidance as appropriate. Importantly, they can also look at the relationships between their vertical and neighbouring verticals with which they interact to ensure there are no coverage gaps between organisations.

The architecture encourages industries to not only look at their cybersecurity in isolation, but also in cooperation with their peers with whom they function as a wider team in either their launch, operate or consume functions. Note that some organisations operate in multiple industry sectors and thus need to incorporate (or combine) more security domains from different parts of this architecture. Cybersecurity is not just technology, it is people, process, and technology, so space industry staff are encouraged to use this architecture to initiate discussions amongst their security teams and when passing security requirements and matching contracts to their supply chains.

1.4 Utilisation and Impact

This is a scoping project intended to inform potential future activity and utilisation by a wide range of users. Space Policy is a large topic of activity within the global space community (see Woomera Manual). Cyber Policy is also a well worked Policy area (see Tallinn Manual). What is missing is the combination of the two. Space Cyber policy is a unique combination of the above plus the intersection of telecommunications and signals intercept regulatory environments. Organisations seeking to provide product and services in the Space environment should understand the policy environment they are operating in from a Space/Cyber perspective.

This is a seed project that could lead to a manual similar to the two mentioned above which will have impact on communities in Australia and around the globe. The capability developed as part of this project will lead to the ability to offer services in the area of Space Cyber Policy for future space missions. It will also be of great value to organisations when carrying out risk assessments of their projects in the early design stage and as part of their ongoing risk management efforts.

The outcomes of this project can be of utility to any space sector company in order to enhance its awareness about the policy and legal ecosystem they operate within and hence its preparedness to cyberattacks. In fact, the output of this project can be offered as a specialised commercial service to companies operating in the space sector, including manufacturers, satellite and ground segment operators, and downstream application service providers to raise their preparedness by enhancing the hardness of their infrastructure and improving their awareness about the policy and legal framework they operate in.

On a broader level, the project outcomes will also inform policymaking, reinforce cyber education programs, and can be utilised by DoD and policy teams within the Australian Space Agency (ASA). Findings of the project can be used to inform policymaking regarding the implementation of operational incident management protocols, the set of strategic response options that are available, and prevention measures that can be put in place in the frame of e.g., public procurement of space assets. For instance, outputs of the project can be used to feed the definition of a baseline cybersecurity requirements list for public purchases and subcontracting activities.

Overall, this research cross-pollinates disciplinary boundaries, providing a holistic set of security controls for space missions, thus positioning Australia's space companies and public stakeholders at the forefront of the international space community in tackling the cybersecurity issues associated to space operations.

Threat Vectors to Australia's Space Systems

2.1 Overview of Cyber Threats to the Space Infrastructure.

In the last few decades, space systems have gone from analogue to digital systems, thereby increasing the surface of attack, lowering the barrier of entry for attackers, and making satellites and satellite services new cyber targets. Indeed, satellites are increasingly equipped with reprogrammable software, on-board computers, and connected through TCP/IP protocols.[16] They can simply be defined as computers in space, which are controlled by other computers on Earth.[17] This trend is rising with inter-satellite links, on-board data processing software, cloud ground stations and other space-based data services. As any connected object, this makes them increasingly vulnerable to cyberattacks.

Cyber threats against the space infrastructure may constitute a paradigm shift for the strategic stability that was maintained during the Cold War development of nuclear ballistic missiles. According to Ivan Martinovic and James Pavur, strategic stability in space used to be partly enabled by a limited number of actors and a limited access to space and cyber technologies; a relatively easy attribution of kinetic attacks by all actors, which rendered plausible deniability and stealth impossible; and the potential creation of debris in case of a kinetic attack on a satellite, which would affect all spacefaring nations, including the attacker.

However, today, the widespread and relatively cheap accessibility to cyber offensive technologies lowers the barrier of entry and enables all actors, including non-space and non-state actors, to conduct cyberattacks on satellites. In addition, cyberattacks are difficult to detect and attribute. Unlike kinetic attacks where radars of any country can monitor the space environment and attribute ASAT attacks, cyberattacks are difficult to attribute, increasing plausible deniability and decreasing deterrence. It is about finding evidence of the attack and its origin through detecting IP addresses, digital signatures, logins, or even the attack patterns, programming languages, alphabet. When it is possible, it is even more difficult to demonstrate who the attackers are working for, when nation-states are sub-contracting these activities to hacker groups, including in third countries. Finally, cyberattacks on space systems do not necessarily create debris and can be reversible, which do not deter attackers and contribute to instability in space as there is no longer an *'environmental interdependence'*.[18] These aspects are not conducive to responsible behaviour in either cyberspace or outer space. Plotnek and Slay further outlined that cyber threats provide malicious actors with the widest range of options in attack vectors and on the attack surface as well as outcomes compared to other space threats, thereby making space cyber threats a very flexible options for attackers.[19]

However, it is critical to underline that cyber threats on space systems are not a new issue. James Pavur distinguished five different periods characterizing the evolution of cyber threats on the space infrastructure:

- **The Early Days** (1957-1979), in which the first instances of political discussions about space cybersecurity occurred. In the 1962 U.S. Congress, the role of private space companies was addressed. While cybersecurity was not on the agenda, policymakers briefly mentioned that commercial satellites would be more susceptible to Soviet attempts of jamming and replay attacks. This

[16] Blount, P.J. (2017). *Satellites are Just Things on the Internet Of Things*. Air & Space Law v.42.
[17] Gini, A. (2014). Cyber crime – *From Cyber Space to Outer Space*. Space Safety Magazine. http://www.spacesafetymagazine.com/aerospace-engineering/cyber-security/cyber-crime-cyber-space-outer-space
[18] Martinovic, I., & Pavur, J. (2019). *The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space*. 11th International Conference on Cyber Conflicts. NATO CCDCOE.
[19] Plotnek, J., & Slay, J. (2022). *Space Systems Security: A Definition and Knowledge Domain for the Contemporary Context*. Journal of Information Warfare. 21.3: 103-19.

period was defined by satellite broadcast abuse between the Soviet Union and the United States to transmit propaganda. Most threats were electromagnetic attacks rather than cyberattacks.

- **Piracy and Spoofing** (1980-1989), in which Pavur explains that the first cyberattacks on space systems took place in the 1980s with a first hijacking attack on an HBO satellite television broadcast conducted by an individual in 1986, an eavesdropping attack carried out by the Indonesian government on a U.S. EO satellite in 1986, as well as a first attack on a ground systems conducted by teenagers on a NASA satellites through a trojan horse in 1987.
- **Broadcast and Flight Control Systems** (1990-1999), which was defined by cyberattacks on satellite TV as well as an increasing number of attacks on ground stations (e.g., NASA'S Goddard Space Flight Center or the ROSAT telescope).
- **Organized Attackers** (2000-2009), in which Pavur notes the rising number of attacks and the emergence of non-state actors as new threat actors (e.g., Tamil Tigers) as well as attacks on ground stations and the first cyberattack using a malware as a threat vector.
- **Evolving Threats** (2010- today), in which Pavur recounts the increasing number of cyberattacks, in particular during armed conflicts as well as the rising complexity of attacks and threat vectors linked to the growing number of cyber operations carried out by State actors.[20]

Recently, the threat landscape has evolved in both cyberspace and outer space. While outer space has been militarized since the dawn of the space age (i.e., the use of space for military purposes on Earth). Today, a new phenomenon is emerging – the weaponization of outer space, that is to say the progressive deployment of weapons in outer space, including cyber ones.[21] In this context, space and cyberspace are interlinked to the extent that space is now militarised and weaponised through cyber means.[22] At the moment, the weaponization of outer space is characterized by discrete threats below the threshold of violence such as cyber or electronic attacks on space systems.[23] This phenomenon is consistent with the militarisation of cyberspace itself in which threats used to come from hacktivists, hackers or criminals looking for financial gains but are now coming from state actors, their proxies, criminals, terrorist groups, hackers and activists in order to serve their interests.[24] [25] As a result, it increases the likelihood of cyberattacks on space systems and extends the attack surface.

However, what is essential to understand with regards to this report is that while cyber threats are not new, they have long been overlooked and misunderstood by policymakers and operators alike[26] and space cybersecurity in general has suffered from a lack of truly interdisciplinary research best described by Falco as the ”vacuum of space cybersecurity.”[27] Plotnek further explains that the literature on space cybersecurity

[20] Pavur, J., & Martinovic, I. (2022). *Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight*. Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac008. https://academic.oup.com/cybersecurity/article/8/1/tyac008/6611670#406985581

[21] Pasco, X. (2017). *Le Nouvel Âge Spatial, De La Guerre Froide Au New Space*. CNRS Editions.

[22] Becht, O., & Trompille, S. (2019). *Rapport d’information sur le secteur spatial de défense*. Assemblée Nationale.

[23] Ibid.

[24] Blount, P.J. (2017). *Satellites are Just Things on the Internet Of Things*. Air & Space Law v.42.

[25] Poirier, C. (2021). *Interdependences Between Space and Cyberspace in a Context of Increasing Militarization and Emerging Weaponization of Outer Space—A French Perspective*. Springer.

[26] Livingstone, D., & Lewis, P. (2016). *Space, the Final Frontier for Cybersecurity?* Research paper. Chatham House.

[27] Falco, G. (2018). *The Vacuum of Space Cyber Security*. Presented at the 2018 American Institute of Aeronautics and Astronautics SPACE and Astronautics Forum and Exposition. https://arc.aiaa.org/doi/abs/10.2514/6.2018-5275

often focuses on niche technologies, formal methods, and narrow topics, which is not conducive to laying the general foundations for general space cybersecurity research.[28]

In political science, the literature on cyber threats against space systems is rather recent, with an increasing interest dating back from the early 2010s. Indeed, in 2013, Valeri recognized that the interdependence between space and cyberspace makes new threats emerge which are difficult to map and characterize.[29] In 2013, Fritz published "*Satellite hacking: A guide for the perplexed*," in which he explained that cyber risks on space systems are too simplified in international relations debates and therefore misunderstood.[30] Also in 2013, del Monte underlined that space legislation and regulations regarding cyber threats are highly complex due to the absence of sovereign territory in outer space.[31] In 2014, Baylon outlined that there is an incompatibility of public policies regarding cyber threats on space systems in a contact of increasing militarization of both space and cyberspace.[32] In 2016, Livingstone and Lewis underlined that cyber risks on space systems are overlooked in public policies.[33] This research marked a turning point in the interest in space cybersecurity in political science research. Gregory Falco recounted Livingstone and Lewis' findings and analysed that cyber threats were not sufficiently considered in U.S. public policies, suggesting that it should be one of the main missions of the U.S. Space Force.[34] The literature regarding the integration and understanding of cyber threats on space systems in Australian public policies seems rather limited at the moment. Yet, Jordan Plotnek conducted a PhD on the cybersecurity of critical space infrastructures in Australia in 2022, which evaluated a space system resilience assessment framework for assessing the resilience of space systems. Nonetheless, it did not necessarily focus on the adequation of Australian space and cyber policies to cyber threats.[35]

2.1.1 Defining Cyberspace and Outer Space

To better understand cyber threats on space systems, it is important to define cyberspace. Cyberspace is a term, which was first coined by the American author William Gibson in the science-fiction novel *Neuromancer* as *'a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts… A graphic representation of data abstracted from banks of every computer in the human system.'* [36] According to the U.S. National Institute of Standards and Technology (NIST), cyberspace is *'a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.'* [37] The Australian Cyber Security

[28] Plotnek, J. (2022). *A Threat-Driven Resilience Assessment Framework and Security Ontology for Space Systems*. Thesis submitted to the University of South Australia for the degree of Doctor of Philosophy.

29 Valeri, L. (2013). Countering Threats in Space and Cyberspace: A proposed Combined Approach. Chatham House, p.3.

[30] Fritz, J. (2013). *Satellite hacking: A guide for the perplexed*. Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies: Vol. 10: Iss. 1, Article 3.

[31] del Monte, L. (2013)

[32] Baylon, C. (2014). *Challenges at the Intersection of Cyber Security and Space Security*. Chatham House.

[33] Livingstone, D., & Lewis, P. (2016). *Space, the Final Frontier for Cybersecurity?* Research paper. Chatham House.

[34] Falco, G. (2018). *Job One For Space Force: Space Asset Cybersecurity*. Harvard.

[35] Plotnek, J. (2022). A Threat-Driven Resilience Assessment Framework and Security Ontology for Space Systems. Thesis submitted to the University of South Australia.

[36] Gibson, W. (1984). *Neuromancer*. Ace Books.

[37] National Institute of Standards and Technology. (n.d.) *Glossary, Cyberspace*. Computer Security Resource Center. https://csrc.nist.gov/glossary/term/cyberspace

Centre (ACSC) defines cyberspace as *'the environment formed by physical and non-physical components to store, modify, and exchange data using computer networks.'* [38]

In fact, cyberspace is often described as composed of three layers: a physical layer (1), a logical layer (2) and a semantic layer (3). Although cyberspace seems only virtual, the first layer is rather tangible. This physical layer, also called the material or infrastructure layer, refers to the equipment, infrastructure, and hardware such as computers, submarine-cables, smartphones; and satellites that enable data to flow through cyberspace.[39] It includes servers, USB keys, and datacentres where data are stored. This infrastructure can be geographically located and physically destroyed.[40] The logical layer, also called software layer, consists of the lines of codes in various programming languages and binary information that the machine will transform into readable information for the end user. It also refers to software and protocols such as the TCP/IP protocol that will allow machines to interact with one another and enable the information to disseminate in the form of data packets.[41] The semantic layer, also called social, cognitive, or informational layer, consists of the actual information and data exchanged in cyberspace. It includes end users, their digital identity; and their interactions.[42]

Similarly, outer space can also be described as composed of different layers: Low Earth Orbit (LEO), which is the space below an altitude of 2,000 km, the Polar Orbit, which is located at an approximate altitude of 850 km above the poles, Medium Earth Orbit, which is located between 8000 and 20,000 km above the Earth, and the Geostationary Orbit (GEO), which is located at an approximate altitude of 36,000 km above the Earth.[43]

2.1.2 Defining a Cyberattack on a Space System

Cyberattacks are generally performed through compromising ground control systems or by intercepting communications from satellites to terrestrial systems and vice versa.[44] Usually, to understand the anatomy of a cyberattack it is common to refer to the Cyber Kill Chain (CKC), a conceptual model created by Lockheed Martin to understand the various stages of a cyberattack (i.e., reconnaissance, weaponisation, delivery, exploitation, installation, command & control, and actions on objectives).[45]

However, there is no universal definition of a cyberattack, let alone of a cyberattack on a space system. Similarly, there is no universally accepted definition of a space weapon and therefore no definition of what could be defined as a cyber weapon in outer space. Plotnek and Slay defined the anatomy of an attack on a space system as a composed of a threat actor, a threat vector, which marks the entry into the satellite systems, the attack is then the exploit used by the attacker to achieve a certain impact.[46]

[38] Australian Cyber Security Centre. (2023). *Glossary, Cyber Attack*. Commonwealth of Australia. https://www.cyber.gov.au/learn-basics/view-resources/glossary

[39] Limonier, K. (2018). Ru.Net: *Géopolitique Du Cyberespace Russophone*. Les Carnets de l'Observatoire. L'inventaire.

[40] Douzet, F. (2014). *La géopolitique pour comprendre le cyberespace.* Hérodote.

[41] Ibid.

[42] Kempf, O. (2014). *Alliances et mésalliances dans le cyberespace.* Collection Cyberstratégie. Economica; Poirier, C. (2021). op cit.

[43] Georgescu, A., et al. (2019). *Critical Space Infrastructures: Risk, Resilience and Complexity*. Springer.

[44] Falco, G. (2018). *The Vacuum of Space Cyber Security*. Presented at the 2018 American Institute of Aeronautics and Astronautics SPACE and Astronautics Forum and Exposition. https://arc.aiaa.org/doi/abs/10.2514/6.2018-5275

[45] Plotnek, J. (2022). *A Threat-Driven Resilience Assessment Framework and Security Ontology for Space Systems*. Thesis submitted to the University of South Australia.

[46] SmartSat. (2022). *Satellite Cyber Resilience Whitepaper*. SmartSat. Adelaide, Australia. https://smartsatcrc.lbcdn.io/uploads/Satellite-Cyber-Resilience-Whitepaper-FINAL.pdf

However, when analysing the policy and legal framework of the cybersecurity of a country's space infrastructure, it is important to investigate the definitions adopted by the Government as it can have consequences on the applicability of the legal framework in case of a cyberattack on a satellite and the possibility to retaliate in compliance with national and international law. Can an attack on a computer located on Earth, which controls a satellite, be considered as an attack on a space system? Is an attack on a ground station considered as an attack on a space system? Can a cyberattack on a satellite be considered by the Australian government as an armed attack?

While it is not a public policy, the NATO CCDOE Tallinn Manual 2.0 is one of the only documents to settle the question by distinguishing 'space-enabled cyber operations' from 'cyber-enabled space operations.' Cyber operations enabled by space assets cannot be considered as cyberattacks on space systems. For example, a cyberattack that would only use satellites as a relay for connection or data transfer cannot be understood as a cyberattack against a space system. In this case, the cyberattack does not produce effects in outer space. However, space operations enabled by cyber means are considered by the Manual as real cyberattacks on space systems. If cyberspace is used to take control of a satellite or its payload, then cyberspace enabled activities in outer space.

The ACSC acknowledges that there are various definitions of a cyberattack but considers it as *'a deliberate act through cyberspace to manipulate, disrupt, deny, degrade or destroy computers or networks, or the information resident on them, with the effect of seriously compromising national security, stability or economic prosperity.'* [47] Does this definition apply to space systems? It does not seem that Australian cyber and space policies provide a definition of a cyberattack on a space system. Similarly, Australian cyber and space policies do not precise whether satellites are part of cyberspace.

Based on the operational environment observed within this report, which is the Australian domestic framework, it is important to use the ACSC's definition of cyberattack and electronic attack. This is because the ACSC leads the Australian Government's efforts on cybersecurity, and, therefore, exerts major influence in the Australian context. Building on ACSC's definition, then, for the purpose of this report, a cyberattack on a space system will be considered as an attack using cyber means and targeting or producing effects on the space infrastructure, including the ground segment, the space segment, and the user segment, to manipulate, disrupt, deny, degrade, or destroy space systems or the information they produce.

Cyberattacks vs. Electronic Attacks

Cyberattacks should not be misunderstood with electronic attacks such as jamming and spoofing. In policy documents, the academic literature, and more generally in strategic debates, there is often a confusion regarding the nature of these attacks. This is also the case in Australian policies where these attacks are often referred to under the umbrella term 'grey zone operations.'

Jamming consists in interferences with links to and from a satellite by emitting noise of the same radio frequency.[48] Spoofing consists in deceiving a satellite signal receiver by broadcasting a fake signal, which is supposed to resemble a normal signal.[49] Meaconing consists in delaying the reception of signals.[50]

Electronic attacks are in the realm of physics and involve the use of radiofrequency spectrum to deny, degrade, or disrupt satellite systems, whereas cyberattacks are in the realm of computer science and directly target data and computer systems or networks.[51] Electronic attacks exploit physical

[47] Australian Cyber Security Centre. (2023). *Glossary, Cyber Attack*. Commonwealth of Australia. https://www.cyber.gov.au/learn-basics/view-resources/glossary
[48] Velkovsky, P., et al. (2019). *Satellite Jamming, A Technology Primer*. On the Radar. CSIS.
[49] Fabio, D. (2015). *GNSS, Interference Threats and Countermeasures*. Artech House.
[50] Ibid.
[51] Rajagopalan, R.P. (2019). *Electronic and Cyber Warfare in Outer Space*. Space Dossier 3. UNIDIR.

vulnerabilities and are often external to the targeted system while cyberattack exploit non-physical vulnerabilities and are often internal to the targeted system.[52]

However, it is important to note that both cyber and electronic attacks can create similar effects on space systems. For instance, the introduction of a malicious code on a ground station may block the reception of the GNSS signal (similar effects to jamming), can delay the reception of the signal (meaconing), or display a fake signal (spoofing).

According to Jeffrey Bardin, this confusion stems from a misunderstanding of the concept of hacking, which refers to a reconfiguration or modification in the system so that it functions according to parameters that have not been defined by the owner, administrator, or designer. Electronic attacks do not necessarily involve an intrusion into a computer system, they simply intercept the signal or frequency emitted by the satellite.[53] Moreover, the confusion may simply be due to historical reasons as electronic attacks appeared long before the invention of computers. As a result, when the first cyberattacks were detected, they were classified as 'electronic attacks' because it was the existing category that most closely resembled to the observed phenomenon, and we did not have yet enough knowledge of cyberspace to differentiate them.[54] Finally, the confusion may also remain due to the convergence between the electromagnetic spectrum and cyberspace. According to Zsolt Haig, cyberspace and the electromagnetic spectrum create a common operational environment that could be named as the cyber electromagnetic domain.[55] To some extent, this is the case in Australia as the DoD's Defence Science and Technology Group established a Cyber and Electronic Warfare Division, which integrates science and technology capabilities across cyber, electronic warfare, signals intelligence, and communications to cover the continuum of the cyberspace and electromagnetic environment.[56]

2.1.3 Typology of Cyberattacks on Space Systems

Cyber threats on space systems can be defined, characterized, or classified in many ways depending on the types of the attack, the target of the attack, the nature and intention of the attacker, the attack surface, or the targeted space segment.

Several typologies have been established by scholars in the past few years: While the American think-tank CSIS established a typology based on data, differentiating data interception and monitoring, data corruption, and seizure of control,[57] the Secure World Foundation categorized cyberattacks based on the attack surface with the risks on the supply chain (hidden back doors on hardware and software components, cyberattacks on space manufacturers, etc.), the space segment (cyberattack against the payload, a sensor, etc.), the user segment, and the ground segment (interception or interference with downlink, etc.).[58] The NATO Joint Air Power Competence Centre (JAPCC) also categorizes attacks based on the various segment, differentiating the ground, space, and link segment.[59] French author Olivier Kempf differentiates cyberattacks through the perspective of information by distinguishing attacks against information (disrupting the system, preventing

[52] Livingstone, D., & Lewis, P. (2016). *Space, the Final Frontier for Cybersecurity?* Research paper. Chatham House.
[53] Bardin, J. (2014). *Satellite Cyber Attack Search and Destroy*. Cyber Security and IT Infrastructure Protection. Elsevier.
[54] Blount, P.J. (2017). op cit
[55] Haig, Z. (2015). *Electronic Warfare in Cyberspace*. Security and Defence Quarterly, 2,7, p.22-35.
[56] Defence Science and Technology Group. (2022). *Cyber and Electronic Warfare Division*. Commonwealth of Australia. https://www.dst.defence.gov.au/divisions/cyber-and-electronic-warfare-division
[57] Harrison, T., et al. (2020). *Space Threat Assessment 2020*. CSIS. https://www.csis.org/analysis/space-threat-assessment-2020
[58] Weeden, B., & Samson, V. (2020). *Global Counterspace Capabilities: An Open Source Assessment*. Secure World Foundation.
[59] NATO Joint Air Power Competence Centre. (2020). *Cyber Threats to Space Systems*. https://www.japcc.org/essays/cyber-threats-to-space-systems/

the user from accessing or using the space systems by making them inaccessible such as DoS, DDoS, etc.), attacks for information (compromising the confidentiality of the system through intrusion, data interception and breaches), attacks by information (injecting fake information or taking control of a system by sending commands such as APT).[60] Plotnek and Slay distinguish attacks based on adversities, namely non-malicious adversities (accidental and environmental), cyber adversities (code and data manipulation, malware, denial of service, hijacking, spoofing, eavesdropping, cyber warfare), electronic adversities (jamming, lasers, spoofing, eavesdropping, EMP weapons, electronic warfare, directed energy weapons, blinding), kinetic adversities (physical attacks missiles, ASAT).[61]

In Australia, the Space Cyber Architecture (SCArch), developed under the Defence Innovation Hub Project, provides strategic and cybersecurity guidance to the nascent Australian satellite industry to provide strategic and operational cybersecurity guidance. The SCArch is constructed to provide both an end-to-end view of the space industry and provides additional detailed guidance for each participating industry vertical. The SCArch also provides tailored technical guidance across the entire sector and considers risks on the entire attack surface: the launch vehicle, the launch site, the satellite, the payload, the ground station, the operator, the user, and the supply chain. Therefore, for the purpose of this report, cyberattacks will be primarily analysed based on the attack surface.

Attack Surface - Points of Access

Plotnek defined the attack surface on space systems in four categories as demonstrated in the table below:[62]

TABLE 3 SPACE SYSTEMS SEGMENTS (SOURCE: PLOTNEK, 2022)

Governance Segment	R&D, Procurement & Supply Chain, Personnel, Legal, Ethical & Compliance
Ground Segment	Teleport & Terminals, Space Traffic Management, Launch Facility / Vehicle, Simulators / Emulators, Manufacturing Facilities
Space Segment	Power System & Wiring, Propulsion System, Weapon System, Life Support Systems, Space Vehicles & Rovers
Comms, Control & Computing C3 Segment	Sensors, Data (scientific, technical, positional, etc), Control Signalling, Radio Link & Telemetry, Computing, Software, Onboard Processing

Regarding the attack surface, three primary points of access exist for exploitation, attack, and service denial of space assets:

- **the supply chain**, which includes:
  - systems and subsystems
  - materials EEE components
- **the software**, which includes:
  - the extended land-based infrastructure that sustains space-based assets including:
  - launch infrastructures

[60] Kempf, O. (2014). op cit, p.44
[61] Plotnek., J., & Slay, J. (2023). *COSMOS2: Contemporary Ontology for the Security Management of Space Systems*. International Journal of Critical Infrastructure Protection.
[62] Plotnek, J. (2022). *A Threat-Driven Resilience Assessment Framework and Security Ontology for Space Systems*. Thesis submitted to the University of South Australia.

  - ground stations
  - data relay
  - terminals
  - radars
  - telescopes
- **the space assets** themselves, which include:
  - launch vehicles
  - satellites bus
  - satellite payload

Effects - Purpose

Cyberattacks on space systems can also be assessed from the perspective of the range of effects, both kinetic and non-kinetic, they can produce. These include:

- Theft of information
- Alteration of service or information
- Denial of service or information
- Control of satellites, their subcomponents, or supporting infrastructure
- Destruction of satellites, their subcomponents, or supporting infrastructure.[63]

Types of Attack

Beyond the attack surface, there are different typologies of cyberattack to space infrastructure. Several highly comprehensive models specifically adapted to the space sector have been recently built to map the various types of attacks such as Aerospace Corporation's Space Attack Research and Tactic Analysis (SPARTA),[64] or ESA Space Shield.[65] Pavur also lists various types of threats on space systems as shown below:[66]

[63] Harrison, T., Johnson, K., Young, M., & Wood, N. (2022). *Space Threat Assessment 2022*. Center for Strategic and International Studies. https://www.csis.org/analysis/space-threat-assessment-2022

[64] Aerospace Corporation. (2022). *Space Attack Research & Tactic Analysis (SPARTA).* https://sparta.aerospace.org/

[65] European Space Agency. (2023). *Space Techniques.* https://spaceshield.esa.int/techniques/space

[66] Pavur, J., & Martinovic, I. (2022). *Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight*. Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac008. https://academic.oup.com/cybersecurity/article/8/1/tyac008/6611670#406985581

Table 4: Satellite Vulnerability Matrix (Source: Pavur & Martinovic, 2022)

Vulnerability type	Posited in	Example attack scenario	Relevant sub-systems	Empirical Examples	Sophistication
Denial of service	[18]	Force satellite to enter "Safe Mode"	Payload	None to date	Very high
Hardware backdoor	[18]	Inject malicious commands on hardware bus	Payload Ground	None to date	Very high
Privilege escalation	[24]	Send flight control commands from payload software application	Payload	None to date	Very high
Bespoke malware	[14]	Exploit vulnerability in satellite firmware or ground telemetry software	Payload Ground	[25,26]	Very high
Payload hijacking	[20]	Maneuver satellite to undermine sensor readings	Payload	Possibly: [27,28]	Very high
Sensor injection	[29]	Blind imagery sensors with long-range laser signals	Payload	[30]	High
Jamming	[18]	Block satellite phone reception in remote conflict zone	Signal	[31]	Low–moderate
Eavesdropping	[15]	Intercept sensitive internet traffic from satellite signals	Signal	[32]	Low
Metadata analysis	[15]	Identify classified satellite based on radio spectrum behaviour	Signal	[33]	Low–moderate
Replay attack	[15]	Re-issue intercepted commands to cause harmful maneuver	Signal	None to date	Moderate–high
Signal injection/ hijacking	[2,17,21]	Overwrite legitimate signal with falsified broadcast	Signal	[34]	Low–moderate
Generic malware	[15,18]	Compromise space-related system with generic ransomware	Ground Payload	[35]	Low
Social engineering	[15]	Phishing campaign used to access satellite design documents	Ground	[27]	Very low
Physical access	[4, 5]	Theft of laptop w/ flight software	Ground	[36,37]	Low–moderate
Data corruption	[15]	Damaging stored imagery data to prevent intelligence use	Ground	None to date	Low

To provide a broader idea and definitions of each type of threats a few examples are cited below:

- **Hacking**: Unauthorized access into a satellite or space system, often to exploit a space system's data or manipulate its normal behaviour (Based on the ACSC definition).
- **Malware**: Any type of code, software, or program that is used for a malicious purpose such as gaining access to a space system, stealing information, modifying information, deny access or service, installing software without an operator's knowledge, etc. (Based on the ACSC definition).
- **Ransomware**: A type of malware, which is designed to enter a system, block access, encrypt the data, lock the system, and demand a ransom from the user to victim to restore access to the data/device.
- **Hijacking**: A type of network security attack in which the attacker takes control of a space system.
- **Replay**: An attack that involves the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access. (Based on the NIST definition).
- **DDoS/DoS**: Denial of Service (DoS) aim at disturbing, paralysing, or blocking a computer system (potentially a space system or control centre) by multiplying requests to overload the system. Distributed Denial of Service (DDoS) usually involves the use of botnets, which are infected computer systems, to send multiple requests to a target and overload the system.
- **Exploitation of a zero-day vulnerability**: A vulnerability which not yet discovered and may be exploited by malicious actors.
- **Exploitation of a known but unpatched vulnerability**: A vulnerability which is not yet fixed, patched, or unfixable.
- **Man in the middle attack**: A general term for when a perpetrator positions himself in a conversation between a user and a space system to eavesdrop or impersonate one of the parties.
- **Insider threats**: Cybersecurity risks that originate from within a space-related organization, which usually involves access, modification, sabotage, or sharing of information that affect the integrity, confidentiality, and availability of the organization, its space systems, its data, personnel, or facilities.

While these types of attack are shared with other infrastructure relying on ICT to operate, the space infrastructure has some specificities that make cyber threats particularly worrisome. Cyberattacks can indeed have serious consequences for the larger space ecosystem, not just the owners of the capability. Some examples of unique space vectors are:

- Lack of physical access to assets to provide reset or independent assessment of current asset status,
- The risk of remote access being denied when attempting to determine satellite status of health and ranging data,
- Globally accessible assets, increasing vectors to access signals and information leakage,
- Spacecraft Control RF links that are susceptible to eavesdropping and interference from ground connections,
- A complex supply chain, and rapidly evolving designs and components,
- Potential weaponization of asset if control of spacecraft manoeuvring is hijacked,
- Unique ecosystem for build, integrate, launch, operate and decommissioning,

- Multiple technologies subject to export control and/or Defence security controls.[67]

Attackers

Cyberattacks to space systems are also concerning due to the large variety of agents that can pose a threat to the space infrastructure. In the past, actors who could pose threats to the space infrastructure were very specific and clearly identifiable. In today's cyber space, almost anyone can initiate aggressive actions towards assets in outer space, with added difficulty of determining the perpetrator. Cyberattacks can be perpetrated by several actors, including nation-state, terrorist, criminal, hacktivist, and individuals.[68]

In a categorisation introduced by the Aerospace Corporation these various types of threats agents have been categorised in seven tiers, as shown below.

TABLE 5: THREATS AGENTS, SKILLS, MOTIVES AND METHODS (SOURCE: AEROSPACE CORPORATION)

Tiers	Name	Skills	Malice	Motive	Methods
1	Script kiddies	Very low	Low	Boredom, thrill seeking	Download and run hacking scripts
2	Hackers for hire	Low	Moderate	Prestige, personal gain, thrill seeking	Write scripts, engage in malicious acts, brag about exploits
3	Small hacker teams: non-state actors OR disorganised state actors	Moderate	Moderate	Power, prestige, intellectual gain, respect	Write scripts and automated tools
4	Insider threats (e.g., disgruntled employees)	Very low-very high	Very low-very high	Unwitting, ideology, politics, espionage	Insider knowledge: methods can range from inadvertent to sophisticated
5	Large, well-organised teams: non-state or state actors	High	High	Personal gain, greed, revenge	Sophisticated attacks by criminals; Very Low-very high', 'guns for hire', or organised crime
6	Highly capable state actors	Very high	Very high	Ideology, politics, espionage	State sponsored cyberattacks against enemy nations
7	Most capable state actors				

[67] CyberOps. (2023). *Australian Space Cyber Framework*. P.6 ; Pavur, J., & Martinovic, I. (2022). *Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight*. Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac008; Bailey, B. (2019). *Defending Spacecraft in the Cyber Domain*. Aerospace Corporation.

[68] Plotnek, J. (2022). *A Threat-Driven Resilience Assessment Framework and Security Ontology for Space Systems*. Thesis submitted to the University of South Australia.

Bradbury, et al. also attempted to map attackers, their motives, capabilities, environment, and resources as shown in the table below:[69]

TABLE 6: THREAT ACTORS (SOURCE: BRADBURY, ET AL. 2020)

	Threat Actor	Example	Goals & Motivations	Capabilities	Environment	Resources
Individual	Outsider	Hacktivist	Personal satisfaction; Passion; Ideology. Doesn't believe in climate change, wants to impact functioning of climate satellite	Limited	Remote access	Minimal
	Insider	Cleaner	Financial gain; Discontent	Limited	Permission-less internet access	Internal knowledge
	Trusted Insider	Contractor	Financial gain; Discontent	Moderate	Internal access with some permissions	Internal knowledge
	Privileged Insider	Employee	Financial gain; Discontent	High	Internal access with high permissions	Internal knowledge
Group	Ad Hoc	A group coming together over a time-critical event (e.g. Brexit or a collective movement of Extinction Rebellion)	Dependant on group purpose: Ideological, financial, political	Limited to Moderate	Remote access	Limited knowledge and financial
	Established	A group (e.g. the Anonymous group)		Moderate to High	Remote access	Moderate knowledge and financial
Organization	Competitor	An organization about to compete for a tender for services	Corporate espionage; Financial gain; Reputation damage	Organisation size related	Remote access	Organisation size related
	Supplier	A supplier who fears their services are soon to be relinquished	Information gain; Financial gain		Remote access; Knowledge of internal structure	
	Partner	A partner with whom a relationship is starting to sour or is soon to end	Information gain; Financial gain		Limited internal access; Knowledge of internal structure	
	Customer	A customer who feels they have had poor or unfair service	Information gain; Financial gain		Remote access; Knowledge of internal structure	
	Nation-State	Geopolitical rival	State rivalry; Geopolitics	Sophisticated; Coordinated; Access to state secrets	Remote and internal access	Extensive knowledge; Extensive financial;

[69] Bradbury, et al. (2020). *Identifying Attack Surfaces in the Evolving Space Industry Using Reference Architectures*. IEEE Aerospace Conference. https://doi.org/10.1109/AERO47225.2020.9172785

						Advanced equipment

James Pavur and Ivan Martinovic also provided their taxonomy of threat actors, their motives, and their capabilities as shown below:[70]

Table 7: Overview of Threat Actors Proposed in Literature (Source: Pavur & Martinovic, 2022)

Attacker Type	Example Motivations	Technical Capabilities	Selected References
National Military	• Space Control • Anti-Satellite Weapon	Very High	[4, 12, 14, 15]
State Intelligence	• Counter-Intelligence • Technology Theft • Eavesdropping	Very High	[15]
Industry Insiders	• Sabotage • Technology Theft	High	[15, 16]
Parts Suppliers	• Sabotage • Espionage	Moderate	[17, 18]
Organized Crime	• Eavesdropping • Ransom • Technology Theft	Moderate	[4, 15]
Terrorists/Militant Org.	• Anti-Satellite Weapon • Message Broadcast • Notoriety	Low to Moderate	[4, 14]
Commercial Competitors	• Sabotage • Technology Theft	Low	[15]
Individual Hackers	• Notoriety • Personal Challenge	Very Low	[4, 14, 19]
Political Activists	• Message Broadcast	Very Low	[14, 15]

[70] Pavur, J., & Martinovic, I. (2022). *Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight*. Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac008. https://academic.oup.com/cybersecurity/article/8/1/tyac008/6611670#406985581

Overall, Plotnek and Slay have summarized these models in the context of threats against critical space infrastructure.[71]

2.2 Australia’s Space Activities and their Cyber Threats

2.2.1 Overview of Australia’s Space Activities

Australia has embarked upon a journey to grow a globally responsible and respected space sector, lifting the economy and inspiring and improving the lives of Australians.[72]

Alongside its traditional security and defence objectives,[73] the country has put a renewed focus on the development of a strong commercial industry as a driver for jobs and economic growth in the last decade. In this respect, the Australian Civil Space Strategy 2019–2028 recognizes the importance of space industry in diversifying the economy, developing national capability, and inspiring and improving lives of all Australians. The declared objective is to triple the size of the space sector from $3.9 billion to $12 billion and grow the segment from around 10,000 jobs to 30,000 jobs by 2030, with further job creation and economy growth expected from spill-over effects. The very creation of ASA responds to the resolve of enabling industry to deliver innovative solutions rather than managing institutional space activities.[74]

Most Australian market sectors are expected to ‘*get direct or spillover benefits from space-enabled services and practical applications of space capabilities, including finance, agriculture, mining, health and tourism.’*[75] In view of this, a closely related goal is the leveraging of space technologies to bring in new innovative solutions that, in turn, support addressing global challenges such as climate change and sustainable development goals and generate societal benefits. For instance, connectivity increasingly bridges the digital divide experienced by remote and rural communities. Also, the capacity to access various space-derived environmental datasets is critical to manage and mitigate climatic risks and disasters such as the bushfires devastating the country.

In the process, this intensification of investments and activities in several fields should also attract foreign workers and entrepreneurs and increase Australia’s international relevance. Ultimately a strategic objective is to grow an internationally renowned space sector that can further underpin Australia’s reputation and weight on the global scene in terms of both the ability to influence international decisions and attract international customers and partners.

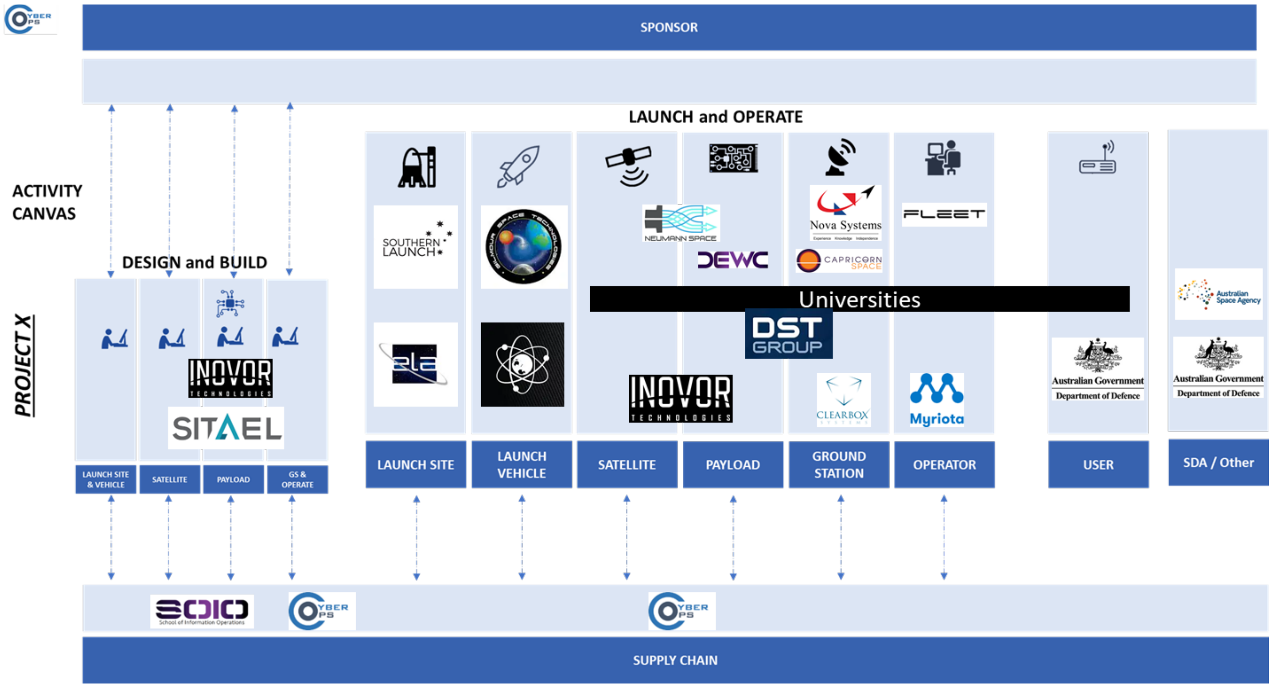
In pursuing these objectives, Australia has adopted a stepped approach that makes use of different institutional, policy and legal tools as well as programmatic and international cooperation measures. These measures ‘*focus on transforming, inspiring and creating a competitive environment for the space sector to grow, and advancing Australia’s competitiveness and role as a responsible actor in civil space.’*

Australia has a dynamic and rapidly expanding commercial space sector, with an annual growth of over 10 per cent over the past five years. Downstream activities account for the majority of revenues, but innovation in space technologies is stimulating growth in the upstream segment as well. In the upstream segment, Australia’s space industry has mature capabilities in the manufacturing of ground systems and satellite laser

[71] SmartSat. (2022). *Satellite Cyber Resilience Whitepaper*. SmartSat. Adelaide, Australia. https://smartsatcrc.lbcdn.io/uploads/Satellite-Cyber-Resilience-Whitepaper-FINAL.pdf
[72] Australian Space Agency. (2019). *Advancing Space: Australian Civil Space Strategy 2019-28*.
[73] Defence has always been an important component of Australian space program and continues to retain a key role today, as evident from the budgetary allocations to the DoD exceeding those of civil space activities. With its new Strategy and Plan, Defence is ensuring investments are made to grow space capabilities that support its national security requirements.
[74] Bedi, R., et al. (2020). *Australian Space Outlook 2020*. Faircount Media Group, 13, p.13.
[75] Australian Space Agency. (2019). *Advancing Space: Australian Civil Space Strategy 2019-28*. p.6.

ranging telescopes. It is also building capabilities to manufacture nanosatellites and microsatellites in partnership with universities. While it still has very limited manufacturing capabilities for larger satellites and launch vehicles, now that the country has found commercial interests, private actors are developing sub-orbital and orbital rockets and building spaceports in different parts of the country.[76] As a result, the Australian space industry currently spans through the entire life cycle of the space activities canvas. Some illustrative examples are provided below.

FIGURE 9: AUSTRALIAN SPACE ACTIVITIES CANVAS (SOURCE: CYBEROPS)

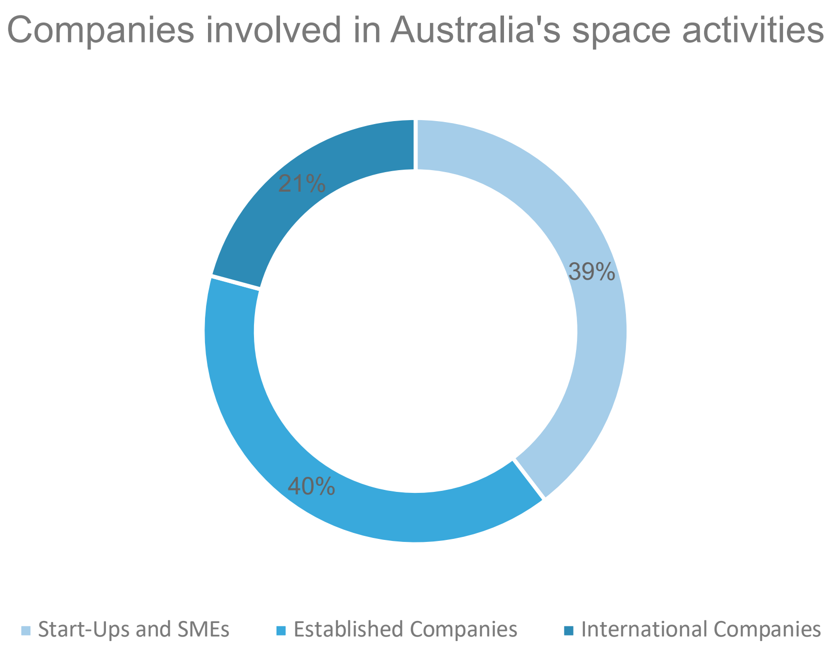


The Australian space ecosystem is comprised of organisations ranging from small start-ups to large multinational companies. According to the Space Industry Association of Australia (SIAA), there are over a hundred companies involved in the space sector to different extents.[77] Some contribute to space on a smaller scale, e.g. through the integration space technologies into their business, e.g. by using data from Earth observation satellites. Others are fully dedicated to developing space technologies and directly shaping the national space sector, for instance by developing end-to-end missions in-house through Australian expertise.

In terms of number and size, the 2018 Review of Australian´s Space Industry Capabilities listed a total of 149 companies with space activities.[78] The catalogue accounted for 59 startups and SMEs, 59 established companies, as well as 31 multinationals with offices and activities in Australia.

[76] Aliberti, M., et al. (2020). *Emerging Spacefaring Nations*. European Space Policy Institute.
[77] South Australian Space Industry Centre. (n.d.) *Ping Services*. https://sasic.sa.gov.au/industry/industry-directory/ping-services/
[78] Expert Reference Group for the Review. (2018). *Review of Australia´s Space Industry Capability*. Australian Space Agency. p.70-77.

Figure 10: Breakdown of Australian Space Companies



2.2.2 Identifying Relevant Cyber Threats to Australia's Space Infrastructure

As the Australian space ecosystem is comprised of organisations ranging from small start-ups to large multinational companies, it is clear that a '*one size fits all approach to cybersecurity will not prove effective due to the difference in terms of company maturity, risk profile, and available resources to respond to cyber compliance tasks*.'[79]

In addition, the space environment in Australia is '*a tightly coupled ecosystem, where local developers are bound to a limited number of local suppliers and a much wider number of options from overseas suppliers. This introduces a level of sovereign risk to the growth of the local industry, if the supply chain is compromised by cybersecurity issues both domestically and abroad*'.[80] In addition, as analysed by Plotnek, there are no obvious threat actors to the Australian space infrastructure that can enable to scope down the study, which renders consultations with both the Australian industry and decisionmakers essential to better grasp the nature of the threat at the national level.[81]

Because of these specific features, any identification of threat vectors must be tailored to the Australian ecosystem. To support the identification of the most representative set of cases studies, Flinders University and CyberOps, organized a series of consultations and dedicated workshop with relevant SmartSat CRC partners. The workshop was specifically intended to collect CRC partners' views on the cyber threats that the Australian space sector is currently confronted with and define the case studies that will be analysed in the project. More broadly, the workshop, organised by Flinders with the support of CRC, aimed at commencing a dialogue to promote a common understanding and appraisal of cybersecurity threats for

[79] CyberOps. (2023). *Australian Space Cyber Framework*. p. 6-7.
[80] Ibid.
[81] Plotnek, J. (2022). *A Threat-Driven Resilience Assessment Framework and Security Ontology for Space Systems.* Thesis submitted to the University of South Australia.

space infrastructures among Australian stakeholders, in view of building a shared vision of the challenges that Australia is called to face.

This first portion of the workshop was focused on identifying the most likely cyber threats that could affect Australia's space missions, considering the entire lifecycle from the supply chain to the manufacturing, the launch and the exploitation of the systems. Considerations included:

- Likelihood and impact of different types of cyberattack in Australia
- Likelihood and impact on the different attack surfaces in Australia
- Specificities of Australia’s space cyber threats

The second part aimed to assess preparedness, gaps, and opportunities to enhance the cyber maturity of Australia’s space sector and collect inputs on how to get there. Considerations included:

- Preparedness and resilience of Australia’s space organisations
- Perceived gaps in the policy, legal and regulatory domain
- Measure to enhance cyber maturity

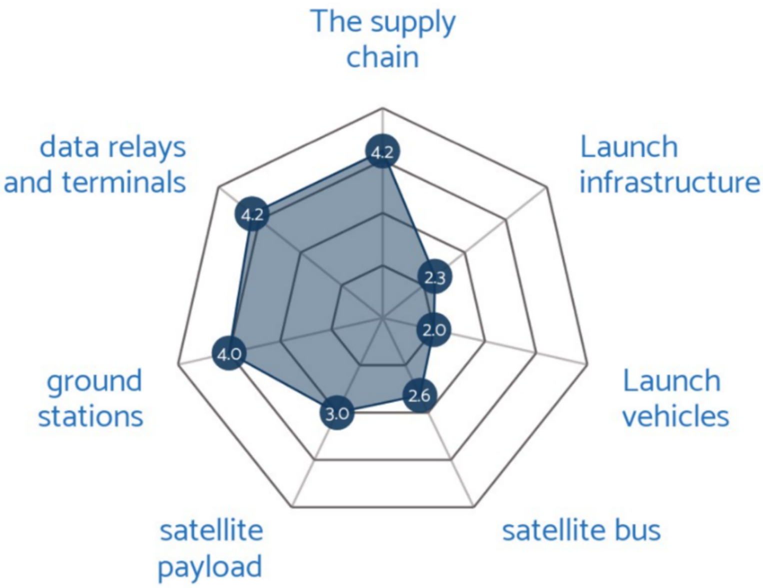
The workshop made use of polls to better identify common views on the attack surface, the attack purposes, and attack typology. Major findings are reported hereby.

Attack Surface

Regarding the attack surface, consulted stakeholders expressed convergence on the fact that the most concerning entry point is represented by the supply chain, followed by data relays and terminals and ground stations. The launch vehicles, launch infrastructure and satellite bus were not identified as concerning attack surfaces under the present circumstances.

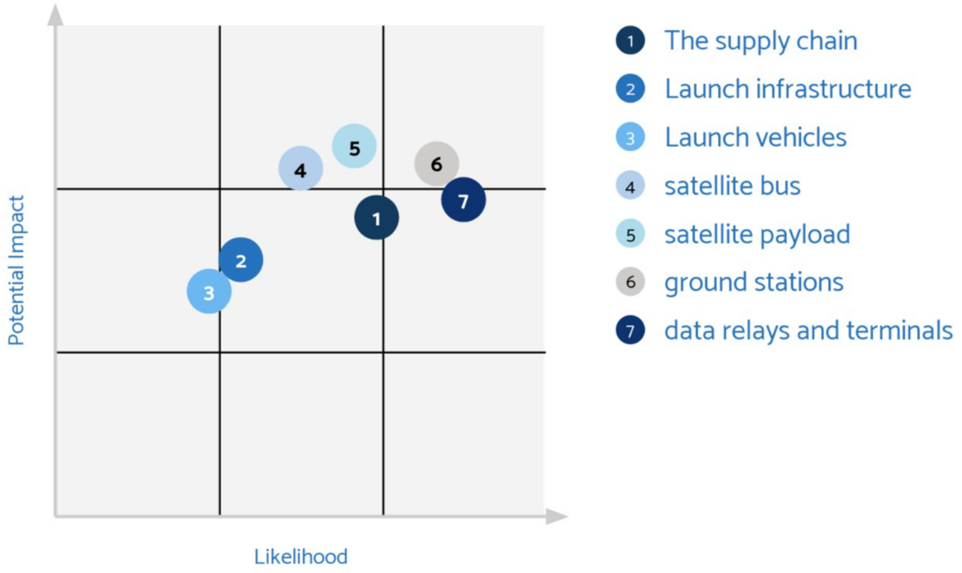
These results are consistent with the fact that Australia does not yet have a strong upstream segment (manufacturing of spacecraft and launch vehicles) and greatly relies on outsourcing most systems, subsystems, and components.

FIGURE 11: MOST CONCERNING ENTRY POINTS FOR AUSTRALIA



This widespread concern more specifically stemmed from the relatively higher likelihood and potential impact of cyberattacks on the supply chain, the ground stations and the data relays and terminals as compared to other attack surfaces (particularly the launch infrastructure and the launch vehicle).

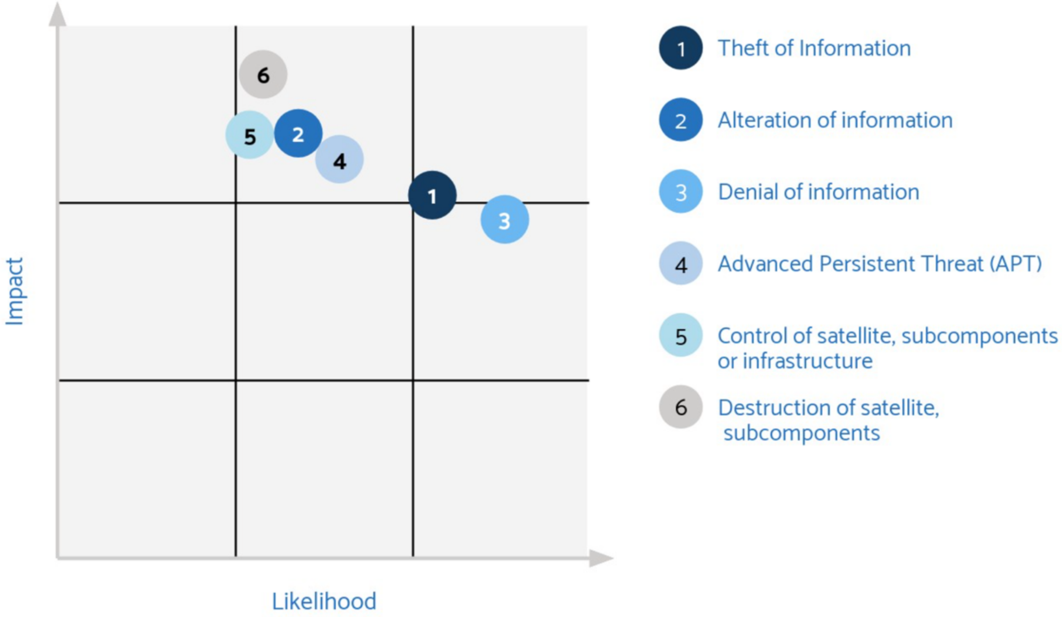
FIGURE 12: LIKELIHOOD AND IMPACT OF THE DIFFERENT ATTACK SURFACES



Attack Purpose

With specific respect to the purpose and effects of a cyberattack, the workshop showed that denial of information and theft of information were the most likely purpose of an attack on the Australia's space infrastructure, even though also the least impactful. Conversely, control and/or destruction of the satellites, their subcomponents, or supporting infrastructure were marked as the potentially most impactful but least likely attack purposes. Results are shown below.

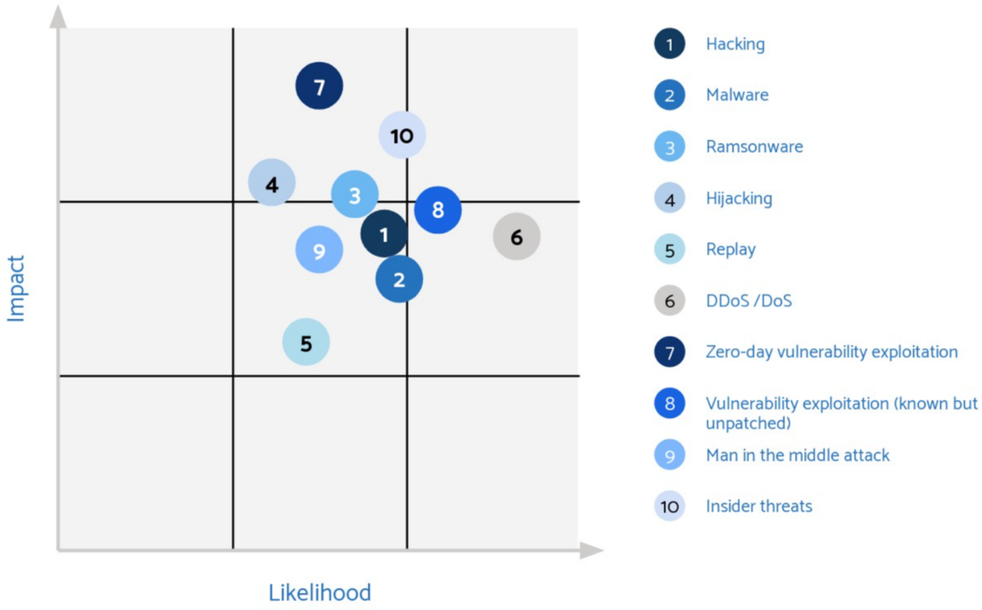
FIGURE 13: LIKELIHOOD AND IMPACT OF THE DIFFERENT ATTACK PURPOSES



Types of Attack

Regarding the specific typology of cyberattack, CRC partners expressed convergence on the fact that DDoS/DoS and vulnerability exploitation currently represent the most likely type of attack for the Australian space sector. Other likely attacks, include insider threats, malware, and hacking. In terms of impact, however, the view was expressed on the fact that zero-day vulnerability exploitation, insider threats and ransomware represent the potentially most impactful types of attack. Replay, malware, man in the middle attack, hacking scored as moderately likely and impactful cyberattacks.

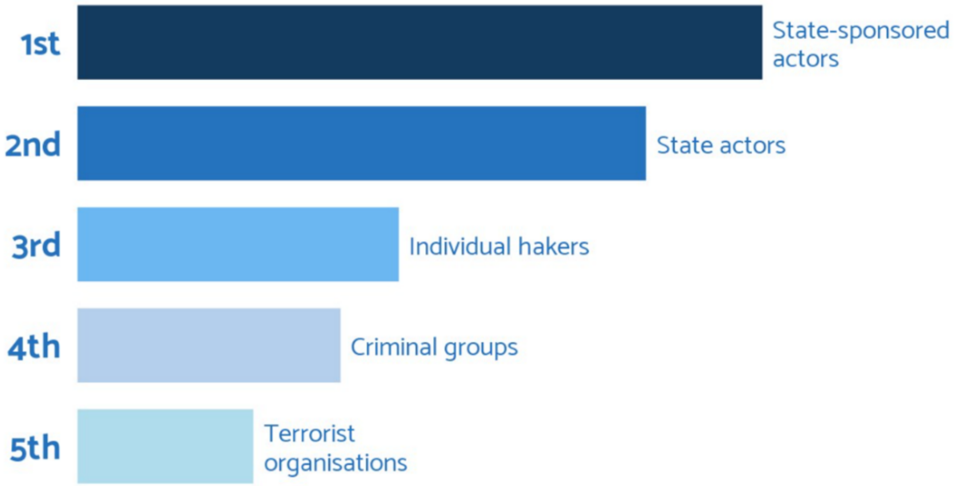
FIGURE 14: LIKELIHOOD AND IMPACT OF DIFFERENT TYPES OF CYBERATTACKS



Attackers

Among CRC partners and other consulted stakeholders, there was wide consensus that the most concerning threat agents are state-sponsored actors, followed by state actors and individual hackers. Results are shown below.

FIGURE 15: RANKING OF POTENTIAL THREAT AGENTS FOR AUSTRALIA'S SPACE INFRASTRUCTURE



Outcomes of the polls were used to inform the definition of use cases presented in the following section.

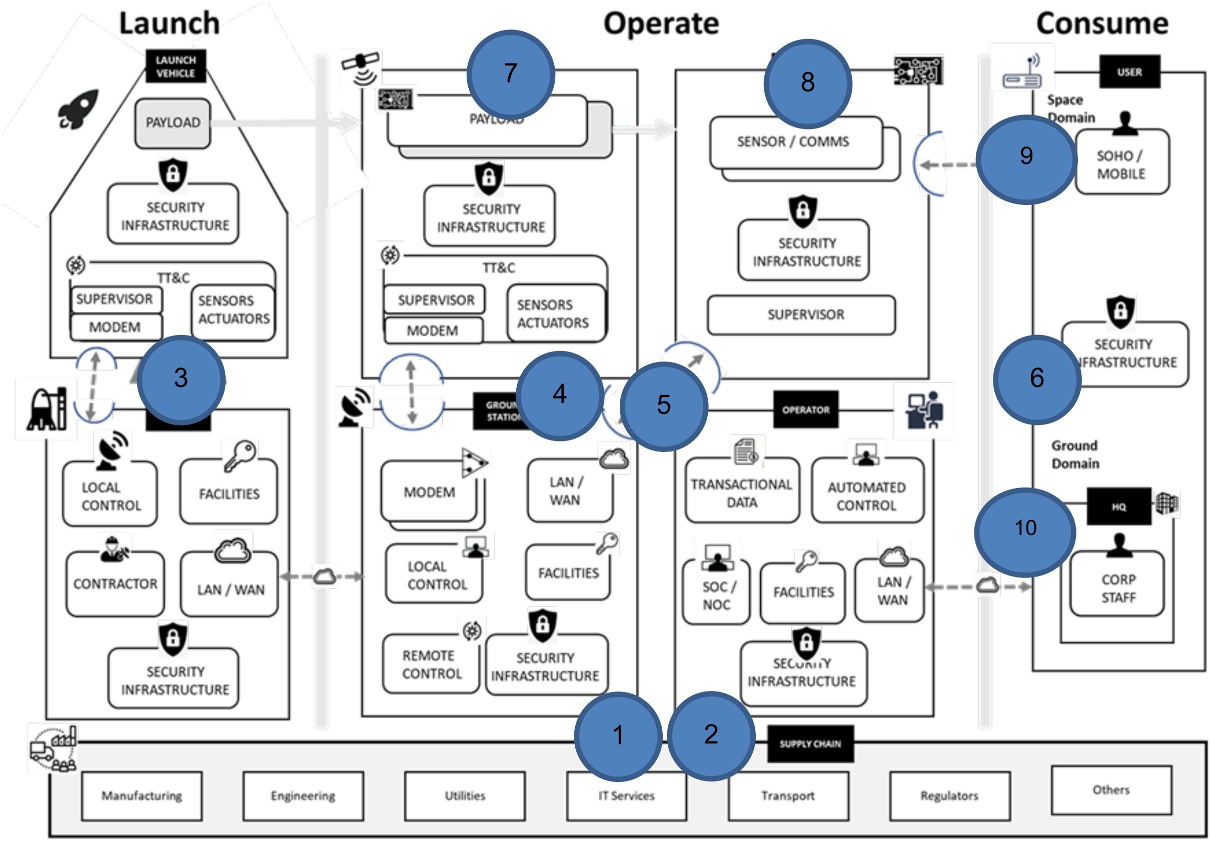
2.3 Definition of Use Cases for Australia's Space Ecosystem

When discussing the cybersecurity of space systems, it is essential to understand that the space infrastructure is only as strong as its weakest link. While the defender must protect and defend its systems from all types of attacks and threats vectors, the attacker must only find one vulnerability or entry point to launch its attack. As a result, space cybersecurity stakeholders must consider the attack surface as a whole.

In addition, whereas all cyberattacks use a specific entry point in the attack surface to enter a system, many cyberattacks are complex and may stem from various vulnerabilities, mistakes, and lack of cybersecurity in a space system's lifecycle. For instance, a cyberattack on the payload of a satellite may stem from various vulnerabilities on the attack surface such as a counterfeit component integrated in the supply chain, a software on board of the satellite, which becomes obsolete and cannot be updated by the provider, leading to unpatched vulnerabilities, as well as a lack of security measure on the ground segment, with weak credentials (passwords, login, etc).

Hence, it is important to consider all segments, including the supply chain and understand the specificities and risks related to each segment. This is particularly so for Australia as its space industry is still rather nascent and may be more prone to supply chain or foreign dependence-related risks. Taking this into account, the following sections provide an overview on the cyberthreats on each segment as well as scenarios that may be plausible on the Australian space infrastructure. Ten cases were more specifically considered for this scoping project (Figure 13).

FIGURE 16: USE CASES MAPPED IN THE SPACE CYBER ARCHITECTURE DIAGRAM



Each use case provided below was created to highlight potential policy, legal, technical, governance, and behavioural gaps in the Australian space ecosystem. None of the use cases are meant to target or implicate a specific company or country, they simply consist of scenarios that provide a good representation of the applicable legal framework based on different threat actors, types of attacks, and consequences. Some use cases are inspired from real-life attacks and vulnerabilities discovered on non-Australian space systems and transposed to the national infrastructure for a realistic and comparative analysis and investigation.

2.3.1 Use Case 1: The Software Supply Chain

General Cyber Threats on the Space Supply Chain

According to UNIDIR researchers Oleg Demidov and Giacomo Persi Paoli, the supply chain is increasingly vulnerable to cyber risks due to:[82]

- The increased complexity and globalisation of supply chains, in which companies must deal with an increasing number of direct (first tier) and indirect (second tier) suppliers. Each company's suppliers have a network of suppliers, which also have various suppliers, etc., making it very difficult for companies to map and trace their complete supply chain and properly assess the cybersecurity of all the sub-contractors and providers. Companies such as Microsoft, Cisco, Kaspersky, etc. consider cyberattacks on software in the supply chain as increasingly complex and increasingly more frequent.
- The increased cross-border interdependency of supply chain, with suppliers all over the world and within different jurisdictions with various cybersecurity practices, standards, and policies, which also poses cyber risks for companies.
- The increased digitized management of supply chains themselves with increasingly automated and digitized communications and document sharing with suppliers; supply chain management and decision-making supported by AI and Machine Learning; the availability of end-to-end organisation's supply chains online; cloud-based services and platforms that enable access to digital supply chain management ecosystem; automated warehouses and inventory management in logistics management; and supply chain risk management solutions based on Big Data.[83]

Additionally, attacks on software in the supply chain are one of the greatest cyber threats because most companies have increasingly taken cyberthreats into account and protect their systems, products, and companies, which makes the supply chain the weakest link.[84]

Cyberattacks on software component of the supply chain can take various forms such as:

- **Insertion:** adding additional information, code, software, or functionality to a system or component during the development, upgrade, or update to change the intended functions of the system.
- **Substitution:** replacing a software component with another to change the intended functions of the system.
- **Modification:** modifying the design, settings, or other information that define the system being developed, updated, or upgraded to change the intended functions of the system.[85]

In the space sector, cyberattacks on the supply chain have evolved with the emergence of New Space. Space systems used to be unique systems built for one specific client, which would define most of the design, software, and system requirements. Now that space is accessible to more actors, an increasing number of established space companies and start-ups use COTS, which may contain vulnerabilities and may be subject

[82] The supply chain can be understood as a 'system of organisations, people, technology, activities, information and resources involved in moving a product or service from supplier to customer'.
[83] Demidov, O., & Persi Paoli, G. (2020). *Supply Chain Security in the Cyber Age: Sector Trends, Current Threats and Multi-Stakeholder Responses*. UNIDIR. https://unidir.org/wp-content/uploads/2023/05/Supply-Chain-Security-in-the-Cyber-Age-UNIDIR-Report.pdf
[84] Ibid.
[85] Ibid.

to the insertion of backdoors, may be sabotaged, destroyed, or replaced with counterfeit components by malicious actors throughout the supply chain.[86] Van der Watt and Slay summarize exploitable vulnerabilities of LEO satellites that could stem from the supply chain such as COTS components, the use of old proprietary IT software, the failure or incapacity to conduct software updates to patch vulnerabilities, etc.[87] Livingstone and Lewis note that space systems frequently have a wide worldwide supply chain and may have tools for installing security and software updates, which may need remote connections and leave the system open to attack.[88]

In addition, Plotnek, who researched the cybersecurity of critical infrastructure, notes that "*a threat to the communications sector also poses a threat to space technologies due to shared systems, software, services, and supply chains between the sectors*."[89]

According to Scott Millwood, cyberattacks in the telecommunication industry almost always happen in the supply chain. For example, in 2019, Airbus suffered a series of cyberattacks which allowed attackers to access confidential data, including on military systems, by exploiting vulnerabilities in the networks of subcontractors (Rolls Royce, Expleo, etc), which were connected to Airbus' VPN network. Similarly, according to Harrison Caudill, president of the company Orbital Security Alliance, cyberattacks on the supply chain can also target the intellectual property of space companies. Space compagnies computers, including their suppliers and their subcontractors, could represent an interest for an adversary. For example, North Korea is looking to develop mature capabilities in the field of launchers but still lacks know-how and knowledge regarding launch capabilities. It could therefore target a company, which has advanced information or technologies on launchers (Arianespace for example) through a cyberattack. It would not target a space system itself, but a computer or server within the company that would have this confidential information. This information may then be used for retro-engineering.[90]

Finally, an attacker can affect the operation of a satellite or access data concerning a space system without targeting any of the software, which will end up on board the satellite or the ground station. It can exploit the vulnerabilities of 'traditional' software, which are used by most computers such as the Microsoft Office Suite or some internet browsers to enter a system or a network. This is what happened with the NotPetya attack in 2017. A group of Russian hackers, linked to Russian military intelligence (GRU), stole cyber-offensive means from the U.S. National Security Agency (NSA) and extracted a part of it containing a computer worm to then insert it into the accounting software used by all Ukrainian companies. Russia sent a system update that contained the ransomware, which was seen by users as legitimate and was therefore installed on all computers. The ransomware then spread by exploiting vulnerabilities on the Windows operating system. The NotPetya ransomware had a significant impact on businesses in Ukraine, Russia, Europe, and the United States. According to Ram Levi, it is entirely possible for this type of attack to occur in the space sector.[91]

[86] Gillette, A. (2021). *From Supply Chains to Spacecraft: Taking an Integrated Approach to Cybersecurity in Space*. Wilson Center. https://www.wilsoncenter.org/blog-post/supply-chains-spacecraft-taking-integrated-approach-cybersecurity-space

[87] Van der Watt, R., & Slay, J. (2021) *Modification of the Lockheed Martin Cyber Kill Chain (LMCKC) for cyber security breaches concerning Low Earth Orbit (LEO) Satellites*. Presented at the 16th International Conference on Cyber Warfare and Security.

[88] Livingstone, D., & Lewis, P. (2016). *Space, the Final Frontier for Cybersecurity?.* Research paper. Chatham House.

[89] Plotnek, J. (2023). *Critical National Infrastructure Supply Chain Dependencies on Space Systems and Satellite Services in the West*.

[90] Caudill, H. (2020). *Space Domain Awareness, Governance, and Security in Outer Space*. AMC Solutions. Webinar.

[91] Levi, R. (2020). *Cybersecurity of Space Assets*. SGAC Webinar.

From a legal perspective, Falco underlines that it is difficult to determine who should be operationally and financially in charge of a system's cybersecurity at different stages of the space system's lifecycle due to complex supply chains in the space sector. The intricacy of the creation, administration, utilisation, and ownership of space systems is what makes the space supply chain complex to understand. Space systems are not owned by the same entities that operate the space infrastructure, in contrast to most critical infrastructure sectors. This raises concerns about liability in the event of an attack.[92]

More recently, Boschetti et al. mention that "*supply chain attacks are less documented for the aerospace sector, where ViaSat (which took place at the beginning of the invasion of Ukraine in February 2022) appears to be the first publicly documented incidence of a supply chain security impact on space systems."*[93]

A Use Case for the Australian Supply Chain

An Australian academic institution is developing a nanosatellite for Scientific, Technology, and Education demonstration, relying on COTS components for software, firmware, and hardware. The university orders COTS for the On-Board Computer and decide to use a 220 MHz StrongARM 32-bit SA1100 RISC processor[94] manufactured by Intel, which had its own supply chain compromised. In this compromised supply chain, a software engineer has access privileges within the software development environment and inserts hidden malicious code (e.g., a logic bomb) in the processor during the testing process to prevent any detection. Intel was not able to detect the malicious code. As the nanosatellite is being developed by a university, the university did not have the technical and financial means to further test the processor to detect the malicious code either. While the malicious code does not prevent the basic operations of the nanosatellite, the On-Board Computer provides automatic control of the spacecraft, which are disabled by the malicious code.[95]

2.3.2 Use Case 2: The Hardware Supply Chain

General Cyber Threats on the Space Supply Chain

Cybersecurity risks on the hardware components of the supply chain can involve the introduction, intentional or not, of components or electronic chips that contain defects, vulnerabilities, or backdoors in order to sabotage a system or to spy on it. In many assembly lines, workers and subcontractors do not necessarily know in which system the components will be installed and whether the use will be military, dual or civilian. However, an adversary can access an assembly line with precise knowledge of the components and the final system and intentionally hide defective components, surveillance microchips, or other electronic chips containing vulnerabilities or backdoors.[96] For instance, this is what happened to the American company, Elemental Technologies, which provides the video compression software used to communicate with the International Space Station and to transfer videos taken by U.S. military drones. A microchip located on the motherboards of servers used by Elemental Technologies, which were manufactured by SuperMicro, was introduced by Chinese military personnel during the assembly of the servers in China. This attack allowed China to access data stored on these servers, which were used by the U.S. Department of Defense, U.S. Navy vessels, and the CIA, creating a major security breach. This intrusion was only discovered because this company was subjected to a security audit following a purchase offer by Amazon. Amazon needed the

[92] Falco, G. (2018). *The Vacuum of Space Cyber Security*. Presented at the 2018 American Institute of Aeronautics and Astronautics SPACE and Astronautics Forum and Exposition. https://arc.aiaa.org/doi/abs/10.2514/6.2018-5275
[93] Boschetti, N., Gordon, N.G., Falco, G. (2022). *Space Cybersecurity Lessons Learned from The ViaSat Cyberattack*. AIAA Ascend 2022. https://arc.aiaa.org/doi/10.2514/6.2022-4380
[94] Firmware is a software program or set of instructions programmed on a hardware device.
[95] Miller, J. (2013). *Supply Chain Attack Framework and Attack Patterns*. MITRE.
[96] Bailey, B. (2019). *Defending Spacecraft in the Cyber Domain*. Aerospace Corporation.

software capabilities of Elemental Technologies to respond to a Pentagon tender to provide a secure cloud service to the CIA. This example demonstrates how complex and difficult it can be to detect attacks on hardware on the supply chain.[97]

Furthermore, according to James Pavur, New Space and the proliferation of space technologies can increase cyber risks as space hardware becomes standardized and easily accessible to all (e.g., COTS, etc.). An attacker may order a COTS satellite component to analyse it and look for vulnerabilities in order to conduct a cyberattack on a space system. Discovering a vulnerability will enable the attacker to target all the systems which use this component.[98]

Moreover, cyberattacks on the hardware of space systems can come from physical access to the spacecraft in the manufacturing plant to introduce a component, sabotage a component, insert a malware on a computer in the manufacturing process by plugging an USB key (e.g., Stuxnet), etc. This type of attacks can come from human errors, insider threats, or negligence in the cybersecurity governance and cybersecurity practices of space companies. According to Harrison Caudill, physically securing the buildings of space companies would reduce the risk of cyberattacks on the supply chain by half. Most space start-ups do not physically secure their offices and do not always apply security standards.[99]

A Use Case for the Australian Supply Chain

An Australian company is relying on COTS components for some pieces of hardware. The company orders a CAN micro-controller to include in the power system to measure solar array temperatures and voltages from a trusted and known supplier. Due to supply chain delays following the COVID-19 pandemic and the shortage in semi-conductors, the company decides to change its supplier for another to keep its project on track. However, the Australian satellite company is not aware that this supplier has a less protected supply chain. As a result, a legitimate hardware was replaced by a malicious component in the supply chain by an adversary, who had access to the plant in charge of the welding and therefore had access to the micro-controller. The malicious hardware added to the micro-controller is an additional battery charge regulator, which is supposed to implement maximum-power point tracking, but instead contains a malicious software, which tells the system that is constantly overcharged when it is not. This leads the battery charge regulator, which has a temperature compensated end-of-charge voltage trigger, to be into a constant trickle-charging mode.[100] As a result, the satellite runs out of electric power and becomes inoperable, eventually ending up in an uncontrolled re-entry on a Brazilian city.

2.3.3 Use Case 3: The Launch Site and Launch Vehicle

General Cyber Threats on the Launch Site and Launch Vehicle

Cyberattacks can also target launch sites as well as launch vehicles. Most cybersecurity risks on the launch vehicles stem from vulnerabilities in COTS components, which are widely used in launchers. Cyberattacks on launchers during launch can be critical and lead to a launch failure, which may create physical damage on inhabited areas as well as impact the surrounding natural environment. Cyberattacks can also lead to

[97] Robertson, J., & Riley, M. (2018). *The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies.* Bloomberg. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

[98] Pavur, J. (2020). *Space for the IoT: Between the Race for Connectivity and Cybersecurity Concerns*. SGAC Webinar.

[99] Caudill, H. (2020). *Space Domain Awareness, Governance, and Security in Outer Space*. AMC Solutions. Webinar.

[100] Underwood, C., et al. (2001) SNAP-1: *A Low Cost Modular COTS-Based Nano-Satellite – Design, Construction, Launch and Early Operations Phase*. AIAA/USU Conference on Small Satellites. https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=1993&context=smallsat

physical damage on launchers, satellites in the nose cone, and the spaceport infrastructure, leading to additional costs, reputation risks, and physical risks for employees, etc. Additionally, cyber risks on launch sites and launch vehicles can be very specific as launchers use the same technology as missiles, which entails that launch site operators are subject to missile technology laws and non-proliferation regulations. As a result, launch site operators must protect the intellectual property of launcher companies and protect their launch and mission control centres against cyberattacks, in particular data breaches. Moreover, spaceports are usually operated jointly by a space agency and a launcher company, which may create conflicts in case of cyberattacks depending on the priorities, duties, and responsibilities of each actor.

Other international law issues arise from attacks on launchers. For instance, in August 2019, Iran failed to launch a satellite into orbit after its rocket exploded on the launch pad. Donald Trump then reacted on Twitter by posting a satellite image, probably from a military satellite, showing the launch site, accompanied by a message denying any involvement of the United States in this explosion. According to Daniel Porras, researcher at UNIDIR, cyberattacks, possibly coming from the United States, affected many tankers in the Gulf shortly before the launch. According to him, it is therefore not entirely unimaginable that the United States may have caused this explosion. Several months earlier, the New York Times published an article about a potential American program that would aim to sabotage Iranian rockets by compromising the supply chain through cyberattacks.[101] Similarly, in 2019, the United Arab Emirates failed to launch a spy satellite. Speculation about the possible conduct of cyberattacks by Iran to prevent the launch emerged following the event. If these two scenarios are true, it would mean that there was potentially an intention to prevent a country from accessing space. However, according to the Outer Space Treaty, all states have the right to access and use outer space and this type of attack, if verified, could constitute a violation of this treaty. While there are only speculations to date, these two examples deserve to be studied and clearly show the complexity of the interdependencies between space and cyberspace as well as the difficulty to regulate them to secure space systems.

A Use Case for the Australian Launch Site

Australia is developing launch sites in Abbot Point (North Queensland), Nhulunbuy (Northern Territory), and at Whalers Way Orbital Launch Complex (Eyre Peninsula).[102] Australia does not have mature launcher capabilities and mostly launches foreign rockets from its soil.

Australia signs a contract with a new U.S. launcher company to launch a Japanese satellite. In this context, the Australian spaceport in the Eyre Peninsula welcomes staff from both the American and Japanese companies for the launch. The foreign staff is staying in a hotel near the launch site. As the launch is being delayed because of the weather, which is common, the foreign staff work remotely from the hotel and use the hotel's Wi-Fi.

An Iranian state-sponsored group knows that foreign staff which come to the launch site always stay at the same hotel. As a result, they target the hotel's Wi-Fi to launch a sophisticated attack. The attackers send a malicious email to the hotel's reception, which appears to be a reservation from a well-known hotel booking website. The receptionist clicks on the emails, which downloads a backdoor and installs it. The attackers are then able to access the Wi-Fi network of the hotel and can launch attacks on computers and smartphones connected to the hotel's Wi-Fi network. They use the open-source Responder tool to listen for MBT-NS (UDP/137) broadcasts from devices that are attempting to connect to the Wi-Fi network and collect

[101] Sanger, S. & Broad, W. (2019). *U.S. Revives Secret Program To Sabotage Iranian Missiles And Rockets*. New York Times. https://www.nytimes.com/2019/02/13/us/politics/iran-missile-launch-failures.html; Karimi, N., & Gambrell, J. (2019). *Iran Acknowledges Rocket Explosion, Says Test Malfunctioned.* Military Times. https://www.militarytimes.com/news/pentagon-congress/2019/09/02/iran-acknowledges-rocket-explosion-says-test-malfunctioned/

[102] Aliberti, M., et al. (2020). *Emerging Spacefaring Nations*. European Space Policy Institute.

credentials (login and passwords). The attackers gain access to the laptops of both an employee from the U.S. launcher company and an employee from the Japanese satellite operator.[103] When the launch is about to take place, the two employees travel to the launch site with their laptops and connect to the Wi-Fi of the Launch Control Centre without any prior cybersecurity check on their computers. As a result, the attackers gain access to the Control Centre's Wi-Fi network and capture all the traffic on the network, including launch tests procedures, revealing some information about the components and systems of the rocket. The attack is detected by the Control Centre, which leads to the interruption of all activities on site, launch delays, additional costs as well as an investigation by the U.S. Department of Justice for potentially violating U.S. export control laws on missile technology. The company is therefore accused of missile proliferation, which affects its reputation and financial stability due to legal costs.

2.3.4 Use Case 4: The Ground Segment

General Cyber Threats on the Ground Segment

According to Michael Krepon, president of the Stimson Center, cyberattacks on the ground segment are more likely than those aimed directly at the space segment.[104] The ground segment enables command, control, and management of satellites (e.g., their position, the position of their solar panels and instruments, sending and receiving data; etc.). As long as these systems are connected, they can be targeted by cyberattacks. Both the uplink and downlink may be targeted by cyberattack as well as the link between the ground station and the control centre.[105] Moreover, ground stations are increasingly digitalized[106] and generally use common software and operating systems such as Linux or Unix, which can be victims of traditional cyberattacks that are not specifically programmed to target a particular space system, thereby increasing the likelihood of an attack.[107]

According to Manulis, et al., compromising a ground station is the easiest way to take control of a satellite. Cyberattacks on the ground segment are generally the same as during a satellite's life cycle such as:

- Physical attacks, including compromising physical security measures, and gaining unauthorized access to a ground station and other physical IT assets.
- An attacker is able to compromise the network to which a ground station is connected to.
- Cloud infrastructure currently powers majority of the computing framework in the ground station. As a result, failure of the cloud infrastructure could have catastrophic effect on the ground station including denial of service (DoS) for the satellite receiver.
- Corruption of data on the ground segment.
- Supply chain attacks on ground systems.
- Unpatched vulnerabilities on ground stations.[108]

According to NATO's Joint Air Power Competence Centre (JAPCC), most cyberattacks against satellite ground stations exploit vulnerabilities on the Internet and directly target the staff of ground stations to push them to click on links or download malware on computers that control the ground stations (e.g., social

[103] SpamTitan. (2017). *NSA Exploit Used in Cyberattacks on Hotel WiFi Networks*. https://www.spamtitan.com/blog/nsa-exploit-cyberattacks-on-hotel-wifi-networks/

[104] Becht, O., & Trompille, S. (2019). *Rapport d'information sur le secteur spatial de défense*. Assemblée Nationale, p.83

[105] Shadbolt, L. (2021). *Satellite Cyberattacks and Security. Technical Study.* HDI. https://www.hdi-specialty.com/downloads/_Global/HDIS209_Satellite%20Cyberattack_whitepaper_V8_05JULY21.pdf

[106] Becht, O., & Trompille, S. (2019). op cit, p.41

[107] Rives, A. (2019). Sécurité Des Liaisons Satellites. CEIS.

[108] Manulis, M., et al. (2020). *Cybersecurity in New Space*. Springer.

engineering). This type of attack can enable the attacker to access the satellite controlled by the ground station as the JAPCC also considers that most cyber risks on the space segment derive from the exploitation of vulnerabilities on ground stations and receivers on Earth.[109] For instance, in 2007 and 2008, a cyberattack hit the U.S. remote sensing satellite Landsat-7 using an entry point on a ground station in Norway, resulting in 12 minutes of interference in both attacks. Even though the attackers did not take control of the satellite, they managed to reach the command-and-control functions of the satellite.[110]

According to Jacob Oakley, an attacker can target the ground stations, send commands to the satellite, and potentially access the satellite itself. If an attacker has access to the satellite and the ground station, then they can delete or modify the satellite's encryption keys. If the attack is not detected in time by the operators, the satellite may no longer be able to communicate with its ground station, the attacker then becoming the only stakeholder capable of controlling the satellite.[111]

A Use Case for the Australian Ground Segment

Australia's space industry has mature capabilities in the manufacture of ground systems and has many ground stations on its soil, which could be the target of cyberattacks. A zero-day vulnerability in the Telemetry, Tracking; Commanding and Monitoring (TTCM) subsystem of an Australian SATCOM ground station located in Adelaide is exploited by a Russian hacker group. The TTCM enables them to control and monitor the satellite's functions from the ground. The telemetry protocol used by the subsystem contains a vulnerability, which does not implement encryption correctly, enabling the attackers with adjacent short-range access to the ground station to intercept the data, which is in clear text. In addition, the telecommunication satellite, to which the ground station sends commands, is used for telemedicine purposes, which includes personal data and health data. This type of data can then be sold online on the dark net to the highest bidder, resulting in a massive personal data breach because of a vulnerability in a SATCOM ground station, affecting credibility and bankrupting the business.

2.3.5 Use Case 5: The Ground Space Situational Awareness Infrastructure

General Cyber Threats on the SSA Ground Infrastructure

The Space Situational Awareness (SSA) infrastructure spreads over different segments. It comprises the user segment with SSA services, which provide e.g., Space Surveillance and Tracking (SST) or Space Weather data to satellite operators; the ground segment with optical telescopes, radars, and antenna on Earth; and the space segment with SSA instruments on-board of satellites.

On the ground segment, radio frequency of SSA radars can be intercepted. However, the reception of radar signals often needs GPS synchronisation, which makes it more difficult to intercept the signal.[112] In addition, radars are also increasingly digitalised, which can make them vulnerable to cyberattacks.

A Use Case for the Australian SSA Ground Infrastructure

A hacktivist from an environmental group manages to highjack the link between a commercial SSA radar located in Australia and a control centre to protest the set-up of the radar near a protected natural area. The environmental group believes that the radiofrequency may harm the natural environment. The hacktivist convinces a frustrated employee of the SSA company of his cause. The employee provides the environmental group with his access credentials (login and passwords) to the control centre, which controls

[109] Baram, G., & Wechsler, O. (2020). *Cyber Threats to Space Systems*. JAPCC. https://www.japcc.org/cyber-threats-to-space-systems/
[110] Rajagopalan, R.P. (2019). *Electronic and Cyber Warfare in Outer Space*. Space Dossier 3. UNIDIR.
[111] Oakley, J. G. (2020). *Cybersecurity for Space: Protecting the Final Frontier*. Apress L. P. p.59
[112] Becht, O., & Trompille, S. (2019). op cit.

the radar. The hacktivist then takes control of the control centre, resetting the password and removing access for other users, making him the only stakeholder with access to the radar. He then shuts down the radar, which leads to a loss of data in SSA for several Australian operators and delays in processing collision alerts as operators must procure additional data elsewhere (e.g., space-track). One collision alert between an Australian LEO satellite and a 50 cm piece of debris is not processed in time and not enough data is available to decide whether to conduct a manoeuvre. As a result, the LEO satellite collides with the debris, destroying a 2-million AUD satellite.

2.3.6 Use Case 6: The Space Situational Awareness User Infrastructure

General Cyber Threats on the SSA User Infrastructure

On the user segment, SSA data and infrastructures are also vulnerable to cyberattacks, including data theft, data modification, intrusion in SSA data repositories, falsification of SSA data, deletion of SSA data, denial of service, etc.

An attacker may enter a public SSA data repository to falsify data, which an informational risk. On the one hand, the biggest risk may be on data repositories, to which several stakeholders contribute. As a result, the number of entry points for attackers increases and each contributor to the SSA data repository can be targeted by cyberattacks (hacking; phishing, etc.), which aim at retrieving their credentials, access the database, and falsify or delete data without being detected. This risk will increase with the rise of private SSA companies, which contribute to national databases. On the other hand, the emergence of public SSA repositories can also improve the confidentiality, availability, and integrity of databases as more of the same data is being integrated in the repository, enabling to compare data and assess the accuracy and integrity of data sets against potential manipulations. The increase in data about each system (velocity, size, position, trajectory, etc.) from various users can improve the quality of SSA and render malicious modifications more difficult as more data sets from more contributors would have to be modified by the attacker to deceive operators.

Moreover, public databases can also lead to influence operations (information warfare) to manipulate public opinion. SSA data may be used or manipulated to scare the population regarding the risk of the Kessler syndrome; or used to conduct disinformation campaigns regarding the space operations of another country.

Furthermore, collision alerts mechanisms and systems, or the lack thereof, can also be targeted by cyberattacks. For instance, in 2019, there was a collision risk between the ESA Aeolus satellite and a Starlink satellite. The management of this collision was conducted through simple emails between ESA and SpaceX, raising cybersecurity risks. There is no protocol or dedicated platform with a strict procedure to share collision alerts between operators.[113] This lack of dedicated system for collision alerts and manoeuvres can be exploited by malicious actors by simply targeting email accounts to send illegitimate collision alerts emails to cause useless or dangerous manoeuvres that may lead to an actual collision or send an overwhelming number of illegitimate emails to cause a DoS. It is also important to note that in the ESA-Starlink case, SpaceX explained that their alert system did not properly function and prevented from reading the emails sent by ESA although there was no cyberattack.

A Use case for the Australian SSA User Infrastructure

Australia is reliant on SSA data from the United States' repository space-track.org. Russia decides to launch an ASAT test. In parallel, North Korean hackers decide to launch a DDoS cyberattack on the website of space-track.org by overwhelming the website with millions of illegitimate requests. To do so, North Korean

[113] Moranta, S., et al. (2020). *Towards a European Approach to Space Traffic Management.* ESPI Report 71. p.13

hackers hack millions of traditional computers in Southeast Asia and Africa to turn them into zombie bots to use them to send requests to space-track.org, rendering the website inaccessible. Therefore, the U.S. must share SSA data with Australia in another way, delaying Australia's capacity to monitor the effects and threats of the ASAT test on its satellites, leading to a collision between a satellite and debris.

2.3.7 Use Case 7: The Space Segment

General Cyber Threats on the Space Segment

According to Brandon Bailey, the cybersecurity of space systems has long focused solely on electronic attacks such as jamming and spoofing as well as on the ground segment and not on the space segment because satellites were not perceived as hackable devices for several reasons:

- Satellites were built using unique hardware and software components, which were not perceived as susceptible to traditional cyberattacks,
- Satellites were not perceived as vulnerable to cyberattacks due to their physical distance from Earth,
- Satellites were not connected to the Internet and contained little software components,
- Satellites were mostly manufactured by defence companies, which applied strict security measures in the entire satellite's lifecycle,
- Encrypted military satellites were perceived as hack-proof.[114]

However, satellites are increasingly digitized, interconnected, linked to the Internet or an intranet network, their distance from the earth does not make them less vulnerable and the encryption keys can be decrypted. According to the Secure World Foundation, many Nations-States are developing cyber offensive capabilities that could be used against space systems and many non-state actors are actively trying to find cyber vulnerabilities on satellites that are similar in nature to those found on traditional computers on Earth.[115] The space segment is therefore as vulnerable to cyberattacks as the ground segment.

While most researchers agree that military satellites are more or less well protected, this is not the case of commercial satellites.[116] According to UNIDIR Researcher Laetitia Zarkan, a cyberattack against a commercial satellite can be potentially more dangerous than a cyberattack against a military satellite since military systems are generally more secure and military satellite operators are used to being attacked and even expect to be. As a result, there is a better chance that they know how to react to an attack, which is not always the case in the commercial sector.[117] However, governments are increasingly using commercial solutions. For instance, in the U.S., 80% of the needs in bandwidth come from commercial telecommunication satellites. As a result, cyberattacks against commercial satellites can have consequences on military operations.

Overall, New Space bring new and additional cyber risks on the space segment. Regarding satellite constellations, new cyber risks arise as software and hardware are usually identical for all the satellites of the constellation, which increases the surface of attack and put the entire constellation at risk. Should an

[114] Bailey, B. (2019). *Defending Spacecraft in the Cyber Domain*. Aerospace Corporation.
[115] Weeden, B., & Samson, V. (2020). *Global Counterspace Capabilities: An Open Source Assessment*. Secure World Foundation.
[116] The Economist. (2019). *Attacking Satellites is Increasingly Attractive—And Dangerous*. https://www.economist.com/briefing/2019/07/18/attacking-satellites-is-increasingly-attractive-and-dangerous; Bailey, B. (2019). *Defending Spacecraft in the Cyber Domain*. Aerospace Corporation.
[117] Zarkan, L. (2020). *Space Domain Awareness, Governance and Security in Outer Space*. AMC Solutions. Webinar.

attacker discover one vulnerability on one satellite, it may enable the attacker to target all the satellites of the constellation.

A Use Case for the Australian Space Segment

Considering that Australia mostly has GEO communications satellites, a hacker buys a commercial satellite dish (the one found on the roof of private individuals who have a satellite TV subscription); a DVB board (a circuit board for watching satellite TV on a computer), which costs around $300; a COTS software that allows to search for satellite signals (e.g., EPS Pro) to try to intercept communications' satellites data from Very Small Aperture Terminals (VSAT), which are very present in Australia and used by both commercial and government stakeholders. Then, through Open-Source Intelligence technics, this hacker assembles various information that are readily available on the internet such as the spectrum and radiofrequency bands used by Australian communication satellites, their payloads, and ground stations, as well as their precise positions in orbit.[118] Furthermore, VSAT are using standardized protocols worldwide, which are information available on the internet. The standardisation protocols used for VSAT are the DVB-S and the GSE protocols, which are open-source standards. Then, this hacker writes an algorithm that understands these standards and can find IP data packets to capture. As the communication satellites are not properly encrypted, this method enables the hacker to intercept critical information from users as all the data is in clear text.

This scenario is not far-fetched as it is inspired by true events from an experiment conducted by James Pavur, who used this technique to analyse more than 18 communication satellites and managed to collect up to one terabyte of data in one week. Intercepted data included critical information such as passport data and immigration data from the crew of cargo vessels, credential of personal email accounts, health information, and other data in clear text. This type of personal information can also be further used to create phishing attacks that target staff that work in the space sector.[119]

It could be assumed that now that this type of attack is known, commercial companies would apply the proper cybersecurity protocols and standards. However, this type of attack seems persistent since similar methods of satellite eavesdropping had already been presented at the BlackHat conference in 2009 and 2010.[120] A similar method was also used for about 8 years by the group of Russian hackers Turla APT, which succeeded in gathering sensitive diplomatic and military data from European states and the United States by exploiting IP addresses from broadband satellites, which were not properly encrypted.[121] However, this case does not seem to have been a black swan event and pushed satellite companies to improve cybersecurity.

2.3.8 Use Case 8: The Space Segment (The Payload)

General Cyber Threats on the Payload

According to Jacob Oakley, with the emergence of new State and non-State actors, there are many instances in which one organisation owns and operate the satellite bus and another organisation owns and operate the payload on board of the satellite. As a result, one organisation, one organisation's ground station may track and send commands to the satellite bus and another organisation's ground station may send commands to the payload. This situation raises cybersecurity risks as the two organisations may implement different cybersecurity protocols and standards, and a cyberattack on the payload may affect the bus and

[118] Optus Yes. (2013). *C1 Satellite Payload Information*. https://www.optus.com.au/content/dam/optus/documents/about-us/our-network/Optus_C1_Payload.pdf
[119] Pavur, J. (2020). *Space for the IoT: Between the Race for Connectivity and Cybersecurity Concerns*. SGAC Webinar.
[120] Paganini, P. (2013). *Hacking Satellites… Look Up To The Sky*. Infosecinstitute.com. https://resources.infosecinstitute.com/hacking-satellite-look-up-to-the-sky/
[121] West, J. (2019). *Space Security Index 2019.* Project Ploughshares. p.113

vice versa.[122] This risk usually arises from a lack of containers and logical separation between the satellite bus and the payload software and network environments, which would prevent cyberattacks on the bus to spread to the payload. This situation raises policy questions regarding the legal responsibility of each stakeholder in case of an attack.

Furthermore, with the digitalisation of satellites, software defined radios (SDRs) have replaced hardware equipment such as modulators, demodulators, and antennas. Software defined radios are reprogrammable and reconfigurable software, which enable digital signal processing to adjust frequencies, coverage, and bandwidth. Software defined radios are computer systems, and therefore are vulnerable to cyberattacks.[123]

A Use Case for the Australian Space Segment

An attacker from a state-sponsored hacker group finds protocol vulnerabilities in software defined radios. This vulnerability is not patched on the SDR of a commercial customer hosted on an Australia communication satellite and therefore can be exploited. The attacker uses this vulnerability to enter the SDR and infect it with malicious code without being detected. The code aims at making the SDR believe that the frequencies are correct when it should adjust them to establish communication with the ground station. As a result, the SDR stays on the same frequency and cannot communicate with the ground segment anymore, resulting in a denial of access. In addition, the fact that the SDR stays on this same frequency also creates interference with other satellites. The ground station cannot communicate with its satellite but instead send signals, which are received by the neighbouring satellites, creating confusion for all operators.[124] Consequently, the SATCOM service is interrupted for end-users, which lose access to satellite television services.

2.3.9 Use Case 9: The User Segment (Services)

General Cyber Threats on the User Segment

End-user services based on Earth Observation, satellite communications, or GNSS can also be affected by cyberattacks. Cyberattacks on the user segment are rising with the emergence of downstream applications and space-based data web portals. End-users can now access space-based data and space systems through software and web portals, extending the attack surface to the user segment. These risks are similar to cyber threats on traditional computers on Earth and not necessarily specific to the space sector. However, an access to these systems may enable a malicious actor to gain access to a space system or space-based data, in particular when these end users solutions support on-demand service, send commands to the satellite, or enable payload reconfiguration. For instance, the emergence of the 'as-a-service' business model, which enable satellite operators or end-users to send commands to a satellite through a cloud-based environment, can increase cyber risks. For instance, attackers can buy services such as AWS Ground Station to access the system and look for vulnerabilities to exploit.[125]

Cyber risks on end user services, in particular downstream applications, software, and web portals, often stem from vulnerable authentication and authorisation controls.[126]

A Use Case for the Australian User Segment

Cyber risks can also be seen from the perspective of reliance on foreign systems and services. A DoS can result from an interruption of service by a foreign software or system provider if the interests of Australia or

[122] Oakley, J. G. (2020). *Cybersecurity for Space: Protecting the Final Frontier*. Apress L. P. p.111
[123] Ibid. p.60
[124] Ibid.
[125] Pavur, J. (2020). *Space for the IoT: Between the Race for Connectivity and Cybersecurity Concerns*. SGAC Webinar.
[126] Manulis, M., et al. (2020). *Cybersecurity in New Space*. Springer.

an Australian company and a foreign country or company no longer align. For instance, GNSS such as GPS, GLONASS, or Beidou can be interrupted at any time by the service provider.

Australia does not possess its own GNSS. Nonetheless funding is allocated to PNT infrastructures and downstream application. Navigation data mostly come from the U.S. GPS, but Australia also uses data from Galileo (EU), GLONASS (Russia), Beidou (China), and two regional systems, the QZSS (Japan), and NAVIC (India).[127] Following the Russian invasion of Ukraine, Australia decided to impose sanctions on Russia. In retaliation, Russia decided to cut the GLONASS signal for Australian users. This could be seen as a 'cyberattack' through intentional denial of service from the provider. As a result, the decision affects any system or service relying on GLONASS, which is critical with the emergence of the Internet of Things, autonomous cars, connected and smart manufacturing, and other applications which rely on GNSS.

2.3.10 Use case 10: The User Segment (Terminals)

General Cyber Threats on the User Segment

Cyberattacks can also target user terminals such as SATCOM internet modems, Broadband Global Area Network (BGAN) portable terminals, BGAN Machine to Machine (M2M), FleetBroadband (FB), or SwiftBroadband. User terminals are particularly vulnerable to DNS usurpation, TCP/IP session theft, GRE protocol attacks, etc.[128]

In 2014, the cybersecurity company IOActive scanned Inmarsat and Iridium BGAN terminals and discovered many vulnerabilities such as hardcoded credentials, undocumented and/or insecure protocols, and weak encryption algorithms, which allowed an attacker to intercept, manipulate, or block communications, and in some cases, to remotely take control of the terminals. A cyberattack could have critical consequences as BGAN terminals are often used by the military on the battlefield as well as civil security and disaster management organisations. For instance, IOActive discovered vulnerabilities on land portable and land mobile Harris BGAN terminals, which are used for tactical radio network capabilities. These vulnerabilities would allow an attacker to inject malicious code to install a malware on a laptop connected to the terminal that would retrieve geolocation data from the built-in GPS to determine where the soldiers are located, putting the troops at risk of kinetic attacks as well as impacting their ability to communicate with their commanders. The vulnerabilities discovered by IOActive were patched.[129] However, it does not mean that other unknown vulnerabilities exist on these systems.

A Use Case for the Australian User Segment

An Australian satellite communication company is providing internet broadband to users. Users connect to the satellite broadband through a router provided by the company. The router uses the TR-069 remote management protocol to enable the satellite company to remotely update the routers of all its customers and perform diagnostics as well as other remote tasks. However, this protocol has software vulnerabilities, which are exploited by several criminal groups. The satellite company did not set up the router to use HTTPS and simply kept the use of HTTP between its Access Control Service (ACS) and the users' satellite routers. Additionally, the software used by the company's ACS to enable the remote management of their customers' TR-069-enabled routers contains vulnerabilities, enabling several remote code executions. As a result, the criminal groups retrieve all the internet traffic of the customers, which is in clear text, and contains bank

[127] Aliberti, M., et al. (2020). Emerging Spacefaring Nations. European Space Policy Institute; Expert Reference Group for the Review. (2018). *Review of Australia´s Space Industry Capability*. Australian Space Agency.
[128] Rives, A. (2019). *Sécurité Des Liaisons Satellites Observatoire du monde cybernétique.* CEIS.
[129] Ruben, S. (2014). *A Wake-Up Call for SATCOM Security*. IOActive. https://ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf

account credentials and credit card numbers used for online shopping, enabling them to steal money. Following this attack, the company's reputation is damaged, and all the routers must be replaced as the company did not enable end-users to access the management settings of the routers to disable the TR-069 protocol, leading to additional costs.[130]

[130] Jackson, M. (2014). *Millions of Routers Supplied by Broadband ISPs Vulnerable to TR-069 Hackers*. ISP Review. https://www.ispreview.co.uk/index.php/2014/08/routers-supplied-broadband-isps-vulnerable-tr-069-hackers.html

A Policy and Legal Analysis of the Use Cases

3.1 Australia's Governance, Policy, and Legal Frameworks

This section provides an overview of the governance framework set up at Commonwealth level to deal with cybersecurity issues and of the relationship between Australia's legal and policy framework and the governmental actors that operate such framework.

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. Of course, these positions are not necessarily static, but have relative mobility.

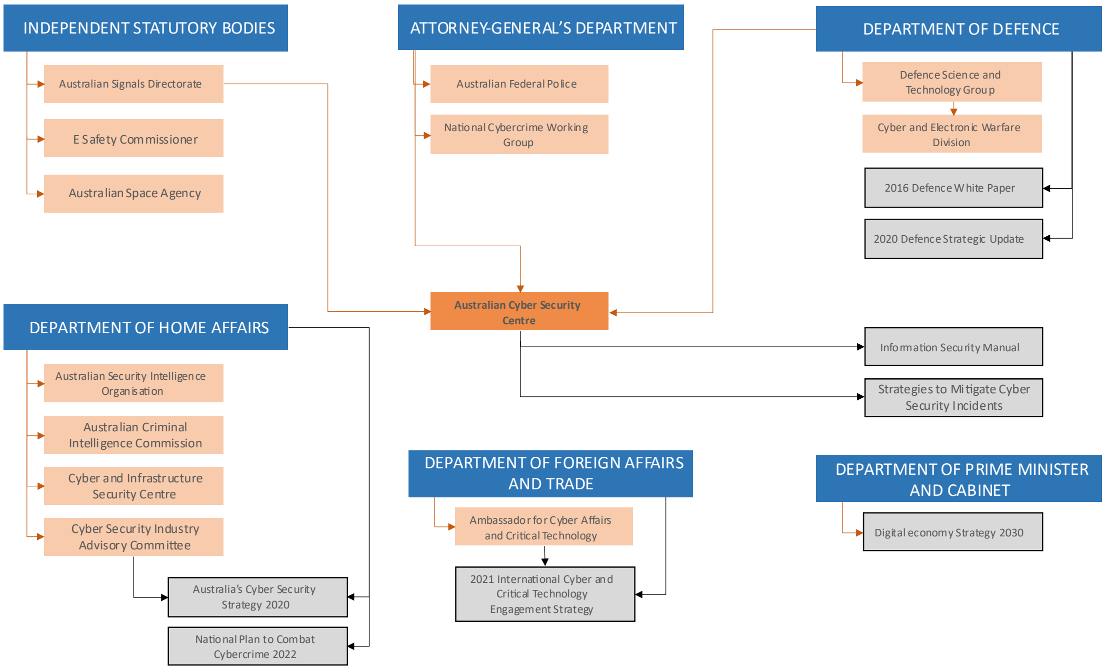
In Section 3.1.1 we more specifically cover the top-level governmental structures at Commonwealth level and describe their main responsibilities. We identify key stakeholders, their relationship, and competences in the space cyber domain.

In Section 3.1.2, we analyse the most important policy documents and implementation frameworks. We review those 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.

In Section 3.1.3 we analyse relevant legislation at both domestic level (e.g., the Cybercrime Legislation Amendment Act of 2012, the Privacy Amendment Act of 2017, the Telecommunications and Other Legislation Amendment Act of 2017, etc.) and international level (e.g., the UN Charter, the Outer Space Treaty, ITU Convention, the Budapest Convention, etc.).

3.1.1 Organisational Setting

FIGURE 17: RELEVANT ORGANISATIONS AND POLICIES IN THE SPACE CYBER FRAMEWORK OF AUSTRALIA (SOURCE: AUTHORS' VISUALISATION)


INDEPENDENT STATUTORY BODIES
Australian Signals Directorate
E Safety Commissioner
Australian Space Agency
ATTORNEY-GENERAL'S DEPARTMENT
Australian Federal Police
National Cybercrime Working Group
DEPARTMENT OF DEFENCE
Defence Science and Technology Group
Cyber and Electronic Warfare Division
2016 Defence White Paper
2020 Defence Strategic Update
Australian Cyber Security Centre
Information Security Manual
Strategies to Mitigate Cyber Security Incidents
DEPARTMENT OF HOME AFFAIRS
Australian Security Intelligence Organisation
Australian Criminal Intelligence Commission
Cyber and Infrastructure Security Centre
Cyber Security Industry Advisory Committee
Australia's Cyber Security Strategy 2020
National Plan to Combat Cybercrime 2022
DEPARTMENT OF FOREIGN AFFAIRS AND TRADE
Ambassador for Cyber Affairs and Critical Technology
2021 International Cyber and Critical Technology Engagement Strategy
DEPARTMENT OF PRIME MINISTER AND CABINET
Digital economy Strategy 2030

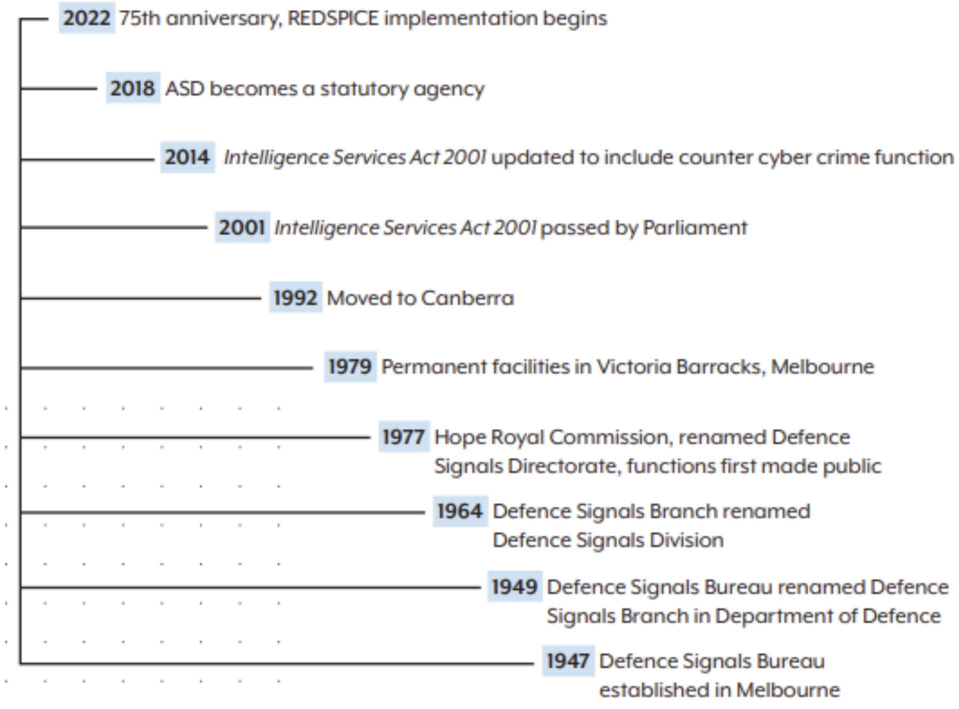
Cybersecurity in Australia is handled by different government departments and agencies, each operating based on their specific mandate. The main departments are the Attorney General's Department, the Department of Defence, the Department of Home Affairs, the Department of Foreign Affairs and Trade and the Department of the Prime Minister and Cabinet. Independent statutory bodies such as the Australian Signals Directorate also play a pivotal role. An introductory overview of the main organisations and the relative policies/implementation frameworks is provided above.

A specific feature of Australia's organisational setting has been the 'co-location' of agencies as a means 'to achieve the benefits of a single-agency approach, without significantly changing the existing machinery of government'.[131] As more broadly highlighted by Nevill, 'the Australian government has largely resisted the impulse to form new cybersecurity policy and operational bodies, instead modifying existing structures to manage cybersecurity threats. Adjustments to the machinery of government have been made, but the pre-existing government departments have retained their own identities, budgets, and chains of command'.[132]

Australian Signals Directorate and the Australian Cyber Security Centre

The Australian Signals Directorate (ASD) is an independent statuary body, working across the full spectrum of operations required to support the Australian Government and Australian Defence Force (ADF), including intelligence, cybersecurity, and offensive signals operations. The story of the ASD goes back to World War II, with the formation of the Central Bureau in 1942.[133] Since then, it changed name many times,[134] having expanded its role in 1986 to include government computer security, which would later evolve into its cybersecurity mission.[135]

FIGURE 18: AUSTRALIA'S SIGNAL DIRECTORATE EVOLUTION OVER TIME (SOURCE: ASD)


2022 75th anniversary, REDSPICE implementation begins
2018 ASD becomes a statutory agency
2014 *Intelligence Services Act 2001* updated to include counter cyber crime function
2001 *Intelligence Services Act 2001* passed by Parliament
1992 Moved to Canberra
1979 Permanent facilities in Victoria Barracks, Melbourne
1977 Hope Royal Commission, renamed Defence Signals Directorate, functions first made public
1964 Defence Signals Branch renamed Defence Signals Division
1949 Defence Signals Bureau renamed Defence Signals Branch in Department of Defence
1947 Defence Signals Bureau established in Melbourne

[131] Nevill, L. (2018). *Cyber Security Governance in Australia*. Centre for International Governance Innovation.
[132] Ibid.
[133] Australian Signals Directorate. (n.d.) *Central Bureau formed*. Australian Government. https://www.asd.gov.au/75th-anniversary/timeline/173-1942-central-bureau-formed
[134] Ibid.
[135] Ibid.

The ASD became a Statutory Agency, separated from DoD in 2018, with the Australian Cyber Security Centre (ACSC) as an integral part of its constitution (see further).[136] This change was brought by the Intelligence Services Amendment (Establishment of the Australian Signals Directorate) Bill 2018.

ASD activities are legitimated by the Intelligence Services Act 2001,[137] which discriminated its functions, establishment, and role of its Director-General. The Act also stipulates ASD's main functions, which are:[138]

- Collect and communicate foreign signals intelligence
- Prevent and dismantle offshore cyber-enabled crime
- Present cybersecurity advice and assistance to Australian governments, businesses, and individuals
- Support military operations
- Protect the specialised tools ASD uses to achieve its functions
- Cooperate with and assist the national security community's performance of its roles.

According to the agency's Annual Report 2020-2021, its purpose is to defend Australia against global threats and advance national interests through the provision of foreign signals intelligence, cybersecurity, and offensive cyber operations. To do this, ASD masters technology and its application to inform (signals intelligence), defend (cybersecurity) and generate effects (offensive cyber operations).[139] Underpinning ASD's purpose is five strategic objectives:[140]

- Provide strategic advantage for Australia by supplying intelligence to protect and advance national interests
- Lead in cybersecurity, making Australia the safest online environment, and promote national cybersecurity resilience
- Support military operations and protect DoD personnel and assets
- Counter cyber-enabled threats, protecting Australia by countering cyber-enabled crime and disrupting terrorists' use of the internet
- Deliver trusted advice and expertise, delivering timely, quality advice to government, law enforcement, businesses and the community.

Even though the ASD focuses on the protection of Australians through defensive cyber capabilities, it is important to point out that offensive cyber capabilities have been used to counter offshore threats, including the dismantling of online infrastructure used by foreign cybercriminals targeting Australians during the COVID-19 pandemic.[141]

[136] The Intelligence Services Amendment (Establishment of the Australian Signals Directorate) Bill 2018, which implements the recommendations of the review, was given Royal Assent and passed into law on 11 April 2018. Consequently, ASD became a statutory agency in the Defence portfolio on 1 July 2018.
[137] Federal Register of Legislation. (2001). *Intelligence Services Act 2001*. https://www.legislation.gov.au/Details/C2022C00014
[138] Section 7 of the Intelligence Services Act 2001.
[139] Australian Government. (2020). *Australian Signals Directorate Annual Report 2020-2021*. https://www.transparency.gov.au/annual-reports/australian-signals-directorate/reporting-year/2020-21-41
[140] Ibid.
[141] Ibid.

REDSPICE: An Initiative to Increase ASD's Capabilities

In 2022, REDSPICE (Resilience, Effects, Defence, Space, Intelligence, Cyber, Enablers) was established as an initiative to transform the ASD and increase its capabilities. To face new threats in the strategic environment, the ASD announced it will invest $9.9 billion in intelligence and cyber capabilities.

Measures include growing and delivering asymmetric strike capabilities and offensive cyber for the ADF; enabling next-generation data science and artificial intelligence (AI) capabilities; hardening networks against cyberattacks with sharpened response capability; enhancing intelligence capabilities; improving core ASD resilience by bolstering national and international footprint; providing opportunities for Australian industry, including cyber, ICT, cloud computing and enabling services.

While REDSPICE covers both space and cyberspace, there are no specific measures dedicated to space cybersecurity. However, measures focus on improving the resilience of critical infrastructures against sophisticated cyberattacks, which includes space. REDSPICE also aims to increase the visibility of threats to critical systems and create redundancy in critical capabilities through national and international dispersal.[142]

In addition, as part of REDSPICE, the **Critical Infrastructure Uplift Program (CI-UP)** was established to enhance the cyber resilience of Australia's critical infrastructure, including space. It aims to: (1) assist ACSC's Partners that own or operate critical infrastructure or Systems of National Significance (SoNS) to better understand and improve their cybersecurity maturity; (2) deliver a set of prioritised vulnerability and risk mitigation recommendations to assist Partners to plan and implement these recommendations; (3) increase the visibility of threats to Australia's most critical systems, with a focus on Operational Technology (OT) and IT/OT convergence points; and (4) connect Partners to other ACSC Services.

The Program can provide operators with cybersecurity posture assessments, cybersecurity technical validation, cyber threat hunt, tabletop exercises, threat briefings; and CI-UP Reporting and Debrief. ACSC also provides operators a self-assessment tool so that they can assess their level of cybersecurity on their own.[143] However, it is not necessarily clear how and to what extent space operators are benefiting from this program and whether activities and solutions are adapted to the orbital environment.

The Australian Cyber Security Centre (ACSC), in turn, leads the Australian Government's efforts on national cybersecurity. While formally part of ASD, the ASCS is also closely linked with both the Department of Defence and Department of Attorney General, since the ACSC is a joint responsibility of the Attorney-General and Minister for Defence.[144] Staff from Department of Home Affairs, AFP, ASIO, ACIC, ADF and the Defence Intelligence Organisation are also co-located at ACSC.

The ACSC thus brings together cybersecurity capabilities from across the Australian Government to improve domestic cyber resilience,[145] helping to create a safer online environment as a hub for private and public sector collaboration and information-sharing, providing advice and assistance across the whole economy, including not only systems of national interest and critical infrastructure, but also federal, state and local governments, and the Australian community.[146] When serious cyber incidents take place, the ASD – through the ACSC – leads the Government response to help mitigate the threat and strengthen defences.

[142] Australian Signals Directorate. (n.d.) *REDSPICE*. Commonwealth of Australia. https://www.asd.gov.au/about/redspice

[143] Australian Cyber Security Centre. (n.d.) *Critical Infrastructure Uplift Program (CI-up).* https://www.cyber.gov.au/acsc/view-all-content/programs/critical-infrastructure-uplift-program-ciup

[144] Directory. (2021). *Australian Cyber Security Centre.* Commonwealth of Australia. https://www.directory.gov.au/portfolios/defence/australian-cyber-security-centre

[145] Australian Signals Directorate. (n.d.) *Cyber Security*. Commonwealth of Australia. https://www.asd.gov.au/cyber-security

[146] Ibid.

It is especially interesting for organizations and businesses the Information Security Manual (ISM),[147] produced by the ACSC, in this document is outlined a cybersecurity framework that companies, and organisations can apply, using their risk management framework, to endure their systems,[148] it also provides useful cybersecurity principles and guidelines.

Specifically, the ACSC responds to cybersecurity issues as Australia's Computer Emergency Response Team (CERT),[149], works together with the private and public sectors to share information on threats and increase resilience, and with governments, industry, and the community to increase awareness of cybersecurity, advice, and assistance, aiming to enhance awareness of cybersecurity to all Australians.[150]

Attorney General's Department and National Cybercrime Working Group

The Attorney-General Department (AGD) plays a pivotal role in Australia's cybersecurity ecosystem. It supports the development of Australia's cybersecurity policies, particularly on matters related to privacy and protective security as well as oversight of security, intelligence, and law enforcement agencies, including administration of criminal justice. The AGD also supports the government by providing advice on the application of international law (including space law) in cyberspace.

Within the AGD, the National Cybercrime Working Group (NCWG) was established to facilitate a national response to cybercrime. The group was created by the then Standing Council of Attorneys-General and is chaired by the Secretary of the Australian Attorney-General's Department,[151] comprising of representatives from Commonwealth, State and Territory police and justice agencies,[152] the idea is that since the internet facilitates criminal acts operated across jurisdictions, it is critical to have a national approach regarding cybercrime.[153]

Creating a more interconnected environment regarding national coordination of cybercrime policy and strategic response facilitates enhancing public awareness and State resolution on receiving and dealing with online offences.[154] For this reason, the NCWG had as one of its main attributions the review of different legislations and arrangements to identify how they could be improved, including proposals for clarifying lines of responsibility and raising coordination between law enforcement agencies.[155]

The Protocol for Law Enforcement on Cybercrime Investigations is a good example of this interconnected approach, the Protocol was developed in 2011 by the NCWG and other groups, providing a simple way to identify the most appropriate agency to deal with a cybercrime matter, considering the different kinds of

[147] Australian Signals Directorate. (2022). Information Security Manual.

[148] Ibid.

[149] Launched in 2010, CERT Australia's mandate is to provide Australian businesses with advice and support in mitigating cyber threats. It focuses on cybersecurity issues affecting major Australian businesses, Australia's critical infrastructure and other systems of national interest, rather than on cybercrime affecting the public or small/medium-sized businesses. (Standing Committee on Communications 2010).

[150] Ibid.

[151] Directory. (2023). *National Cybercrime Working Group*. Commonwealth of Australia. https://www.directory.gov.au/portfolios/home-affairs/national-cybercrime-working-group

[152] Department of Home Affairs. (2013). *National Plan to Combat Cybercrime*. p. 26.

[153] Wills, T. (2010). *Cyber Crime: The Net Is Closing in on You*. Bulletin (Law Society of South Australia) 32. no. 6:26.

[154] Ibid.

[155] Parliament of Australia. (2010). *Government Response – House of Representatives Standing Committee on Communications Report on the Inquiry into Cyber Crime – Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime*. p. 2.

cybercrimes, the nature and location of victims and offenders and some other contextual factors,[156] acting almost as a manual to deal with the question; whose responsibility is this?

During the Standing Council on Police and Emergency Management (SCPEM) that occurred in 2012, ministers were updated on the work by the NCWG and advised to develop the Australian Cybercrime Online Reporting Network (ACORN),[157] a key initiative under the National Plan to Combat Cybercrime that consisted of a governmental implementation of a centralised online reporting facility for cybercrime, making it easier for the public to report such crimes, in a more uniformed way, and helping Australian agencies to formulate and deliver more embracing measures, having a clearer picture of the national scene as a whole. Besides the reporting system, the website also provided general information on cybercrime and how individuals can protect themselves. A well-informed public can not only understand and protect itself against threats but can also help to safeguard systems and networks operated by business and government.[158] Understanding and awareness are also key in framing issues of cybersecurity in public policymaking.[159]

According to the National Organised Crime Response Plan 2015-18, while State and territory agencies are responsible for pursuing cybercrime that affects individuals, businesses and government systems in their jurisdictions, Commonwealth agencies are responsible for developing the threat picture of nationally significant cybercrime, including those directed at critical infrastructure, systems of national interest and Commonwealth Government systems.[160] ACORN would support this arrangement, helping both poles, State/Territory agencies and Commonwealth agencies, in an integrated system.[161]

In 2019 the ACORN system transitioned to the ACSC’s ReportCyber, an online platform for reporting cybercrimes by any member of the community or business,[162] after the initial contact, the report is referred to the appropriate police jurisdiction for assessment and intelligence purposes.

The NCWG was also responsible for overseeing the implementation of the National Plan to Combat Cybercrime 201,[163] a comprehensive strategy for a more collaborative national effort to confront cybercrime, ensuring that Australia became a harder target for sophisticated cybercriminals, and providing an annual update to the Standing Council on Law and Justice and the Standing Council on Police and Emergency Management regarding the national response to cybercrime.

On 21 March 2022, it launched the updated National Plan to Combat Cybercrime 2022,[164] building on its predecessor from 2013, focusing on three key pillars: Prevent and Protect; Investigate, Disrupt and Prosecute; and Recover. A more detailed overview is provided below.

[156] Department of Home Affairs. (2013). National Plan to Combat Cybercrime. p.18
[157] Australian Journal of Emergency Management. (2012). *COMMUNIQUÉ: Standing Council on Police and Emergency Management*. Australian Journal of Emergency Management. 29 June 2012, Vol. 27, Issue 3
[158] Department of Home Affairs. (2023) *Cyber Security*. Commonwealth of Australia. https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security
[159] de Bruijn, H., & Janssen, M. (2017). *Building Cyber Security Awareness: The Need for Evidence-Based Framing Strategies*. Government Information Quarterly, Volume 34, Issue 1, p 1-7.
[160] Department of Home Affairs. (2015). *National Organised Crime Response Plan 2015-18*.
[161] Ibid.
[162] Australian Cyber Security Centre. (n.d.) *Report Cyber*. https://www.cyber.gov.au/acsc/report
[163] Department of Home Affairs. (2015). *National Organised Crime Response Plan 2015-18*. p.10
[164] Department of Home Affairs. (2022). *National Organised Crime Response Plan 2022*.

Table 8: Overview of the National Plan to Combat Cybercrime 2022

The National Cybercrime Forum's Roadmap		
A secure, safe, just, and prosperous online world for the Australian community, and a hostile environment for cybercriminals targeting Australians and their businesses.		
Strengthen Australia as a hostile environment for cybercriminals to ensure that they are unable to operate effectively against the Australian community		
Continue to engage with international partners to respond to the threat of cybercrime		
Pillar One **Prevent and Protect**	**Pillar Two** **Investigate, Disrupt, Prosecute**	**Pillar Three** **Recover**
Strengthening Australia as a hostile environment for cybercriminals to ensure that they do not profit from targeting the Australian community Supporting industry leadership to prevent and protect against cybercrime threats and consider how products and services can be made safer through security and safety by design concepts Building confidence within the Australian community to improve their cybersecurity and safety habits to protect themselves from cybercrime threats Continuing to work with international partner to enhance global responses to the threat of cybercrime, including through robust international frameworks that ensure our law enforcement agencies have the mechanisms and electronic evidence to investigate and prosecute cybercrime, while respecting human rights and the rule of law Appropriately calling out those that willingly support or provide safe havens to cyber-criminals	Enhancing coordination across Commonwealth, state and territory law enforcement agencies, prosecutorial bodies, and other government agencies Continuing to strengthen partnerships between public and private sectors to investigate, disrupt and prosecute cybercrime Supporting law enforcement to access electronic evidence in foreign jurisdictions to investigate and prosecute cybercrime and criminals Ensuring law enforcement capabilities remain responsive to the rapid evolution of technologies, digital services and platforms Delivering on government investments over the forward years to enhance Australia's capability to counter malicious cyber threats Ensuring Australia's cybercrime legislation remains world leading and fit-for-purpose Enhancing cybercrime data collection, reporting and intelligence to better understanding cybercrime impacting Australia	Continuing to build awareness among victims of cybercrime about how to access resources on recovery and how to report incidents in partnership with law enforcement and the private sector to streamline access where possible Continuing efforts between law enforcement and industry to stop illicit and fraudulent payment structures and processes Reviewing post-incident feedback mechanisms to ensure feedback loops for cybercrime victims are as effective as possible Continuing to support organisations specialising in post-incident support services; a commitment considered even more vital as cybercrime continues to evolve and impact more Australians and their businesses

Government Action on the National Plan to Combat Cybercrime
The National Plan will bring together all jurisdictions to build a strong multi-faceted response to cybercrime harming Australia and Australians
Action: Establishing the National Cybercrime Forum, through the leadership of the Department of Home Affairs, to develop consolidated action plans under each pillar of the National Plan
Action: Engagement with state, territory and Commonwealth law enforcement and justice agencies
Action: Engagement with industry and academia to better protect the Australian community
Action: Monitoring, implementation, and reporting to Ministers through the National Cybercrime Forum
Action: Ministerial level agreement to the National Plan

Launching similar functions that the NCWG had, this time Home Affairs will establish the National Cybercrime Forum, consisting of representatives from across Commonwealth, State, and Territory agencies.[165]

The forum will help to achieve the objectives of the 2022 National Plan, and drive outcomes and support the development of the Cybercrime Action Plan, which will combine the powers, capabilities, experiences, and intelligence from all jurisdictions to build a robust multi-faceted response to the newer modern cyber threats in Australia.[166]

Department of Home Affairs

The Department of Home Affairs is responsible for developing the national cybersecurity policy and coordinating the implementation of Australia's Cyber Security Strategy, having in its Minister the task of coordination, and setting the strategic direction of the government's cyber effort.[167]

In October 2020, it was established by the Home Affairs Minister a Cyber Security Industry Advisory Committee to assist in the implementation of Australia's Cyber Security Strategy 2020. The Committee builds on the success of the Industry Advisory Panel, providing strategies, and ensuring the industry plays a continued role in influencing the delivery of the Strategy. The Committee provides advice to Government through regular meetings and reports directly to the Minister.[168]

The Australian government recognizes the enhanced importance that cybersecurity plays in modern society, which is reflected by the resources allocated to the segment, involving a $1.67 billion investment over 10 years into Australian cybersecurity initiatives, significantly more substantial than the investment related to the implementation of the 2016 Cyber Security Strategy (2016 Strategy), which was only $230 million.

The Department of Home Affairs includes a number of portfolio agencies that share cybersecurity roles and responsibilities, such as the Australian Security Intelligence Organisation (ASIO), focussing on the investigation of threats posed by hazardous state-sponsored cyber activity, the Australian Criminal

[165] Department of Home Affairs. (n.d.) *Cybercrime and Identity Security*. Commonwealth of Australia. https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/cybercrime-identity-security
[166] Ibid.
[167] Department of Home Affairs. (2023) *Cyber Security*. Commonwealth of Australia. https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security
[168] Department of Home Affairs. (n.d.) *Cyber Security Industry Advisory Committee*. Commonwealth of Australia. https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/industry-advisory-committee

Intelligence Commission (ACIC), responsible for understanding the cybercrime structure and enhance defence against it through partnerships, and the Cyber and Infrastructure Security Centre (see Focus Box).

Cyber and Infrastructure Security Centre

In 2021, the Department of Home Affairs established the Cyber and Infrastructure Security Centre to increase the resilience of the critical infrastructure in domains such as energy, communications, data storage and processing, defence industry, transport, health care, financial services, higher education and research, water and sewerage, food, and space technology.

The Centre complements the work of ACSC by acting as a regulator under the Security of Critical Infrastructure Act 2018, Part 14 of the Telecommunications Act 1997, the Aviation Transport Security Act 2004, the Maritime Transport and Offshore Facilities Security Act 2003, and the AusCheck Act 2007. The Centre assist companies in critical infrastructure sectors by sharing best practices, exercises, and modelling. The Centre also works with the Trusted Information Sharing Network (TISN) to engage with the industry.

The Trusted Information Sharing Network (TISN)

Established in 2022, TISN is the entity in charge of engaging with critical infrastructure sectors to ensure that they comply with the critical infrastructure legislation and that industries understand threats, vulnerabilities, consequences as well as cross-dependencies between sectors. TISN established sector groups to enable operators to share information on threats and vulnerabilities and collaborate on some initiatives. TISN groups are supervised by the Critical Infrastructure Advisory Council (CIAC).

In 2022, TISN established the Space Sector Group, which gathers experts from academia, industry, government, and state and territory representatives. The Space Sector Group *‘provides input, advice, support and guidance to the TISN on current, emerging and future (medium to long term) issues and trends relating to the operation, integration and use of space-based systems, technologies and information by Australian critical infrastructure.’* The Secretariat is managed by the Australian Space Agency.[169]

Department of Defence

The Department of Defence has the mission to defend Australia and protect its national interests, it does so by abiding by the 2016 Defence White Papers and the 2020 Defence Strategic Update, the government's most valuable guidance regarding Australia's long-term Defence capabilities. This document provides a plan aligned with capability and resources to deliver a future force that is more capable, agile, and ready to respond to future challenges.[170] Cyber, of course, as a key point for Australia’s defence aspirations, would not be left out and it is contemplated by the document and mainly by one of the department’s divisions.

Within the department is the Defence Science and Technology Group (DSTG), the government’s lead agency responsible for applying science and technology to defence and delivering valued scientific advice and innovative solutions for Defence and national security. capabilities aiming to safeguard Australia,[171] working closely with industry, universities, and the scientific community, with an annual budget of approximately $408 million. The roles of the Group can be better explained by the two following images:[172]

[169] Cyber and Infrastructure Security Centre. (2023). *TISN Sectors*. Commonwealth of Australia. https://www.cisc.gov.au/engagement/trusted-information-sharing-network/tisn-sectors

[170] Directory. (2023). *Department of Defence*. Commonwealth of Australia. https://www.directory.gov.au/portfolios/defence/department-defence

[171] Australian Government. (2020). *Defence Science and Technology Group.* https://www.dst.defence.gov.au/discover-dst

[172] Defence Science and Technology Group. (2020). *Our Role*. Commonwealth of Australia. https://www.dst.defence.gov.au/discover-dst/our-role

TABLE 9: OVERVIEW OF THE DSTG MAIN ATTRIBUTIONS

Role		Description
CORE	Operations	Supporting operational capability with science and technology expertise
	Sustainment	Providing support to Defence to sustain and enhance current capability
	Acquisition	Providing support throughout the genesis, development, acquisition, and introduction to service of major capability projects
	Future Proofing	Investigating client-focussed future concepts, contexts, and capability
EXTENDED CORE	Advice to government	Shaping defence and national security strategic policy through expert and impartial advice
	National security	Leading and coordination and delivery of science and technology to enhance whole-of-government national security
	Strategic research	Conducting research into high-impact areas for future Defence capability
SUPPORT	Emerging futures	Scanning the environment to gain an understanding of emerging science and technology threats and opportunities
	Partnerships	Enhancing our impact by collaborating with research and industry partners, nationally and globally
	Outreach	Promoting defence, science, and education in the broader Australian community

DSTG is made up of nine divisions, and, in terms of cyber protection, it can be highlighted the Cyber and Electronic Warfare Division (CEWD). The CEWD focus, through electronic means, on identifying, analysing, and countering threats to Australia's defence and national security. It also produces and validates concepts, tools and techniques that are used by Australia's Army, Navy, Air Force, Defence Intelligence and broader national security agencies against such risks, and provides technical advice to major Defence acquisitions,[173] being also responsible for situational awareness and communications in complex electromagnetic and cyber

[173] Defence Science and Technology Group. (2022). *Cyber and Electronic Warfare Division*. Commonwealth of Australia. https://www.dst.defence.gov.au/divisions/cyber-and-electronic-warfare-division

environments; development and validation of countermeasures; and development of techniques, technologies and tools for ensuring cyber and EW mission success.[174]

Defence Industry Security Program (DISP)

DISP is a program aimed at Australian businesses with some engagement with Defence projects, contracts, and tenders, assisting to identify and meet the expected security obligations to such businesses.

Although not mandated in all conditions, DISP membership is highly recommended for any projects in connection or potential to connect with Defence. There are situations, however, in which this membership is compulsory, depending on the type of work undertaken or contractual requirements particular to each project, when working on classified information or assets, storing, or transporting weapons or explosive ordnance, or providing some security services for Defence facilities.

Before applying, it is important that businesses get familiarized with the Defence Security Principles Framework (DSPF) and Australian Government Security Clearances, to determine what is the level of membership that is required for the company and consider which security measures are already in place and which still need to be further developed. Another pivotal document that can assist not only in this initial phase but during the whole membership is the Working Securely with Defence Guide, with crucial information regarding the program.

There are 4 levels of membership, Entry Level, and Levels 1, 2 and 3, each one with specific requirements, that are associated with four security classifications, Governance, Personnel Security, Physical Security, and ICT and Cyber Security. The interaction between these two variables will determine the level of security and the measures that the business must maintain.

	Governance	**Personnel Security**	**Physical Security**	**ICT and Cyber Security**
Entry Level	OFFICIAL / OFFICIAL: Sensitive	OFFICIAL / OFFICIAL: Sensitive	OFFICIAL / OFFICIAL: Sensitive	OFFICIAL / OFFICIAL: Sensitive
Level 1	Protected	Protected	Protected	Protected
Level 2	Secret	Secret	Secret	Secret
Level 3	Top Secret	Top Secret	Top Secret	Top Secret

There are certain requirements that businesses must achieve to be eligible to plead for a DISP membership, which includes, among other measures to obtain certain accreditations like Top 4 of the ASD Essential 8, and ISO/IEC 27001 and 27002. Once obtained, the membership requires some ongoing obligations, such as submit an Annual Security Report, undertake regular security training of all staff, including new employees, ongoing employment screening and suitability checks, and others.

In a nutshell, DISP aims to:

- Assist in the meeting of expected security requirements when dealing with Defence contracts and tenders
- Provide access to Defence security advice and support services
- Aid the recognition and management of security risks across businesses
- Provide trust and confidence to Defence and other governmental bodies to formalize all sorts of agreements with industry members while aware that security standards will be achieved

[174] Defence Science and Technology Group. (2016). *Cyber and Electronic Warfare Division, Strategic Plan 2016-2021*.

Australian Space Agency

In July 2018, the ASA after a review of the capabilities of Australia’s space industry. The Agency is within the Australian Department of Industry, Science, Energy, and Resources. The ASA’s charter outlines six roles and responsibilities:

- Providing strategic advice and national policy on the civil space sector,
- Coordinating Australia’s domestic civil space sector activities,
- Supporting the growth of Australian space industry and the use of space across the broader economy,
- Leading international civil space engagement,
- Administering space activities legislation and delivering on international obligations, including elements that pertain to cybersecurity.
- Inspiring the Australian community and the next generation of space entrepreneurs.

A key task of the ASA is to maintain close links with all government agencies involved in space activities to ensure continuity and centralisation. This in principles also applies to cyber-related organisations. ASA also cooperates and communicates with industry actors, as well as state and regional governments to further contribute to this task.

Additional entities support the ASA in maintaining coordination across different levels of government and with industry:

- **Australian Government Space Coordination Committee (SCC):** The SCC is an inter-departmental committee established in 2012 that brings together all relevant Australian Government departments to coordinate and formulate priorities for the civil space sector. Notably, it coordinates with the Strategic Policy Division of the DoD.
- **Space Industry Leaders Forum:** The Forum was established by the ASA to engage with the private sector in Australia to receive input on the business and technological aspects of the space industry which should be included in space policy and strategy. Members are industry representatives, academics, representatives from associations, and representatives from other non-government space organisations.
- **State and Territory Space Coordination Meeting (S&T Meeting):** The S&T meeting is a regularly scheduled meeting organised by the ASA to bring together representatives from states and territories.[175]

3.1.2 Policy Framework

It is just as important to understand the main actors that steer the Australian space cyber ecosystem, as to know which policies are triggered by them. Such policies draw in the Australian structure the roles and responsibilities of government agencies to combat cyber threats in the space domain, stipulating goals to be met.

A better understanding of these documents can clarify how the Australian government intends to achieve its own objectives, being the difference between a simple desire of having stronger cyberspace capabilities, and having a solid, studied, and justified plan to reach such intention.

[175] Aliberti, M., et al. (2020). *Emerging Spacefaring Nations*. European Space Policy Institute.

These policies must present coordination between them, not overlapping or contradicting themselves, in a way to create an organic and functional autopoietic ecosystem that feeds and gets fed on and by itself, always demarcated by the Australian legal archetype.

TABLE 10: OVERVIEW OF MAJOR CYBER-RELATED POLICIES IN AUSTRALIA

Strategic Frameworks	**Australia's Cyber Security Strategy 2020**
	International Cyber and Critical Technology Engagement Strategy
	2016 Defence White Papers and 2020 Defence Strategic Update
	2021 International Cyber and Critical Technology Engagement Strategy
	Digital Economy Strategy: A Leading Digital Economy and Society by 2030
	2020 Force Structure Plan (FSP20)
	Advancing Space – Australian Civil Space Strategy 2019-2028
	Defence Space Strategy
	Australia in Space: a Decadal Plan for Australian Space Science 2021-2030
Implementation Frameworks	Information Security Manual
	Strategies to Mitigate Cyber Security Incidents
	2022 National Plan to Combat Cybercrime
	Risk Assessment Advisory for Critical Infrastructure Space Technology Sector
	Cyber Incidents Response Plan
	Ransomware Action Plan

Australia's Cyber Security Strategy 2020

Australia's Cyber Security Strategy 2020 envisioned designing a plan to protect Australians online against malicious states, state-sponsored actors, and individual cybercriminals. To achieve this protection, the government instituted the investment of $1.67 billion over ten years in the cybersecurity area through this strategy and $1.35 billion destined for the Cyber Enhanced Situational Awareness and Response (CESAR) package. CESAR will assist ASD to identify more cyber threats and disrupt more foreign cybercriminals, enabling the flowering of more partnerships with industry and government.[176]

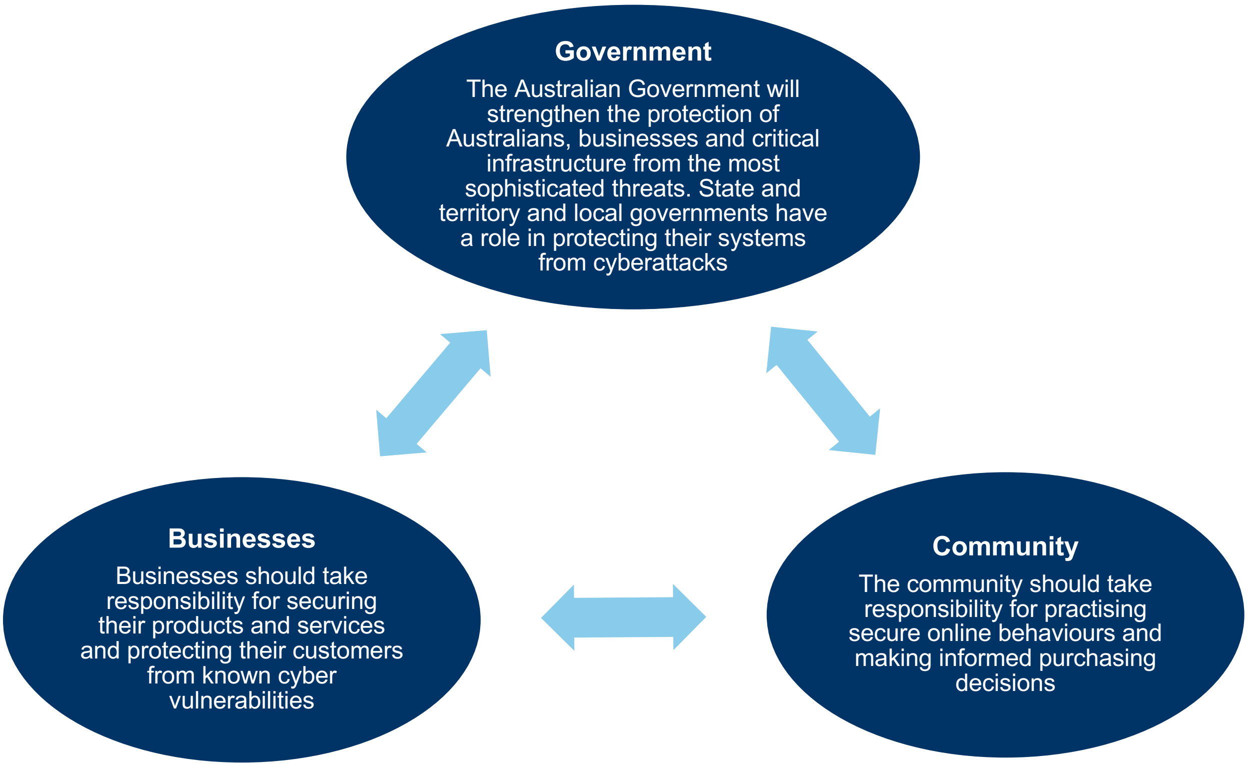
The document drinks in the fountain of the 2016 White Pages, which started rolling the ball with an investment of $320 million, developing its ideas into a more connected Australia than ever before and imputing cybersecurity on the average Australian as an everyday part of life, a safety tool, *just as pool fences provide peace of mind for households*.[177]

[176] Department of Home Affairs. (2020). *Australia's Cyber Security Strategy 2020*. pg. 21.
[177] Ibid. p. 7.

Influenced by the Industry Advisory Panel established by the Minister of Home Affairs to support the development of this document, a standing Industry Advisory Committee was put in place to ensure industry plays a continuing role in shaping the delivery of short and longer-term actions set out in this Strategy.[178]

Roles and responsibilities in cybersecurity are divided between government, society, and business, in an interlinked chain that needs the full combined participation of every sector for a truly protected society.[179]

FIGURE 19: ROLES AND RESPONSIBILITIES LISTED BY AUSTRALIA'S CYBER SECURITY STRATEGY 2020



Government
The Australian Government will strengthen the protection of Australians, businesses and critical infrastructure from the most sophisticated threats. State and territory and local governments have a role in protecting their systems from cyberattacks

Businesses
Businesses should take responsibility for securing their products and services and protecting their customers from known cyber vulnerabilities

Community
The community should take responsibility for practising secure online behaviours and making informed purchasing decisions

The government plays a pivotal leadership role, shaping policies for enhancing Australia's cybersecurity and providing a clearer self-aware position regarding the roles that businesses and the community need to play for a safer general digital environment. Initially, it focuses on setting expectations for critical infrastructure and systems of national significance, clarifying what are the minimum expectations that infrastructure owners need to ensure, and providing a hefty investment.

It also aimed to develop new powers proportionate to the consequences of a possible catastrophic attack, accompanied by appropriate safeguards and oversight mechanisms to mitigate and overcome such a disaster. Legislative changes were also considered for setting a minimum-security baseline across the economy, considering, among other proposals, changes on the role of privacy, consumer and data protection laws, duties for company directors and other business entities, and obligations on manufacturers of internet-connected devices.[180] [181]

To put in place all these measures, the document incentivised a deeper partnership with businesses, formally recognising businesses in governments' Cyber Incident Management Arrangements, and increasing

[178] Ibid. p.16.
[179] Ibid. p.19.
[180] Ibid. p.22.
[181] It is important to note that several of these goals had already started being contemplated by The Telecommunication and Other Legislation Act 2017 and the Security of Critical Infrastructure Act 2018 and its amendments.

investment in the Joint Cyber Security Centres (JCSCs)[182] to engage state and territory governments and industry.

The Strategy recognizes that the Australian government could not be powerless when facing encrypted activities, especially due to the increasing malicious use of the dark web, hence, it encourages the fortification of Australian security agencies and the AFP to identify and act against criminals that performances in this area, having the Telecommunications and Other Legislation Amendment (Assistance and Access) Act as legal ballast to contour encrypted segments.

At the international level, the government is responsible for complying with existing international law and norms of responsible state behaviour in cyberspace and encourages the maximum adhesion to these legislations to allied states, while working to cooperate in the building of a more complete international cyber framework.

Attending the feedback from consultation on the elaboration of this document about the defence of critical infrastructure, the Strategy highlighted several measures to enhance the security regulation framework in this area through amendments to the Security of Critical Infrastructure Act 2018 to include cyber-specific requirements to protect most critical national systems. This means empowering businesses, offering guidance and advice on critical points to set up a secure network, recognising their responsibility to take steps to protect themselves and the services they deliver, but also recognise the Australian government's obligation to act in the national interest when threats or consequences are too high for individual entities to manage solo.[183]

At the other end of the scale, small and medium businesses were also covered by the Strategy, with online training, toolkits, online guides, an $8.3 million Cyber Security Connect and Protect Program, providing tailored advice and assistance from trusted sources, and ACSC's 24/7 cybersecurity hotline for cybersecurity advice or assistance.

Aiming to help businesses to find qualified cybersecurity professionals, this Strategy also includes a Cyber Security National Workforce Growth Program, encouraging businesses and academia to partner together to find innovative new ways to improve cybersecurity skills and promote its market.

Finally, the community, as one of this Strategy's main links, also receives attention, mainly through awareness and education on safely using technology, with plenty of information and training offered by the ACSC, to protect data, information, devices, and networks from malicious actors. The eSafety Commissioner has also an important role to maintain online safety, protecting individuals, families, and communities from harmful content and behaviours such as cyberbullying, image-based abuse and illegal online content.[184]

2021 International Cyber and Critical Technology Engagement Strategy

This document replaces the 2017 International Cyber Engagement Strategy (ICES) which was the first comprehensive international cyber affairs agenda, setting a clear vision of Australia's interests and objectives in cyberspace for a three-year period,[185] adding critical technology in its content and refreshing Australian directives in the matter.

[182] The establishment of such JCSCs were an important achievement of the 2016 Cyber Security Strategy.
[183] Ibid. p.29.
[184] Ibid. p.35.
[185] Department of Foreign Affairs and Trade. (2017). *Australia's International Cyber Engagement Strategy*. Commonwealth of Australia. p.5

Critical technology is defined by the Australian government[186] and by the Critical Infrastructure Centre (CIC)[187] as those technologies with the capacity to significantly enhance, or pose risks, to Australia's national interests, including our prosperity, social cohesion, and national security. It is clear that, by this definition cyberspace, Artificial Intelligence (AI), 5G, or applications of these technologies are considered as being critical.[188]

The ICCTES's main objective is to enhance Australia's international engagement across cyber and critical technology issues, to enable a safe, secure, and prosperous global cyber environment, shaping the development and use of cyberspace and critical technology in line with national interests and values, strengthen engagement with like-minded democracies through a range of Partnerships and Agreements[189] and Multilateral Engagement,[190] especially in the Indo-Pacific and Southeast Asia regions.[191]

The Strategy is based on three interconnected and mutually reinforcing main pillars that guide Australian action in international cyber engagement: values, security, and prosperity.

Regarding values, it intends to uphold and protect liberal democratic standards through the online protection of human rights, the use of critical technology in a consistent way with international law, and advocating for diversity, gender equality and women's empowerment in the design, development and use of cyberspace and critical technology.[192]

The document recognizes the growing importance of cyberspace and ethically designed and conducted critical technologies for the strengthening of democracies and the protection and exercise of human rights and freedoms, in a free internet environment that promotes democratic principles, diversity and gender equality, consistent with ethical frameworks and international law.

In terms of security, it incentives the building of a strong and resilient cybersecurity capability for Australia and the world, equipped with international resilience to digital disinformation, misinformation, and foreign interference, firming cooperation for enhanced prevention, detection, investigation and prosecution of cybercrime in a safe and inclusive online environment that supports international peace and stability.[193] To achieve this, it takes into consideration the United Nations Framework for Responsible State Behaviour in Cyberspace to guide its actions and cooperates with other states to ensure accountability to states that act

[186] Australian Government. (2021). *Australia's International Cyber and Critical Tech Engagement Strategy 2021*. p.8

[187] Department of Home Affairs. (n.d.) *What is the Critical Infrastructure Centre?.* Commonwealth of Australia. https://www.homeaffairs.gov.au/nat-security/files/cic-factsheet-what-is-critical-infrastructure-centre.pdf

[188] Hence these technologies are protected by the Security of Critical Infrastructure Act 2018 and its Amendements.

[189] Australian Government. (2022). *Partnerships and Agreements, Australia's International Cyber and Critical Tech Engagement*. https://www.internationalcybertech.gov.au/about/partnerships-and-agreements

[190] Australian Government. (2022). *Multilateral Engagement | Australia's International Cyber and Critical Tech Engagement*. https://www.internationalcybertech.gov.au/about/multilateral-engagement

[191] Australian Government. (2022). *Cyber and Critical Technology Diplomacy | Australia's International Cyber and Critical Tech Engagement*. https://www.internationalcybertech.gov.au/our-work/cyber-and-critical-technology-diplomacy

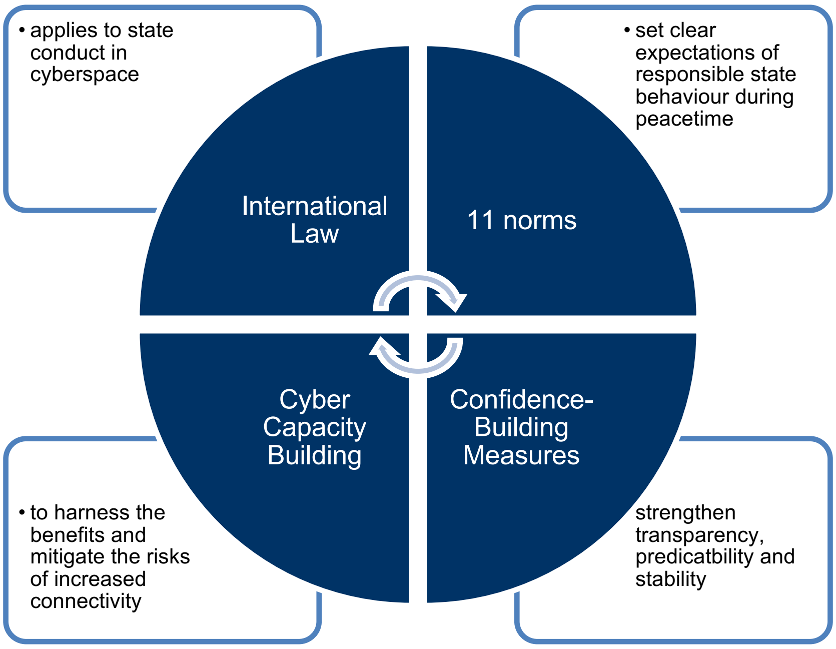
[192] Australian Government. (2021). Australia's International Cyber and Critical Tech Engagement Strategy 2021. p.18

[193] Ibid. p.34.

against the Framework. Against those, Australia has a deter and respond to malicious cyber activities policy which relies on international cooperation to counterattack even with military measures, if necessary.[194]

This Framework includes the UN Charter in its entirety, 11 voluntary non-binding norms of responsible state behaviour endorsed by all states, that also recognised the need for confidence-building measures (CBMs) and coordinated capacity building. These four elements combined (international law,[195] voluntary norms, CBMs and capacity building) are referred to as the UN Framework for Responsible State Behaviour in Cyberspace.[196]

FIGURE 20: UN ROLE IN THE PROMOTION OF RESPONSIBLE STATE BEHAVIOUR IN CYBERSPACE


• applies to state conduct in cyberspace
• set clear expectations of responsible state behaviour during peacetime
International Law
11 norms
Cyber Capacity Building
Confidence-Building Measures
• to harness the benefits and mitigate the risks of increased connectivity
strengthen transparency, predicatbility and stability

Regarding international law, and considering the often distorted way in which it can be perceived by countries, taking into account complex issues such as jurisdiction and sovereignty, Australia brings as Annex B to this Strategy precious material on how it interprets such issues of international law with regard to cyberspace, encompassing sensitive themes such as the peaceful settlement of disputes, use of force, self-defence against an offensive cyber operation, human rights, state responsibilities, etc.[197] The country also encourages other nations to do the same, thus contributing to greater clarity in the midst of a still so bleak field.

Influenced by what happened during the COVID-19 pandemic, Australia recognised the need for international cooperation and public communications resources to promote facts, avoiding menaces such as

[194] At this point is relevant to point out that, as previously referred, according to the Australian Signals Directorate Annual Report 2020-2021, offensive cyber capabilities have already been used, for example to counter offshore threats, including the dismantling of online infrastructure used by foreign cybercriminals targeting Australians during the COVID-19 pandemic.
[195] This includes, where applicable, the law regarding the use of force, international humanitarian law (IHL), international human rights law (IHRL), and the international law of State responsibility. Annex B: Australia's position on how international law applies to State conduct in cyberspace.
[196] Ibid. p.37.
[197] Ibid. p.98.

foreign interference, disinformation and misinformation that promotes the mining of a country's independent decision-making system, affecting its national sovereignty is also addressed.[198]

Also, due to the increase in scams and fraud attempts in the digital world, it saw the need for enhancing national and regional collective security and resilience to cybercrime to finally destroy the idea of cybercrime as a low-risk and high-return criminal activity, empowering the Indo-Pacific region countries to develop their own policies and domestic legislation in accordance with the Budapest Convention principles. In this sense, the development of cybercrime-relevant skill sets in the region complements a range of initiatives led by the eSafety Commissioner and other Australian agencies aiming at mitigating a range of online harms such as online child exploitation and abuse, terrorist/violent extremism,[199] etc.

The third pillar, prosperity, also heavily relies on Australia's international engagement, supporting the Indo-pacific region to foster its own independent technological market, creating a diverse and competitive market for this segment, to fortify Australian research, industry and innovation through international cooperation and maximise economic growth by shaping an enabling environment for digital trade.[200]

Australia will be supporting its neighbours through investment in secure telecommunications infrastructure that does not pose longer-term considerations of the possible impact on their sovereignty, placing the country as a reliable provider of safe technology, a gap that if remained it could have been fulfilled by nations that do not represent the best for Australia's national interest. The support will be made not only by investments but also by helping states modernise their policy and regulatory frameworks.

The idea is to break the current monopoly situation in which high technology is dominated by fewer and more dominant market players, decreasing the risks that monopolisation of critical technology may pose, such as varying degrees of economic coercion, and undermining their ability to participate meaningfully in global markets, diversifying the segment into an open, resilient, diverse and competitive market,[201] investing in science and technology diplomacy in close cooperation with domestic research, industry and government aiming a multi-stakeholder model of Internet governance.

This does not mean that Australia will encourage the indiscriminate growth of any segments of technology, the COVID-19 pandemic demonstrated that a higher degree of diversification, if not correctly planned, can have a considerable impact on the security of the final product, especially regarding supply chain technology, for this reason, the country seeks to promote responsible cyber and critical technology capabilities that can strengthen supply chain resilience and sustainability,[202] guided by international standards to promote security-by-design and by principles and guidelines developed by the ACSC, such as the Critical Technology Supply Chain Principles, in consultation with industry.[203]

[198] Ibid. p.45.
[199] Ibid. p.62.
[200] Ibid. p.64.
[201] Ibid. p.71.
[202] Ibid. p.72.
[203] The ACSC also produced a document updated in October 2021 named Cyber Supply Chain Risk Management, which alerts organisations regarding supply chains' possible threats. The document helps to understand and identify cyber supply chain risks by referencing the Identifying Cyber Supply Chain Risks and setting cybersecurity expectations through the Cyber Security Principles and the Essential Eight Maturity Model. The biggest concern is that adherence to these principles, guidelines and documents is non-mandatory. However, the Security of Critical Infrastructure Act 2018 grants provision for specific direction to be issued by the Government where national security concerns exist, creating among other requirements, the need for a Register of Critical Infrastructure Assets, obligation to give information and notify of events and entitles agents government agencies to require certain reports and information, etc.

These measures if correctly applied could lead to a decentralised cyber and technological market with multiple independent sources, conducted in a multi-stakeholder model of Internet governance that enables wider digital trade with reduced barriers, supporting the growth of an open and competitive economic environment. All this multifaceted environment ruled by common principles and shared policies. In summary, desiring a decentralised international model, for a vaster variety, based on centralised and communicable paradigms, for an easier dialogue.

Digital Economy Strategy: A Leading Digital Economy and Society by 2030

To secure Australia's economy and recovery from the COVID-19 pandemic it launched the Digital Economy Strategy in Budget 2021-22, setting an ambitious vision for a digital Australia and charting the necessary actions toward Australia being a top 10 digital economy and society by 2030, keeping the country at the forefront of emerging technologies and delivering the right foundations to grow the digital economy, including, of course, cybersecurity.

The Strategy intends the facilitation of small and medium businesses to use digital tools, enhance Australian companies' presence in the E-commerce world, incentivise modern industry and emerging tech sectors such as AI, the internet of things, and innovative aviation technology, and provide frictionless, simple, and trusted essential and governmental services. For this it puts in place foundations to sustain such changes, investing in digital infrastructure, like 5G and NBN upgrades, promoting training to assist Australians to lift their digital capabilities in the workforce, making them advanced digital skilled professionals, expanding Australia's trade and international engagement, including digital trade agreements, modernising systems, and regulations, while promoting guidelines drawn by the Cyber Security Strategy.[204]

When specifically dealing with cybersecurity, the Strategy recognises that businesses and consumers will only actively engage in the digital economy when feeling confident, safe, and protected online, hence cybersecurity enhancement plays a crucial role in the goal's achievement. To reach this a stage, the document planned the following steps over the period.[205]

TABLE 11: STEPS PLANNED BY THE DIGITAL ECONOMY STRATEGY 2030

Timeframe	Cyber Security, Safety, and Trust
Next 2 Years	Strengthening Australia's cybersecurity incentives and regulations through the Cyber Security Best Practice Regulation Task Force and feedback from industry
	Improve protections for Australian's privacy online and transparency of data handling practices through the review of the Privacy Act 1988
	Deliver a review and updates to the cybersecurity related occupations as coded in the Australian and New Zealand Standard Classification of Occupations
Next 5 Years	Develop a cybersecurity skills shortage forecasting methodology and model with reporting and ongoing data collection by 2024 to more effectively target initiatives that address cybersecurity skills demand

[204] Department of Industry, Science, and Resources. (n.d.) *Promoting and protecting critical technologies*. https://www.industry.gov.au/science-technology-and-innovation/technology

[205] Department of the Prime Minister and Cabinet. (2021). *Digital Economy Strategy 2030*. Commonwealth of Australia.

	Privacy settings in place that empower consumers, protect their data, and serve the Australian economy
	A National Data Security Action Plan makes public and private data more secure through the introduction of standards and policies as part of a National Data Security Action Plan
Next 30 Years	Strengthened cybersecurity and data settings supports Australian businesses and Australians to improve cybersecurity practices

The Digital Economy Strategy 2022 Update brought an overlook of the progress made in the first couple of years, underlining the development of CESAR as an important weapon for the ASD to identify and disrupt more cyber threats, and several legislative innovations and amendments such as the Security Legislation Amendment (Critical Infrastructure) Act 2021 uplifting the security and resilience of Australia's critical infrastructure, the Surveillance Legislation Amendment (Identify and Disrupt) Act 2021 introducing new law enforcement powers to identify and disrupt serious online crimes, the Online Safety Act 2021 providing additional protections for Australians online, and more. New policies were also introduced in this period, contributing to the national cybersecurity framework filling, in this sense, the Ransomware Action Plan and the National Plan to Combat Cybercrime are pointed up.

2016 Defence White Paper and 2020 Defence Strategic Update

The 2016 Defence White Paper represents a comprehensive plan for the defence of the Australian territory and domestic interests, expanding national policies to the Asia Pacific region and the whole world, and aligning Defence's strategy, capability, and resources. The strategy outlines all elements of the Government's Defence investment, including new weapons, platforms, systems, and the enabling equipment, facilities, workforce, information and communications technology, and science and technology,[206] in a shared effort between the government, Australian defence industry and science and technology research organisations.

The paper identifies the United States as Australia's most important strategic partner in the region, stressing that the North American country plays an essential role in the continued stability of the rules-based global order on which Australia relies for our security and prosperity, especially on the Indo-Pacific region.

It is acknowledged that in this area the U.S. can have with China some points of friction, that could lead to rising tensions, particularly in the cyber and space domains.[207] Consequently, since Australia is also the main partner of the U.S. in the region and has been consistently adopting U.S.-like approaches and policies in the area, such tensions can spill over Australia.

In this sense is particularly interesting to point out to the ANZUS Treaty, a triple alliance between Australia, New Zealand and the US, the treaty recognises that an armed attack in the Pacific Area on Australia or the United States obliges each country to act to meet the common danger.[208] In 2011, Australian and U.S.

[206] Department of Defence. (2016). *2016 Defence White Paper*. Commonwealth of Australia.
[207] Ibid. p.42.
[208] Ibid. p.121.

representatives during the 60th anniversary of the signing of the ANZUS announced that the alliance would be extended into cyberspace,[209] making an already tangled situation even more complex.

This complication deriving from the cyber environment was contemplated as one of the six key drivers that will shape the development of Australia's security environment to 2035; 'the emergence of new complex, non-geographic threats, including cyber threats to the security of information and communications systems,'[210] being cited as a direct threat not only to the ADF's warfighting ability but also to many other government agencies and domestic critical infrastructure, including space ones.

To prevent this interference, the document prescribes enhancing the U.S. partnership, looking to strengthen Defence's space surveillance and situational awareness capabilities, including through the space surveillance C-band radar operated jointly by both countries and the relocation of a U.S. optical space surveillance telescope to Australia. It also determines better cooperation with the international community aiming to expand the framework around the theme and fill possible gaps in which cybercriminals could be acting or hiding.[211]

To counter the growing threat of malicious cyber activities, the Papers also focussed on improving the resilience of the internal Australian structure, enduring Defence's cybersecurity capabilities to protect ADF's warfighting and information networks and providing better coordination with industry and academia.[212]

In this sense, key achievements of the 2016 Defence White Papers include increasing investments in cyber skill education, opening the Australian Cyber Security Centre (ACSC), Establishing Joint Cyber Security Centres (JCSCs) to engage state and territory governments and industry, Appointing the Ambassador for Cyber Affairs,[213] establishing the Cyber Security Cooperative Research Centre and the AustCyber, the Australian Cyber Security Growth Network.[214]

Recently the 2016 Defence White Papers was refreshed by the 2020 Defence Strategic Update, reassuring several pillars of the previous document, and planning investments of approximately $15 billion over the next decade in strengthened Information and Cyber domain capabilities, investing in defensive and offensive cyberspace operations, signals intelligence, joint electronic warfare, as well as systems to integrate intelligence, surveillance and reconnaissance programs and data.[215]

2020 Force Structure Plan (FSP20)

The 2020 Force Structure Plan, released in 2020 along with the Strategic Update, describes the envisaged investments in defence capabilities until 2040 that would support the objectives of the Strategic Update. Regarding the space sector, the capability program architecture of Defence relies on two things: space services (providing communications, PNT and GEOINT services) and space control (SSA and SST; freedom of operations in space).

While the Plan covers all warfighting domains including cyberspace, the part covering the space domain does not mention cyberspace or cybersecurity.[216]

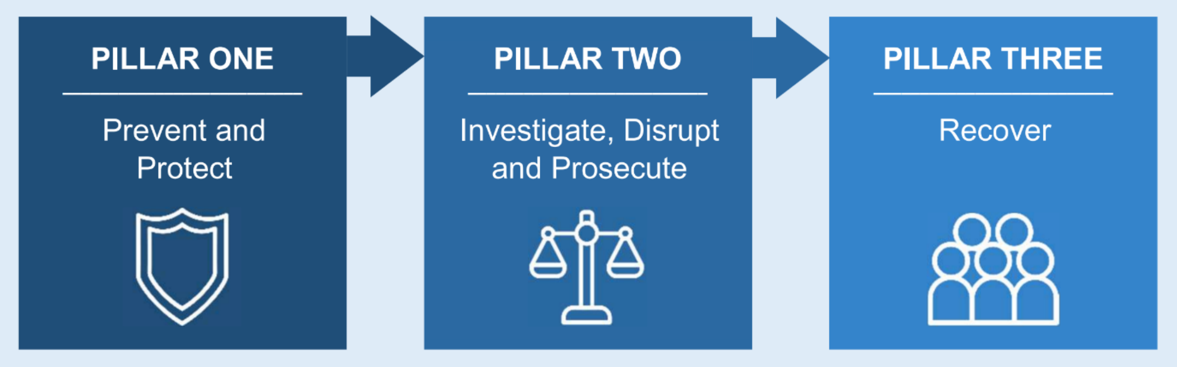
[209] Davies, A., et al. (2012). ANZUS 2.0: *Cybersecurity and Australia–US Relations*. Australian Strategic Policy Institute, Issue 46. p.1. https://www.aspi.org.au/report/special-report-issue-46-anzus-20-cybersecurity-and-australia-us-relations
[210] Department of Defence. (2016). *2016 Defence White Paper*. Commonwealth of Australia. p.41.
[211] Ibid. p.52.
[212] Ibid. p.73.
[213] Nowadays the position is entitled 'Ambassador for Cyber Affairs and Critical Technology'.
[214] Department of Home Affairs. (2020). *Australia's Cyber Security Strategy 2020*. p.9
[215] Department of Defence. (2020). *Defence Strategic Update*. p.36.
[216] Department of Defence. (2020). *Force Structure Plan*.

2022 National Plan to Combat Cybercrime

Being a key deliverable under Australia's Cyber Security Strategy 2020 and building on the 2013 Plan,[217] it was released the 2022 National Plan to Combat Cybercrime, taking into consideration the state of today's cyber domain, which faces a greater degree both of malicious technology and online users, an unfortunately, combination that made with that the self-reported Australian losses due to cybercrime were almost 17 times more in 2021 than in 2013.[218]

To keep up with the rapid pace at which cybercrime evolves and adapts, the document intends to establish a nationally coordinated response, with better proximity between government and the Australian community and businesses, centring on three key pillars; prevent and protect (i), investigate, disrupt, and prosecute (ii), recover (iii).

FIGURE 21: PILLARS OF THE NATIONAL PLAN TO COMBAT CYBERCRIME (SOURCE: NPCC)



The first pillar intends to enhance collaboration between government and industry, to sharpen Australia's ability to act flexibly and promptly when responding to emerging cyber threats. The main actions under this section focus on making Australia a hostile environment for cybercriminals, incentivising industry leaders to develop safer products and services through security and safety by design concepts, investing in research and academia, and building the confidence of the Australian community to improve their cybersecurity habits. Internationally, it encourages the partnership with other countries to facilitate the work of domestic law enforcement agencies to investigate and prosecute cybercrime, while appropriately calling out those states who somehow support cybercriminals.[219]

Consistency is the key word for pillar number two, which recognises the diverse environment in which cybercriminals operate, a scenario in that usually the intricacy of laws and regulations serves as a hindrance for investigations but affirms that this cannot serve as an obstacle to justice, creating a haven for these perpetrators.

To revert this is necessary to ensure consistency of national cybercrime legislation and criminal justice responses, across the Commonwealth, states, and territories, with world-leading legislative frameworks that represent the most modern in the subject with the possibility to quickly adapt to respond to the evolution of technology. This consistency is also desired at the global level, with the use of international forums for strengthening global resilience to cybercrime, using as an example the Council of Europe Convention on Cybercrime (the Budapest Convention).[220]

[217] Department of Home Affairs. (2022). *National Plan to Combat Cybercrime 2022*.
[218] Ibid. p.2.
[219] Ibid. p.11.
[220] Ibid. p.12.

The deepening of the public-private relationship is also highlighted, with greater information sharing, to equip Australian law enforcement agencies and prosecutorial bodies, ensuring that they can effectively gather necessary and relevant evidence for investigations and undertake prosecutorial action, if applicable.

The last pillar relates to the recovery of those who were affected by cybercrime, people and businesses, regularly examining feedback loops to provide progress updates to victims concerning their matter following a cybercrime incident. The goal is to continue building awareness among victims about how to access resources on recovery and how to report incidents, while empowering law enforcement agencies and industry to curb criminal practices and continue to support organisations specialising in post-incident support services.[221]

Another important action derived from the Plan is the establishment of the National Cybercrime Forum, consisting of all jurisdictions (including state and territory justice departments, Commonwealth, state and territory law enforcement agencies, and other regulators such as the Office of the eSafety Commissioner), working together with industry, academia, and the community.

The Department of Home Affairs will lead the forum with the objective of developing the Cybercrime Action Plan that brings together the experience, powers, capabilities, and intelligence of all jurisdictions to build a strong multi-faceted response to cybercrime harming Australia, outlining detailed actions under each of the three pillars of the National Plan, as well as mechanisms for monitoring and reporting on implementation progress and outcomes.[222]

Australian Government Information Security Manual (ISM)

Developed by the ACSC, the Information Security Manual's (ISM) purpose is to outline a cybersecurity framework that organisations can apply, using their risk management framework, to protect their information and systems from cyber threats.[223] Its elaboration was made in accordance with ASD's designated functions under section 7(1)(ca) of the Intelligence Services Act 2001.

Despite being a very comprehensive document, and its widespread use would generate a great advantage for the security of Australian society, the ISM is not mandatory by itself, unless legislation, or a direction given under legislation or by some other lawful authority, compels them to comply.

The Manual is mainly composed firstly of cybersecurity principles, to provide strategic guidance to protect organisations, grouped into four activities; govern (identifying and managing security risks), protect (implementing controls to reduce security risks), detect (detecting and understanding cybersecurity events to identify cybersecurity incidents) and respond (Responding to and recovering from cybersecurity incidents), [224] totalizing 24 principles, and secondly, of security guidelines, delivering more practical guidance, presenting 22 topics that include outsourcing, physical security, email, cryptography, etc.

The ISM content can be very useful for individuals and families, small and medium businesses, and even government critical infrastructure agencies and organisations, provided that the guidelines do not conflict with others to which such agencies are already legally bound. With so much variety of the final recipient that could use Manual's directives, aiming to assist its application, the document also presents a maturity model to assess the implementation of individual principles, groups of principles or cybersecurity principles as a whole.[225]

[221] Ibid. p.13.
[222] Ibid. p.14.
[223] Australian Signals Directorate. (2022). *Information Security Manual*. p.1
[224] Ibid. p.5.
[225] Ibid. p 6.

Risk Assessment Advisory for Critical Infrastructure Space Technology Sector

In 2021, the Cyber and Infrastructure Security Centre compiled a Risk Assessment Advisory for Critical Infrastructure Space Technology Sector which, among other objectives, aims to assist in determining the criticality of assets.[226] According to the document, it is imperative to identify criticality so that responsible entities can allocate necessary resources to the protection of the operational capability of such assets.

The document specifies that "the critical sites and components of an asset are ultimately those most crucial to its effective functioning and consequently integral to Australia's national interests". The following points can be highlighted from the envisaged process:

- A function of a critical infrastructure asset may be the provision of a critical service or good that is a contributor to the economic or social well-being, security, or defence of the country.
- Within critical assets, critical sites are where the proper functions of these assets are located; these could include control rooms, satellite assembly sites, launch sites, and data centres that host critical software. Critical sites are physical locations that without them the asset would not achieve its proper purpose.
- Critical components are those required to provide the function of the asset, or whose absence, compromise or damage could cause substantial harm to the asset. For a space technology organisation, critical components may include tracking telemetry and command equipment used to receive and send satellite communications, or a feed horn used to gather reflected signals from the satellite dish and transfer them to a low noise block.

Although there are still key discussions in determining the criticality of an asset, the envisaged process of identification can positively assist in eliminating some of the uncertainties, resulting in a more harmonic combined effort of owners and operators of such assets and the Australian government to protect Australia's critical infrastructure.

Strategies to Mitigate Cyber Security Incidents

Also developed by the ACSC, the document was first published in 2010, having its last updated version in 2017. The document aims to assist cybersecurity professionals in all organisations mitigate cybersecurity incidents, including targeted cyber intrusions, ransomware and external adversaries with destructive intent, malicious insiders, 'business email compromise', and industrial control systems.[227]

The Strategy content should not be the first step for starting cyber threat proofing the organisation, before implementing any of these mitigation strategies, organisations need to identify their assets and perform a risk assessment to identify the level of protection required from various cyber threats.

This document is complemented by the Strategies to Mitigate Cyber Security Incidents – Mitigation Details publication, which includes implementation guidance for the mitigation strategies, and the inclusion of two other cyber threats.[228] Also, by the Essential Eight Maturity Model publication, which advises how to implement mitigation strategies in a phased approach and how to measure the maturity of their

[226] Cyber and Infrastructure and Security Centre. (2021). *Risk Assessment Advisory for Critical Infrastructure Space Technology Sector*. CISC. https://www.cisc.gov.au/critical-infrastructure-centre-subsite/Files/raa-space-technology.pdf

[227] Australian Government. (2017). *Strategies to Mitigate Cyber Security Incidents*. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/strategies-mitigate-cyber-security-incidents/strategies-mitigate-cyber-security-incidents

[228] 'Business email compromise' and threats to Industrial Control Systems guidance.

implementation. With the inclusion of the Information Security Manual, this framework is considered by the ACSC as an effective new baseline for all organisations.

Cyber Incidents Response Plan

For the unwanted cases of cyber incidents occurrence, the ACSC created a cyber incident response plan to ensure Australian organisations have the parameters to tailor an effective response and quick recovery internal strategy that must be regularly tested and updated. While seeking to assist, the document also empowers such organisations highlighting that they are responsible for managing incidents affecting their business.

Due to this feature of not taking control but supporting organisations, the document offers guidance to aid the development of individual response plans, that must primarily align with the organisation's incident, emergency, crisis, and business continuity provisions, as well as jurisdictional and national cyber and emergency arrangements. It intends to be used as a starting point to create customised response plans, making with that the organisations develop more detailed procedures that are relevant to their line of work, taking into consideration the unique operating environment, priorities, resources, and obligations of every company, while also supports personnel to fulfil their roles by outlining their responsibilities and all legal and regulatory obligations.

For its elaboration, the ACSC, based on several external sources, such as the Australian Government Information Security Manual (ISM), Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Incident & Vulnerability Response Playbooks 2021, several ISO standards, etc.[229]

Ransomware Action Plan

Developed by the Department of Home Affairs, the document is based on inputs from the 2016 and 2020 Cyber Security Strategies, focussing on the specific problem of ransomware, which had a 15% increase in ransomware attacks reported to the ACSC from October 2020 to October 2021.

The strategy developed clearly indicates that the government considers non-sustainable the idea of conducting ransom payments, which collaborates to maintain the whole ever-evolving ransomware business mode,[230] instead, it aims to strengthen the country's cyber defences, making it a unified and unpleasant target for criminals and a hostile place for their illicit operation to operate.

The improvement of Australian cyber defences comes from multiple directions and sources, in a multifaceted approach, that is guided by the three objectives that base the Plan; prepare and prevent, respond and recover, and disrupt and deter, encompassing more concrete measures consubstantiated not only on economic investments to better equip the Australian Federal Police, but also on the introduction of new policies and legislation, the development of the next National Plan to Combat Cybercrime, the offering of aiding tools to support small and medium businesses such as the Cyber Security Assessment Tool, and the IDCARE to victims of cybercrime, the Australian Cyber Security Centre's 'act now, stay secure' campaign, and the enhanced integration of the country with international partners to address ransomware globally

[229] ISO/IEC 27035-1, Information technology – Security techniques – Information security incident management, Part 1 Principles of incident management; ISO/IEC 27035-2, Information technology – Security techniques – Information security incident management, Part 2 Guidelines to plan and prepare for incident response; ISO/IEC 27035-3, Information technology – Information security incident management, Part 3 Guidelines for ICT incident response operations.

[230] This position of not conducting ransom payments can be identified in the recent cyberattacks that targeted Optus and Medibank.

establishing the Operation Orcus, a multi-agency law enforcement operation led by the Australian Federal Police to face the growing ransomware threat, both internally and overseas.

Australia's Space Policies

Advancing Space – Australian Civil Space Strategy 2019-2028

Australian plans to transform the space sector over the coming ten years to diversify the economy, build international partnerships and national capabilities, ensure the security of the space infrastructure, and produce socioeconomic benefits are outlined in the Australian Civil Space Strategy 2019-2028.

ASA will implement the strategy in three stages. PNT and Earth observation were given priority in the first phase, which aimed to provide the framework for expansion through the year 2019. With a major emphasis on SATCOM, the second phase was scheduled to be implemented between 2019 and 2021. From 2021 to 2028, the third phase is expected to be executed, with a particular emphasis on R&D, robotics and automation, SSA, and access to space.

The strategy is based on four principles:

- Open doors approach at the international level (leveraging international partnerships and develop the space industry),
- Increase national capabilities (develop the space sector in areas where Australia can have a competitive advantage),
- Promote responsible regulation, risk management and culture (ensure safety and security and apply international norms),
- Inspire and build a future workforce (encourage the youth to pursue careers in STEM and identify required skills for the future workforce).

Cyber is mentioned in an interesting way as it considers cybersecurity as a space technology and as a risk for Australia's space infrastructure: *'The rapid advance of space technology, including cybersecurity, artificial intelligence, optical communications, and other emerging technologies creates opportunities, but also risks for Australia's growing space industry and government regulation.'* In addition, it considers as a responsibility for the government to *'advise on the intersection between civil space matters, military space matters, national interest, and the broader security environment (including cybersecurity), as it applies to civil space.'* It also outlines the measure to *'develop a world-class regulatory system that enables entrepreneurship while ensuring national safety and security, including cybersecurity, and meeting international and national obligations.'* [231]

Defence Space Strategy

In 2022, Australia released a Defence Space Strategy following the recognition of space by the Department of Defence as a warfighting domain. The strategy describes the strategic situation in space and defines a vision and a mission to make Australia an integrated space power by 2040.

The main objectives focus on:

- Enhancing Defence's space capability to assure Joint Force access in a congested and contested space environment

[231] Australian Space Agency. (2019). *Advancing Space: Australian Civil Space Strategy 2019-28*.

- Delivering military effects integrated across the government and with allies and partners in support of Australia's national security
- Increase the national understanding of the criticality of space
- Advance Australian sovereign space capability to support the development of a sustainable national space enterprise
- Evolving the Defence space organisation to ensure a coherent, efficient and effective use of the Space warfighting domain.

Cyber is mentioned three times in the strategy in the following:

- '*The Department of Defence has acknowledged the importance of space, by recognising the space domain alongside the existing warfighting domains of air, maritime, land and cyber*.'
- '*Consistent with the other domains of Air, Maritime, Land and Cyber, Defence will shape the space domain, deter competitor actions, and respond as necessary to assure Defence's access to space capabilities*.'
- '*Australian sovereign systems may be vulnerable to cyber, electronic and kinetic attack, so Defence must improve the reconstitution, resilience and defence of the Defence Space Enterprise capabilities*.'[232]

Australia in Space: A Decadal Plan for Australian Space Science 2021-2030

The Australian Academy of Science and Australia in Space outlined a ten-year strategy for Australian space science, along with suggestions and measures to advance national priorities and interests in space, as well as to boost the innovation economy, build sovereign capabilities, and enhance the quality of life.

The main recommendations of the plan are:

- Making space science a national research priority that aligns with civil and defence sovereign industry capability requirements, encourages discovery and innovation, and helps build capacity for national benefit and international impact.
- Establishing a Lead Scientist role in the Australian Space Agency with responsibility for space science policy settings. The role should include responsibility for providing strategic science policy advice, facilitating cross-sector engagement and international collaboration, and fostering capacity development initiatives.
- Committing to and investment in an ongoing national space program, enabled by space missions that advance science, stimulate technical innovation, address national priorities, grow capability, and inspire citizens.

The plan mentions cyber threats on the space infrastructure: '*Australia's reliance on accurate, available and reliable PNT information will continue to expand, amplifying concerns about vulnerabilities and risks, particularly those impacting national security such as cyberattacks, jamming and spoofin*g.' Recommendations also include R&D in the field of quantum technologies.[233]

[232] Department of Defence. (2021). *Defence Space Strategy*.
[233] Australian Academy of Science. (2021). *Australia in Space: a Decadal Plan for Australian Space Science 2021-2030*

3.1.3 Legal Framework

In this section, we provide an overview of the most relevant legal and regulatory documents dealing with the cybersecurity of the space infrastructure. The Section pays consideration to both domestic legislations (e.g., the Cybercrime Legislation Amendment Act of 2012, the Privacy Amendment Act of 2017, the Telecommunications and Other Legislation Amendment Act of 2017, etc.) and of the international legal regimes (e.g., the UN Charter, the Outer Space Treaty, ITU Convention, the Budapest Convention, etc.) Australia has ratified. An overview is provided in Table 3 below.

TABLE 12: OVERVIEW OF GENERAL AND SPACE-SPECIFIC DOMESTIC AND INTERNATIONAL LEGAL TOOLS IN AUSTRALIA

Domestic	**General**	• Privacy Act 1988 • The Cybercrime legislation Amendment Act • Telecommunications and Other Legislation Amendment Act • Security Legislation Amendment (Critical Infrastructure Protection) Act 2021 • Telecommunications and Other Legislation Amendment (Assistance and Access) Act
	Space-specific	• The Space Activities Act and the Launches and Returns Act
International	**General**	• Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' • The Constitution and Convention of the International Telecommunication Union • The Council of Europe Convention on Cybercrime • Draft Articles on Responsibility of States for Internationally Wrongful Acts
	Space-specific	• The Outer Space Treaty (1967) • The Rescue Agreement • The Liability Convention • The Registration Convention

Domestic Legal Framework

The Privacy Act

The Privacy Act 1988 (Privacy Act)[234] is one of the first pieces of legislation relevant to cybersecurity. It was passed by the Australian Parliament in 1988 with the aim to promote and protect the privacy of individuals and to regulate how Australian Government agencies and organisations with an annual turnover of more than $3 million, and some other organisations, handle personal information.[235] It contains 13 Australian Privacy Principles (APPs), considered the foundation of the privacy protection framework in the Privacy

[234] Federal Register of Legislation. (1988). *Privacy Act*.
[235] Office of the Australian Information Commissioner. (n.d.) *The Privacy Act*. https://www.oaic.gov.au/privacy/the-privacy-act

Act,[236] which applies to some private sector organisations and most Australian Government agencies. These are collectively referred to as 'APP entities.'

These principles were divided into five parts, respectively named as consideration of personal information privacy (i), collection of personal information (ii), dealing with personal information (iii), integrity of personal information (iv), and access to, and correction of, personal information (v).

It is important to highlight that although the Privacy Act does not directly include specific cybersecurity protections, it imposes obligations on entities that collect and manage personal information, creating a more secure and responsible domestic data environment. A good example is a precept brought under part four, regarding the security of personal information, which prescribes that if an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information from misuse, interference, and loss; and from unauthorised access, modification or disclosure.[237] It also commands that if an APP entity holds personal information that is no longer needed, and does not have any legal obligation to maintain it, it shall destroy the information or re-identified it.[238]

Consequently, this legislation can be used to make accountable APP entities that do not take such reasonable steps to protect personal information, this could be interpreted as not possessing adequate cyber defences and risk management plans, in case of a breach, for example.[239] So, even not dealing directly with the cyber threat problem, by incentivizing the build of a more solid environment for obtaining, storing, using, and disposing of private information, the act contributes to a scenario less prone to be victimized by cyberattacks, or, if attacked, it reduces the impact of such actions.

Of course, the term reasonable steps leave room for much discussion, so it is the responsibility of the Office of the Australian Information Commissioner (OAIC) to act and enforce the Privacy Act. The OAIC is an independent statutory agency in the Attorney-General's portfolio that has a range of powers and responsibilities under the Australian Information Commissioner Act 2010 (AIC Act)[240] and exercises powers under the Freedom of Information Act 1982 (FOI Act),[241] the Privacy Act, and other laws.[242]

To avoid this nebulosity, the OAIC provides a guide to assist organisations and agencies to prepare for and respond to data breaches in line with their obligations under this Act[243] and, since the Privacy Amendment (Notifiable Data Breaches) Bill 2016,[244] it has to be notified of eligible data breaches which occur when there is unauthorised access to, or disclosure of, information, and a reasonable person would conclude that the access or disclosure would likely result in serious harm to any of the individuals to whom the information relates (i); or Information is lost in circumstances where unauthorised access to, or unauthorised disclosure of, information is likely to occur and, if it did occur, a reasonable person would conclude that the access or

[236] Office of the Australian Information Commissioner. (n.d.) *Australian Privacy Principles*. https://www.oaic.gov.au/privacy/australian-privacy-principles
[237] Schedule 1, Article 11.1 of the Privacy Act 1988.
[238] Schedule 1 – Australian Privacy Principles, Article 11.2 of the Privacy Act 1988.
[239] APP 1 requires entities to take reasonable steps to establish and maintain practices, procedures, and systems to ensure compliance with the APPs.
[240] Australian Information Commissioner Act 2010, No.52, 2010.
[241] Federal Register of Legislation. (1982). *Freedom of Information Act 1982*. https://www.legislation.gov.au/Details/C2022C00056
[242] Office of the Australian Information Commissioner. (n.d.) *What We Do*. https://www.oaic.gov.au/about-us/what-we-do
[243] Office of the Australian Information Commissioner. (2019). *Data Breach Preparation and Respons*e. https://www.oaic.gov.au/__data/assets/pdf_file/0017/1691/data-breach-preparation-and-response.pdf
[244] Parliament of Australia. (2016). *Privacy Amendment (Notifiable Data Breaches) Bill 2016*. https://www.aph.gov.au/parliamentary_business/bills_legislation/bd/bd1617a/17bd052#:~:text=The%20purpose%20of%20the%20Privacy,Government%20agencies%2C%20some%20private%20sector

disclosure would be likely to result in serious harm to any of the individuals to whom the information relates(ii).[245] Penalties for non-compliance include fines of up to $420,000 for individuals and $2.1m for businesses.

For obvious strategic reasons, the Privacy Act is not imposed on several Australian intelligence and national security agencies, such as the Australian Commission for Law Enforcement Integrity, Australian Criminal Intelligence Commission, Australian Geospatial-Intelligence Organisation, Australian Secret Intelligence Service, Australian Security Intelligence Organisation, Australian Signals Directorate, Defence Intelligence Organisation, Office of National Intelligence.[246]

Radiocommunications Act 1992

The Act's main purpose is to manage the use of radio spectrum in a responsible and secure manner for commercial, defence purposes, national security, and other non-commercial purposes, while supporting the Australian government's communications goals.

There are several pertinent sessions for the cyberspace environment, Part 1.4 can be highlighted, which extends the concept of radiocommunications encompassing radio emission in connection with making astronomical or meteorological observations in the same way as it applies to a radiocommunication. Its applicability is also particularly interesting to the topic, the Act can be enforced on members of the crews of Australian aircraft, Australian vessels and Australian space objects, Australian aircraft, Australian space objects and Australian vessels,[247] and it also determines that it can be applied in outer space, although there is an evident debate of legislative competence in this sense.

In Part 4.2 are listed the offences related to radio emissions, which dictates that a person must not use a transmitter in a way likely to interfere with radiocommunications if the person knows that such interference is likely to prejudice the safe operation of a vessel, aircraft, or space object.

The Space Activities Act and the Space Activities Amendment (Launches and Returns) Act

To fulfil its space-related international obligations (see further), Australia enacted the Space Activities Act 1998,[248] a legal document focusing almost entirely on launch activities.

The Act decided on an approach dividing the licensing by the activity, introducing five permits; 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.[249] It also introduced a series of federal criminal offences.

[245] Office of the Australian Information Commissioner. (2019). *Part 1: Data Breaches and the Australian Privacy Act*. https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/part-1-data-breaches-and-the-australian-privacy-act

[246] Division 3 – Other matters, 7 Acts and practices of agencies, organisations, etc. of the Privacy Act 1988.

[247] It also can be enforced on foreign space objects, in the circumstances specified in a written determination by the Australian Communications and Media Authority (ACMA) (Part 1.4, Division 2).

[248] Federal Register of Legislation. (1998). *Space Activities Act 1998*. https://www.legislation.gov.au/Details/C2004C01013#:~:text=to%20establish%20a%20system%20for,regulated%20by%20this%20Act%3B%20and

[249] Froehlich, A., & Seffinga, V. (2018). *National Space Legislation: A Comparative and Evaluative Analysis*. Studies in Space Policy, vol 15. Springer, Cham.

Because the document was aimed at regulating launch activities, nothing relevant was mentioned relating to cybersecurity, this feature also persisted in the approved Space Activities Amendment (Launches and Returns) Act 2018.[250]

The Australian government, after identifying some flaws in the Space Activities Act, that did not stimulate the domestic launching industry as intended, comprehended the importance of being a part of the modern space market and decided to take the wheel into those necessary changes. The 2018 Act tries to keep up with the changes that happened in the Space scenario over the last decades, with the emergence of private actors as important players and the inclusion of new technologies, 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 those new technologies.[251]

The 2018 Act served to modernise the Space Activities Act, bringing significant changes, especially regarding insurance requirements,[252] regulations of launches from aircraft and high-power rockets,[253] amendments to the overall penalties,[254] and the inclusion of a mandatory Debris Mitigation Strategy[255] when applying for a Launch Permit and an overseas payload permit.

In case of accidents or incidents,[256] involving a space object or high-power 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 highly appealing 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.

Regarding cybersecurity, The Act establishes cybersecurity obligations in a broad manner. These obligations entail mandatory technology security plans, outlining procedures to safeguard technology at launch facilities and prevent unauthorized access, along with a cybersecurity strategy.[257]

[250] Federal Register of Legislation. (2018). *Space (Launches and Returns) Act 2018*. https://www.legislation.gov.au/Details/C2021C00394

[251] McGill, I., & Ye, C. (2019). *The Launches and Returns Act: one of the most significant updates to the Space Activities Act since its implementation*. Allens. 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/

[252] Space (Launches and Returns) Act 2018, Part 3, Division 7 especially.

[253] Space (Launches and Returns) Act 2018, Part 3, Division 4.

[254] Space (Launches and Returns) Act 2018, Part 3, Division 1 and Part 6.

[255] Space (Launches and Returns) Act 2018, Part 3, Division 3.

[256] Space (Launches and Returns) Act 2018, Part 7, Division 1.

[257] Shah, R. (2023). *Getting regulation right – Approaches to improving Australia's cybersecurity*. ASPI; Wheelahan, F., & Lee, K. (2020). *Launching a space industry: an overview of Australia's renewed space regulations.* https://www.corrs.com.au/insights/launching-a-space-industry-an-overview-of-australias-renewed-space-regulations

According to the Launch Facility License Applications Guideline 2022, the cybersecurity strategy can detail how security incidents and cyber threats on mission critical systems and networks would be detected. The Act also suggests consideration of the Strategies to Mitigate Cybersecurity Incidents and the Information Security Manual.[258] However, it's crucial to note that these documents lack specific provisions tailored to the unique aspects of the space sector.

The High-Power Rocket Permit Application Guidelines[259] also mandate a cybersecurity strategy but with fewer details than the Launch Facility License Application. It only requires an independent assessment of the strategy's adequacy by a qualified person not affiliated with the applicant. Strangely, the Act's Overseas Payload Permit section does not mention the need for a cybersecurity strategy, nor is it included in the Overseas Payload Permit Application Guidelines.[260]

It's important to emphasize that relying solely on a cybersecurity strategy as the primary defence is insufficient. Without addressing various other dependencies, this measure alone is unlikely to significantly enhance cybersecurity.[261]

The Cybercrime Legislation Amendment Act 2012

To fully aligned and adhere with the Council of Europe Convention on Cybercrime, Australia released its Cybercrime Legislation Amendment Act 2012,[262] presenting relevant changes to the Telecommunications (Interception and Access) Act 1979,[263] Mutual Assistance in Criminal Matters Act 1987 ('Mutual Assistance Act'),[264] Criminal Code Act 1995,[265] and the Telecommunications Act 1997.[266]

The amendments are related to the preservation regime for stored communications, mutual assistance, computer offences, telecommunications data confidentiality and other dispositions.

With the growing number of data exchanged between different sources, service providers were often not able to maintain records of it, which was a clear problem when dealing with investigations in cases of suspected criminal activity, for example.

Facing this issue, Schedule 1[267] of the Act mandates carriers to preserve targeted stored communications when demanded by certain domestic agencies or when requested by the Australian Federal Police (AFP) on behalf of other nations. Without this legislative change, this targeted information could be easily erased

[258] Australian Space Agency. (2022). *Launch Facility License Applications Guidelines*. Commonwealth of Australia. https://www.space.gov.au/sites/default/files/2023-11/launch_facility_licence_-_guidelines.pdf

[259] Australian Space Agency. (2023). *High Power Rocket Permit Application Guidelines*. Commonwealth of Australia. https://www.space.gov.au/sites/default/files/2023-11/high-power-rocket-permit-application-guidelines.pdf

[260] Australian Space Agency. (2022). *Overseas Payload Permit Application Guidelines*. Commonwealth of Australia. https://www.space.gov.au/sites/default/files/2023-11/overseas_payload_permit_-_guidelines.pdf

[261] Shah, R. (2023). Getting regulation right – Approaches to improving Australia's cybersecurity. ASPI.

[262] Federal Register of Legislation. (2012). *Cybercrime Legislation Amendment Act 2012*. https://www.legislation.gov.au/Details/C2012A00120

[263] Federal Register of Legislation. (1979). *Telecommunications (Interception and Access) Act 1979.* https://www.legislation.gov.au/Details/C2021C00341

[264] Federal Register of Legislation. (1987). *Mutual Assistance in Criminal Matters Act 1987*. https://www.legislation.gov.au/Details/C2021C00426

[265] Federal Register of Legislation. (1995). *Criminal Code Act 1995*. https://www.legislation.gov.au/Details/C2022C00065

[266] Federal Register of Legislation. (1997). *Telecommunications Act 1997*. https://www.legislation.gov.au/Details/C2019C00104

[267] According to The Explanatory Memorandum, this Schedule implements requirements of the Budapest Convention, particularly Articles 16 and 29.

while a warrant is being sought. It is important to point out that in cases in which the warrant is not granted, or if the grounds for seeking the order no longer exist, the information is destroyed.

The Act also strengthens international cooperation, as aimed by the Budapest Convention, ensuring, in Schedule 2,[268] that Australian agencies can obtain and disclose telecommunications data and stored communications for the purposes of foreign investigations.

In Schedule 3 the Act provides a series of amendments regarding computer offences, enhancing its scope, broadening the offences provisions, and removing gaps that could have existed between what was covered by the Commonwealth and what was covered by state's legislation. Schedule 4 imposes confidentiality to the existence of authorisations for the disclosure of information or documents made under Chapter 4—Access to telecommunications data of the TIA Act, as a response to the obligations of the Budapest Convention.

The most important characteristic of The Cybercrime Legislation Amendment Act is that it promotes Australia's compliance with the Budapest Convention, updating its cybersecurity legal framework and harmonising it with other parties' domestic legislation, creating a wider and more direct channel of communication between Australia and other states parties.

Telecommunications and Other Legislation Amendment Act

The Telecommunication and Other Legislation Act 2017,[269] also known as the Telecommunication Sector Security Reforms (TSSR), aims to reinforce a regulatory framework to manage national security risks of espionage, sabotage and foreign interference in Australia's telecommunications networks and facilities.[270]

By their nature, telecommunications networks and facilities possess sensitive information, part of this, for example, information concerning the personal data of customers, was already covered by the Privacy Act, nevertheless, there was still a gap regarding the protection of national security information that these entities also hold.

This is most importantly due to carriers and carriage service providers (C/CSPs) being vital for the delivery, support, and maintenance of other critical infrastructures, such as power and water,[271] hence, the disruption or the simple access to this information could be catastrophic for the country and it could leave Australia hostage to foreign states or non-state actors, so, rather than leaving this important role to the discretion of these entities and their dialogue with industry partners, the Australian government has taken steps to ensure that the due consideration to national security and the public interest would be incorporated to C/CSPs policies,[272] fostering collaboration of these entities directly with government agencies.

This was made through the formalization of obligations that these entities must comply with, inserting the government as a proper regulator of such activities to harden networks and facilities against unauthorised

[268] According to The Explanatory Memorandum, this Schedule implements requirements of the Budapest Convention, particularly Articles 30, 31, and 33 of the Convention.
[269] Federal Register of Legislation. (2017). *Telecommunications and Other Legislation Amendment Act 2017*. https://www.legislation.gov.au/Details/C2018C00385
[270] Parliament of Australia. (2017). *Telecommunications and Other Legislation Amendment Bill 2017*. https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=s1051
[271] Parliament of Australia. (2017). *Revised Explanatory Memorandum of the Telecommunications and Other Legislation Amendment Bill 2017.* https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/s1051_ems_37a7641a-7411-409c-82d9-1f5b945486c3/upload_pdf/644130.pdf;fileType=application%2Fpdf
[272] Ibid.

access and interference.[273] This requirement is applied to all C/CSPs, imposing that they 'do their best' to manage these risks, which means that what is required of an entity to comply with is directly proportional to the provider's risk profile.

The main changes brought by this Amendment are:

- **Security obligation**: imposes a security obligation on C/CSPs to do their best to manage the risk of unauthorised access and interference to networks and facilities they own, operate or use, to ensure the availability and integrity of networks and facilities and to protect the confidentiality of the information stored on and carried across them[274]
- **Notification obligation**: imposes a notification obligation on carriers and some carriage service providers to notify of planned changes to their systems and services that are likely to make the network or facility vulnerable to unauthorised access and interference, and providing for exemptions or partial exemptions from the requirement and the option to submit a Security Capability Plan to meet notification requirements[275]
- **Information gathering power**: provides the Secretary of Attorney-General's Department (AGD) an information gathering power to facilitate compliance monitoring and compliance investigation activity in relation to compliance with securities obligations[276]
- **Directions power**: providing the Attorney-General with further directions power to direct a C/CSP to do or not do a specified action[277]
- **Enforcement mechanisms**: provides enforcement mechanisms by extending the civil remedies regime prescript in Part 30 (injunctions), Part 31 (civil penalties), and Part 31A (enforceable undertakings) to address non-compliance with securities obligations, a direction, or notice to produce information or even documents. The Attorney-General would be authorised to commence proceedings to seek these remedies[278]

It becomes crystallised that the Australian government brought closer to itself the regulation of such important measures, directly dealing with national security matters within the C/CSPs, strengthening its role in the maintenance of a preserved cyber environment through the creation of pre-established directives and acceptable security quality standards.

This is important because, although privates, such entities contain vital sensitive information and the disruption or corruption of these can directly impact not only itself but national sovereignty in its most core matters, besides potentially causing billionaire losses that would certainly be felt for all Australian population.

The Security of Critical Infrastructure Act 2018

The Security of Critical Infrastructure Act 2018[279] 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

[273] Ibid.
[274] Ibid.
[275] Ibid.
[276] Ibid.
[277] Ibid.
[278] Ibid.
[279] Federal Register of Legislation. (2018) *Security of Critical Infrastructure Act 2018*. www.legislation.gov.au/Details/C2018A00029

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.

Four were the determined critical infrastructure assets under this Act, relating to electricity, port, water, and gas, being also considered as a critical infrastructure asset one related to a relevant industry declared as critical by the Minister.[280]

Recently, this piece of legislation was amended by the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022, seeking to adapt to the complex national security risks of sabotage, espionage and coercion posed by foreign involvement in Australia's critical infrastructure, and it has nowadays expanded coverage from the previous 4 sectors to 11 sectors, including communications, data storage or processing, space technology and defence industry.

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.

Telecommunications and Other Legislation Amendment (Assistance and Access) Act

The Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, also commonly known as the Assistance and Access Act supports national security agencies to adjust to the new current cyber scenario, especially related to encryption and other forms of electronic protection.

The amendments empower law enforcement and national security agencies to request, or compel, assistance from telecommunications providers (voluntary or mandatory industry assistance). It also established powers enabling law enforcement and intelligence agencies to acquire warrants to access data and amended the search warrant framework to expand the ability of criminal law enforcement agencies to collect evidence from electronic devices,[281] thus, giving effect to important prescriptions of the Budapest Convention.[282]

[280] Ibid. Section 9 (1) and Section 51 (1)

[281] Parliament of Australia. (2018). *Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*. https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/AmendmentsTOLAAct2018

[282] For example, provisions in Schedule 2 can be interpreted as giving effect to articles 19(1) and 19(2) of the Budapest Convention; Schedules 1 and 2 can be interpreted as giving effect to articles 20 and 21 of the Budapest Convention. TRUST BUT VERIFY A report concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and related matters, 2020, pg. 147/148.

These changes enhance industry cooperation with national security agencies, allowing certain governmental branches to access key information in specific situations and compensating such companies for all their reasonable costs related to the governmental requests.[283]

Obviously, for this intention, is the necessity of a warrant, which is the only instrument capable of allowing the lawful collection of evidence from electronic devices. An independent authority approves the use of these powers and agency activities are subject to oversight by the Commonwealth Ombudsman or the Inspector General of Intelligence and Security, by this process, agencies can operate around encryption, without undermining it, guaranteeing the privacy rights of its citizens.[284]

The Act is divided into 5 Schedules, which will be detailed below for a better and broader elucidation:

Perhaps the most important part brought by the Act is on Schedule 1, dealing specifically with industry assistance, stating that companies that provide communications services and devices in Australia have an obligation to help agencies, imposing a certain level acceptable of cooperability, on the assumption that would not be fair to expect unequal compliance from different providers.[285]

Section 317E brings what kind of assistance can be required from Australia's law enforcement and intelligence agencies,[286] including, but not limited to removing one or more forms of electronic protection that are or were applied by, or on behalf of, the provider,[287] doing an act or thing that facilitates giving effect to a warrant or authorisation or enables the effective receipt of information,[288] etc. While the list of the compulsory powers is exhaustive, the voluntary powers, under Section 317G are exemplary, not limited by it.

Contrary to what some misinformation propagated, the Act does not authorize agencies to request any kind of systemic weaknesses or backdoors into encrypted devices,[289] anything that could damage and destabilize the system is not authorised, hence the effectiveness of the encryption must be preserved, the Act merely provides ways to industry partners provide individual and pre-granted access to targeted specific information for government agencies.

The framework introduced by this Act, and particularly by this Schedule, operates in parallel with the existing obligation on C/CSPs to provide 'such help as is reasonably necessary' to agencies under section 313 of the Telecommunications Act. The directive of the present Act applies to a broader range of providers and helps agencies to better shape what kind of assistance is required.[290]

Schedule 2 creates computer access warrants, that must be issued by an independent authority, in case of serious offences (three years or more of maximum penalty offences). These warrants allow law enforcement

[283] Department of Home Affairs. (2018). *The Assistance and Access Act 2018*. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-encryption

[284] Ibid.

[285] Department of Home Affairs. (2023). *Assistance and Access: A New Industry Assistance Framework*. Commonwealth of Australia. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/assistance-and-access-industry-assistance-framework

[286] Ibid.

[287] Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, S317E 1A

[288] Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, S317E 1DA

[289] Department of Home Affairs. (2023). *Assistance and Access: A New Industry Assistance Framework*. Commonwealth of Australia. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/assistance-and-access-industry-assistance-framework

[290] Parliament of Australia. (2017). *Revised Explanatory Memorandum of the Telecommunications and Other Legislation Amendment Bill 2017.* https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/s1051_ems_37a7641a-7411-409c-82d9-1f5b945486c3/upload_pdf/644130.pdf;fileType=application%2Fpdf

to covertly access devices to investigate serious crimes, search devices such as laptops, mobile phones and USBs and collect information, and conceal the fact that a device has been accessed, but it cannot authorise interference with, or material loss or damage to, a computer.[291]

Solidifying this stronger approach, Schedules 3 and 4 allow police to gain access to account-based data via a search warrant, extend maximum penalties for some offences from the Crimes Act[292] and the Customs Act,[293] and extend the time available for examining electronic devices seized under a warrant.[294]

Lastly, Schedule 5 manages details regarding voluntary assistance for the Australian Security Intelligence Organisation (ASIO), providing civil immunity to persons who voluntarily assist the organisation, allowing ASIO to apply to the Attorney-General to require a person to unlock a device where they know the authentication protocol and creating a penalty for non-compliance.[295]

International Legal Framework

Australia is party to serval international treaties and institutional arrangements relevant to the protection of the space infrastructure from cyber threats. These span from customary law and general treaties such as the Budapest Convention and the UN Charter to treaties and soft law instruments specifically dedicated to cybercrime or the space sector.

With specific respect to space, Australia is one of the first members of the United Nations Committee on the Peaceful Uses of Outer Space (UNCOPUOS),[296] and one of the first to ratify all five relevant international space treaties. These are: the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies (The Outer Space Treaty - 1967),[297] the Agreement on the Rescue of Astronauts, the Return of Astronauts, and the Return of Objects Launched into Outer Space (The Rescue of Astronauts – 1968),[298] the Convention on International Liability for Damage Caused by Space Objects (the Liability Convention – 1972),[299] the Convention on Registration of Objects

[291] Department of Home Affairs. (2023). *Assistance and Access: Overview*. Commonwealth of Australia. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/assistance-and-access-overview

[292] Federal Register of Legislation. (1914). *Crimes Act*. https://www.legislation.gov.au/Details/C2022C00059

[293] Federal Register of Legislation. (1901). *Customs Act*. https://www.legislation.gov.au/Details/C2022C00061

[294] Department of Home Affairs. (2023). *Our Portfolio, National Security*. Commonwealth of Australia. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security

[295] Ibid.

[296] United Nations Office for Outer Space Affairs. (n.d.) *Committee on the Peaceful Uses of Outer Space: Membership Evolution*. https://www.unoosa.org/oosa/en/ourwork/copuos/members/evolution.html

[297] United Nations Office for Outer Space Affairs. (2023). *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*. https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html

[298] United Nations Office for Outer Space Affairs. (2023). *Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space*. https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introrescueagreement.html

[299] United Nations Office for Outer Space Affairs. (2023). *Convention on International Liability for Damage Caused by Space Objects*. https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introliability-convention.html

Launched into Outer Space (the Registration Convention – 1975),[300] and the Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (the Moon Treaty – 1979).[301]

Although not specifically intended to address cybersecurity issues, a variety of principles and norms embedded in these treaties can be used for this purpose and inform state behaviour in the space sector.

TABLE 13: INTERNATIONAL SPACE LAW

Treaty	Main Themes and Principles Relevant to Cyber Security
The Outer Space Treaty (1967)	It is the cornerstone of international space law and defines general principles and norms, some of which can be indirectly applied to cybersecurity, including the due regard principle and the need to avoid harmful interference.
	It prescribes that nations shall conduct their activities by avoiding harmful interference with other state's activities in the peaceful exploration and use of outer space
The Rescue Agreement (1968)	It is and extension of OST's Article V. It is built under the idea of astronauts as 'envoys of mankind', therefore deserving all possible help.
	It regulates the return of objects and people that have fallen into Earth.
The Liability Convention (1972)	It is a development of OST`s article VII.
	It brings some useful ideas to the cyber field, including the definition of damage and its approach to face legal disputes regarding liability; however, it lacks enforcing mechanisms, making it hard to implement.
The Registration Convention (1975)	It is a development of OST's article VIII and complements the Rescue Agreement and the Liability Convention since it creates the necessary conditions for the recognition of a space object and its Launching State.
The Moon Agreement (1979)	It focuses on both the juridical nature of the Moon and other celestial bodies and on the exploitation of their natural resources
	Due to its low ratification rate and the absence of ratifications from main space powers, the treaty has limited relevance. It has no relevance for cybersecurity

The Outer Space Treaty

The Outer Space Treaty (OST) is considered by most scholars the cornerstone of international space law. Although not specifically intended to address cybersecurity issues, the OST stipulates that the States shall carry on activities in accordance with international law, including the Charter of the United Nations, in the interest of maintaining international peace and security and promoting international cooperation and

[300] United Nations Office for Outer Space Affairs. (2023). *Convention on Registration of Objects Launched into Outer Space*. https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introregistration-convention.html

[301] United Nations Office for Outer Space Affairs. (2023). *Agreement Governing the Activities of States on the Moon and Other Celestial Bodies*. https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/intromoon-agreement.html

understanding,[302] that would logically prohibit any kind of cyberattacks between nations. At the same time, espionage – and by extension cyber espionage – has always been accepted as common practice and in accordance with international law.

The OST also determines that a State Party to the Treaty which has reason to believe that an activity or experiment planned by another State Party would cause potentially harmful interference with activities in the peaceful exploration and use of outer space, may request consultation concerning the activity or experiment.[303] This could in principle lead to the creation of a channel of communication between the nation victim of a cyberattack and the alleged perpetrator one.

Therefore, despite not dealing directly with the confrontation of current cyber threats, the OST brings a great axiological load that echoes to this day in the most modern pieces of legislation that more specifically deal with the theme. It erected the base in which all descendant legislation was built.

The Liability Convention

The Liability Convention[304] is another example of an important piece of legislation from the same period that also does not directly address cyber issues but that can be tangentially employed. This treaty is a direct offshoot of Article VII of the OST and imposes on the launching state liability for damages caused by its space objects to other states' space objects, defining damage as *damage to property of States or of persons, natural or juridical, or property of international intergovernmental organizations,*[305] that could be somehow useful when dealing with the damage caused by cyberattacks.

However, a complicating factor is that the liability is dependable on the place in which the damage occurred. If the damage was caused on the surface of the Earth or to an aircraft in flight, the Launching State is absolutely liable for it,[306] but if it is elsewhere other than on the surface of the Earth (outer space), the State is only liable if it occurred due to its fault or the fault of the people for whom it is responsible.[307] Since many cyberattacks occur on space systems, the difficulty still remains in proving the other party's fault or intent for the recognition of its liability.[308]

The Liability Convention is primarily concerned with the liability of states for damage caused by their space objects, which are defined as any object launched into outer space, including satellites. However, it is important to note that the Liability Convention does not specifically address liability for damage caused by cyberattacks. The Convention was developed during a time when space activities were primarily limited to physical launches and operations of satellites and did not contemplate the use of cyberattacks to cause damage to space objects.

That being said, if a cyberattack causes damage to a space object that is defined as a "space activity" under the Convention, such as a satellite, it is possible that liability could be established under the Convention. The Convention provides that the state that launched or procured the launching of the space object is liable for damage caused by the space object, regardless of whether the damage was caused by negligence or fault.

[302] The Outer Space Treaty, Article III.
[303] The Outer Space Treaty, Article IX.
[304] It is important to point out that the possible applicability of this piece of legislation refers to acts on this period, modern concepts of cyberattacks practically disable the Liability Convention use for this purpose.
[305] The Liability Convention, Article I A.
[306] The Liability Convention, Article II.
[307] The Liability Convention, Article III.
[308] The juridical term of 'absolute liability' can be explained as the liability that merely requires the proof of the damage and the identification of the responsible, once those are presented there are no exceptions that could excuse a state liability. It is opposed to 'strict liability', in which there are some exceptions that the state can claim.

This liability extends to damage caused on the surface of the Earth or to aircraft in flight and includes damage resulting from a collision with another object.

Therefore, if a cyberattack caused damage to a space object and that damage resulted in harm to persons or property on the surface of the Earth, liability could potentially be established under the Liability Convention, provided that the space object in question is defined as a "space activity" under the Convention. However, as previously noted, the application of the Liability Convention to cyberattacks is not straightforward and could be subject to interpretation and further legal developments.

Additionally, the Convention incentivises the diplomatic resolution,[309] nevertheless, if the question is not solved through diplomacy within one year, the parties shall establish a Claims Commission, at the request of either party,[310] this commission is composed of three members, one appointed from each side plus the Chairman, chosen by both parties, if they cannot agree on a Chairman either party may request for the UN Secretary-General to appoint one.[311]

There is not a hard-predetermined procedure for the Commission to follow, it shall determine its own process, the place where will sit, and other administrative matters.[312] This allows the States to create a more suitable method for both sides, which is still a very modern, flexible, and resolute way of solving legal disputes, ideal for nowadays space legal environmental. This extra-flexible approach was adopted in the convention aiming to obtain the maximum number possible of state parties, and it was well reflected in its adhesion numbers.

However, this style also brought a major flaw to this whole process: after all the procedure, the Commission's decision is not necessarily final and binding, and it is only put into place in those unlikely situations where 'the parties have so agreed.'[313] If the parties have not agreed that the Commission's decision would be final and binding, its determination only constitutes a recommendatory award to be considered in good faith by the parties.[314]

This represents a significant weakness in using this piece of legislation to deal with nowadays cyberattacks and pursuing effective compensation for damages, due to its lack of concrete legal measures to achieve a final reparation.

The Registration Convention

Closely linked to the Liability Convention, another legal tool from the Cold War era with some indirect relevance for cybersecurity is the Registration Convention, specifically Article VI. The article is a well-intended effort and finds root in general international cooperation principles, declaring that if a state is not able to identify a space object which caused damage, other State Parties, in particular the ones that possess space monitoring and tracking facilities, shall help it, *responding to the greatest extent feasible to a request by that State Party, or transmitted through the Secretary-General on its behalf, for assistance under equitable and reasonable conditions in the identification of the object.*[315]

The Constitution and Convention of the International Telecommunication Union

[309] The Liability Convention, Article IX.
[310] The Liability Convention, Article XIV.
[311] The Liability Convention, Article XV.
[312] The Liability Convention, Article XVI.
[313] The Liability Convention, Article XIX.
[314] Freeland, S. (2001). *There's a Satellite in My Backyard - Mir and the Convention on International Liability for Damage Caused by Space Objects*. University of New South Wales Law Journal, vol. 24, no. 2, p. 483. HeinOnline.
[315] The Registration Convention, Article VI.

Another pertinent piece of international legislation is the Constitution and Convention of the International Telecommunication Union (ITU Convention),[316] presented in 1989, but not receiving the necessary number of ratifications, only started to become relevant in 1992, after a thorough revision at the 1992 Additional Plenipotentiary Conference held in Geneva.[317]

The convention declares that *to promote the use of telecommunication services with the objective of facilitating peaceful relations*[318] it shall *coordinate efforts to eliminate harmful interference between radio stations of different countries and to improve the use made of the radio-frequency spectrum for radiocommunication services and of the geostationary-satellite and other satellite orbits*.[319]

It also asserts, in article 45, that *all stations, whatever their purpose, must be established and operated in such a manner as not to cause harmful interference to the radio services or communications*, but, like other legislation, it does not prescribe a solid procedure in the event of non-compliance with these determinations, using a similar approach than the Liability Convention's one, determining a settlement of disputes process' that privileges diplomacy and the use of procedures established by bilateral or multilateral treaties concluded between the states.[320] It should be also noted, however, that within the ITU context harmful interferences typically refer to electronic or radio frequency interferences which, as explained in Section 2, do not necessarily include cyberattacks (see focus box p. 23).

While Electromagnetic interference (EMI), radio frequency interference (RFI) and cyberattacks can all have serious consequences for electronic and communication systems, they differ in their causes and effects. The direct applicability of the ITU Convention to cases of cyberattack to space systems could therefore prove contentious.

Arguably, the most important precept of the ITU Convention is its article 4, which lists the Constitution of the ITU as an instrument of the Union. The ITU enacts rules Administrative Regulations, treaties binding to all member parties, Radio Regulations, also binding, and Telecommunications Standards (non-binding).[321] It also elaborates Digital Skills Toolkits, aiming to provide policymakers and other stakeholders with practical information, examples, and step-by-step guidance to develop a national digital skills strategy,[322] a valuable document, especially for nations that do not have know-how in this area but are seeking to build their national systems.

The Council of Europe Convention on Cybercrime

The Council of Europe Convention on Cybercrime, popularly known as the Budapest Convention,[323] is the first important international treaty that deals specifically with crimes committed via cyberspace and violations of network security. It was created recognising the need for cooperation between States and private industry in combating cybercrime, intending to build a common criminal policy aimed at the protection of society against cybercrime by harmonising national legislations and fostering international collaboration.[324]

[316] International Telecommunication Union. (1992). *Final Acts of the Additional Plenipotentiary Conference, Constitution and Convention of the International Telecommunication Union, Optional Protocol Resolutions Recommendation*.

[317] International Telecommunication Union. (n.d.) *Constitution and Convention Collection*. https://www.itu.int/en/history/Pages/ConstitutionAndConvention.aspx#

[318] ITU Convention, Article 1, 1e.

[319] ITU Convention, Article 1, 2b.

[320] ITU Convention, Article 56.

[321] Hathaway, O. A., et al. (2012). *The Law of Cyber-Attack*. California Law Review 100, no. 4, 817-886.

[322] International Telecommunication Union. (n.d.) *Digital Skills Toolkit*. https://academy.itu.int/itu-d/projects-activities/research-publications/digital-skills-toolkit

[323] Council of Europe. (2001). *Convention on Cybercrime*.

[324] The Budapest Convention, Preamble.

The idea is that aligning multiple domestic laws, centring on common principles, should facilitate the dialogue, cooperation and exchange of information when targeting these crimes, even if committed in other States. This harmonization is desired not only during the prosecution phase but also in the detection and investigation.[325]

The Convention has a wider scope than only targeting pure cybercrimes like deploying malicious software, also encompassing cyber-enabled crimes such as terrorism and child exploitation material.

The Convention does not specifically address the issue of cyberattacks on critical infrastructure or other systems that could potentially have an impact on public safety or national security. Instead, the Convention focuses on a range of other types of cybercrime, including offenses related to computer systems and data, network intrusions, and online fraud.

However, the Convention does contain provisions that could be used to address certain types of cyberattacks. For example, Article 2 of the Convention requires parties to criminalize a range of activities related to the unauthorized access, interference, or interception of computer systems and data. Article 3 requires parties to criminalize the production and dissemination of tools, such as malware, that are designed to commit cybercrime. Article 10 requires parties to establish procedures for the expedited preservation of data related to cybercrime, which could be important in the investigation and prosecution of cyberattacks.

In addition to these specific provisions, the Convention also includes general principles related to the prevention and investigation of cybercrime, including the need for effective cooperation between law enforcement agencies and other relevant stakeholders, the importance of protecting the rights of individuals, and the need for adequate resources and training to address the problem of cybercrime.

In summary, while the Budapest Convention does not specifically address cyberattacks on critical infrastructure or other systems, it does contain provisions and general principles that could be used to address certain types of cyberattacks, and it provides a framework for international cooperation and legal harmonization to address the broader problem of cybercrime.

To be able to fully scrutinize and prosecute these crimes, the document incentivises state parties to empower their competent authorities' investigative technological apparatus so that they can efficiently perform several complex tasks, such as a real-time collection of traffic data[326] and interception of content data.[327]

The Convention had two additional protocols, the first one related to the criminalisation of acts of a racist and xenophobic nature committed through computer systems[328] and the second being related to enhanced cooperation and disclosure of electronic evidence.[329]

This second additional protocol was created taking into consideration the reality of the rapidly changing cyber environment nowadays, in which ordinary legal forms and processes, due to their slowness, can result in impunity. Because of this, it brings some controversial and debatable prescriptions, in particular article 7, disclosure of subscriber information, that raises concerns related to abusive requests, the scope of the

[325] The Budapest Convention, Preamble.
[326] The Budapest Convention, Article 20.
[327] The Budapest Convention, Article 21.
[328] Council of Europe. (2003). *Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems*.
[329] Council of Europe. (2022). *Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence*.

definition of disclosure of personal and sensitive data, and the infringement of the national sovereignty of states relating to the privacy of its citizens.[330]

The UN GGE Reports 2013, 2015, and 2019 - 2021

In 2004 the United Nations General Assembly established the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (UN GGE), six of which occurred since then, being highlighted as most impacting the outcomes from GGE 2013 and GGE 2015, bringing welcomed innovations in the international legal scenario, and the last one, the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (GGE 2019-2021)[331] that reaffirms and clarify much of the previous directives.

The GGE 2013 Final Report was a pioneer to declare the applicability of international law and in particular the United Nations Charter on cyberspace, being essential to maintaining peace and stability and promoting an open, secure, peaceful, and accessible ICT environment, but it did not delineate how such norms apply to State behaviour and the use of ICTs by States.[332]

The Australian position on this applicability became more palpable and clearer when further revealed by the International Cyber Engagement Strategy (2017) and especially by Australia's International Cyber and Critical Tech Engagement Strategy's Annex B: Australia's position on how international law applies to State conduct in cyberspace. The GGE 2013 final report also suggests the adoption of voluntary measures to promote trust and assurance among States, increasing predictability and reducing misperception.[333]

Developing the ideas of the previous report, the GGE 2015 Final Report agreed on 11 Norms of Responsible State Behaviour in Cyberspace, these norms reflect the international community's expectations, allowing it to assess the activities and intentions of States. These norms are composed of 8 positive actions, that the state is encouraged to take, and 3 others that it should avoid. It also provides more comments on how international law would apply to the cyber environment including some basic international principles such as state sovereignty, sovereign equality, non-intervention in the internal affairs of other states, respect for human rights and fundamental freedoms.

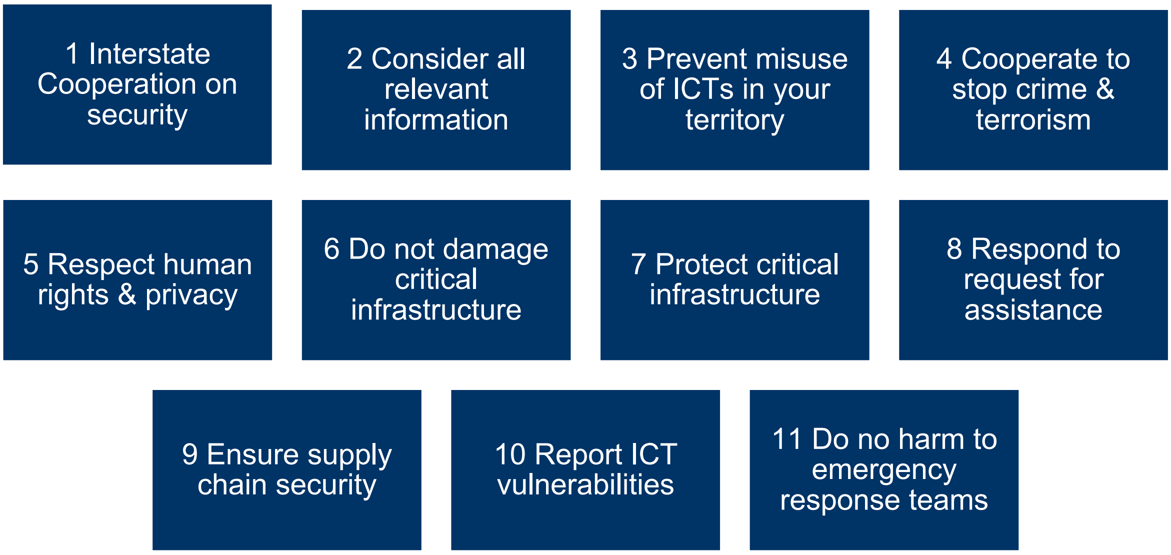
[330] Electronic Frontier Foundation. (n.d.) *Joint Civil Society Response to the Provisional Draft Text of the Second Additional Protocol to the Budapest Convention on Cyber Crime*. https://www.eff.org/document/eff-comments-additions-budapest-protocol-cybercrime

[331] United Nations. (n.d.) *Group of Governmental Experts*. https://www.un.org/disarmament/group-of-governmental-experts/

[332] United Nations. (2013). *Group of Governmental Experts 2013 Final Report*. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf?OpenElement

[333] Ibid. p.9.

FIGURE 22: UN NORMS OF RESPONSIBLE STATE BEHAVIOUR IN CYBERSPACE (SOURCE: UN)



1 Interstate Cooperation on security

2 Consider all relevant information

3 Prevent misuse of ICTs in your territory

4 Cooperate to stop crime & terrorism

5 Respect human rights & privacy

6 Do not damage critical infrastructure

7 Protect critical infrastructure

8 Respond to request for assistance

9 Ensure supply chain security

10 Report ICT vulnerabilities

11 Do no harm to emergency response teams

The most recent GGE (2019-2021), in its final report, reaffirms the recommendations of the 2010, 2013 and 2015 GGE consensus reports,[334] acknowledging the important role of regional and sub-regional bodies in developing region-specific mechanisms and strengthening capacity-building efforts to support their implementation.[335]

It also reiterates the necessity of an open, secure, stable, accessible, and peaceful Information and Communications Technology (ICT) environment, demonstrating concern related to ICT threats identified in previous reports such as states' ICT capabilities for military purposes that can pose a significant threat to stability, economic and social development of other nations.[336]

The report also states preoccupation with the malicious use of ICTs against critical infrastructure that provides essential services to the public, domestically, regionally, or globally,[337] with the use for political and other purposes, acting on information campaigns to influence the processes, systems, and overall stability of another State,[338] and with the exploitation, via cyber destabilisation, of vulnerabilities in a broader sense.[339]

Most important is the report's reaffirmation of the applicability of international law and in particular the Charter of the United Nations to the ICT environment,[340] declaring that norms and existing international law sit alongside each other and that the voluntary use of these can help the maintenance of international peace, security, and stability.[341]

Also, in accordance with the content of the 2015 report of the GGE, and expanding its directives, the GGE 2019 has developed an additional layer of understanding of the11 voluntary GGE 2015 norms, underscoring

[334] Ibid.
[335] Ibid.
[336] United Nations. (2021). *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*. Section II. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/075/86/PDF/N2107586.pdf?OpenElement
[337] Ibid.
[338] Ibid.
[339] Ibid.
[340] Ibid.
[341] Ibid. Section III.

their value regarding the expected behaviour of States in their use of ICTs in the context of international peace.[342]

It is advised by the group on the use of Confidence-building measures (CBMs) for the promotion of trust, cooperation, and transparency, resulting in a stable and peaceful ICT environment. The CBMs are long-term and progressive commitment, requiring the sustained engagement of States,[343] and a number of these cooperative measures is highlighted, including Points of Contact (PoCs) and Dialogue and consultations.

In relation to Points of Contact, states are encouraged to consider appointing PoCs at the policy, diplomatic, and technical levels and creating inter-and intra-governmental procedures to guarantee their effective communication during crises,[344] also to draw lessons and good practices from regional PoC networks to use it beyond, in national, regional, and international contexts. Besides this, it also incentivizes dialogue through bilateral, sub-regional, regional, and multilateral consultations and engagement to advance understanding between States.

Strengthening this collaborative approach, the GGE lists some areas in which states can mutually beneficiate from cooperation and assistance in ICT security and capacity building,[345] reaffirming the importance of a peaceful, transparent, and responsible ICT environment, identifying potential areas for future work, and encouraging States to continue efforts to further the framework of responsible State behaviour within the United Nations and other regional and multilateral forums.[346]

International Cooperation

Australia has signed several agreements and cooperation formats with a several countries on both a bilateral and multilateral level. These are reported hereby.

Bilateral Agreements	Date of Signature
Australia-Singapore MOU on Cyber Cooperation[347]	2017
Australia-Papua New Guinea MOU on Cyber Cooperation[348]	2018
Australia-Indonesia MOU on Cyber Cooperation[349]	2018
Australia-Thailand MOU on Cyber Cooperation	2019

[342] Ibid.
[343] Ibid. Section V.
[344] Gavrilović, A. (2021). *What's New with Cybersecurity Negotiations? The UN GGE 2021 Report.* Diplo. www.diplomacy.edu/blog/whats-new-with-cybersecurity-negotiations-the-un-gge-2021-report/
[345] United Nations. (2021). *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*. p.21. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/075/86/PDF/N2107586.pdf?OpenElement; Gavrilović, A. (2021). *What's New with Cybersecurity Negotiations? The UN GGE 2021 Report*. Diplo. www.diplomacy.edu/blog/whats-new-with-cybersecurity-negotiations-the-un-gge-2021-report/
[346] United Nations. (2021). *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*. Section VII. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/075/86/PDF/N2107586.pdf?OpenElement
[347] Renewed by the Renewed Australia-Singapore MOU on Cyber Cooperation (2020).
[348] Renewed by the Renewed Australia-Papua New Guinea MOU on Cyber Cooperation (2022).
[349] Refreshed and expanded by the Expanded Australia-Indonesia MOU on Cyber and Emerging Cyber Technology Cooperation (2021).

Australia-India Cyber and Critical Technology Partnership	2020
Australia-Republic of Korea MOU on Cyber and Critical Technology Cooperation	2021
Australia-Republic of Korea MOU on a Digital Cooperation Initiative in Southeast Asia	2021
Australia-UK Cyber and Critical Technology Partnership	2022

On a multilateral level, Australia engages in initiatives such as the ASEAN Regional Forum's (ARF) ICT work stream, the inaugural Open Ended Working Group (OEWG) (A/Res/73/27), and a sixth Group of Governmental Experts (GGE) (A/Res/73/266).[350]

Australia also leads the Cyber and Critical Tech Cooperation Program across the Indo-Pacific region to improve cyber resilience in a consistent manner with priorities identified in Australia's International Cyber and Critical Technology Engagement Strategy, partnering with many countries, including Brunei, Cambodia, Thailand, Laos, Malaysia, Singapore, Vietnam, Indonesia, Timor-Leste, Papua New Guinea, and most of the Pacific Islands.

3.2 Applicability of the Policy and Legal Framework

In this section, we provide an analysis of the applicability of the above discussed legal and regulatory documents dealing with the cybersecurity of the space infrastructure to the considered use cases. The Section pays consideration to both domestic legislations (e.g., the Cybercrime Legislation Amendment Act of 2012, the Privacy Amendment Act of 2017, the Telecommunications and Other Legislation Amendment Act of 2017, etc.) and of the international legal regimes (e.g., the Outer Space Treaty, ITU Convention, the Budapest Convention, etc.) Australia has ratified. For each use case, some general and specific questions were addressed.

- How is this specific risk taken into account in Australia?
- Are current policies and regulations addressing this menace?
- Are there any specific procedures to be followed?
- Is any improvement required on the policy side?

For each case, the analysis was complemented with the results of ad-hoc consultations undertaken in a dedicated workshop. Beyond questions pertaining to the applicability and maturity of the policy and legal framework to the cases, during the consultation, participants were asked to assess the type of challenges and solutions that each use case implied. Specifically:

- Policy challenges refer to issues related to acknowledging and integrating the cyber threats on space infrastructure in policy documents, public speeches, and official addresses and ensuring the consistency between space and cyber policies. This type of challenges can also arise from the lack of

[350] The participation in such multilateral approaches can be better understood through the analysis of the document Australia's position on the application of international law to state conduct in cyberspace.

dialogue between the multiplicity of sources that create such policies, e.g., state and Commonwealth, which may result in conflicting policies.

- Legal challenges include challenges related to applicability of Australian laws to a wide range of cyberattack types against space systems to protect manufacturers, operators, and users as well as the integration of legally binding cybersecurity obligations for space operators and manufacturers to better protect the space sector at large. This type of challenge can also stem from the lack of specific legislation on the theme or the inadequacy between the international treaties that a state is a signatory and the country's domestic legal framework, which is supposed to reflect such treaties (for instance, the Cybercrime Legislation Amendment Act 2012 was a key tool to align the Australian framework to the Budapest Convention).
- Governance challenges relate to the clear and identified mandate for space cybersecurity in public institutions as well as adapted fora for intergovernmental or intersectoral management and information sharing regarding space cybersecurity; This form of challenge is related to how the governmental bodies are prepared to respond to a certain situation, if their internal organization is clear and sufficient and if it is easily perceived and plainly understood by the stakeholders involved in that situation, that is, if the stakeholders can easily identify what is the correct governmental branch to address a situation and what is the official procedure that it dictates for that scenario.
- Behavioural challenges pertain to human or organisational behaviours that should be conducive to implement best practices, raise awareness among space sector professionals, and cyber situational awareness. Behavioural challenges are associated to relevant human action, an incorrect human act that can lead to an undesired situation, despite the existence of proper technical, governance, legal and policy procedures. Although related to human action, which is by nature always unpredictable, this challenge can be mitigated through correct training and surveillance.
- Technical challenges pertain to security controls and operational measures that can be implemented on systems to better protect them such as encryption, QKD, hardening, redundancy, etc. In this context, technical challenges are correlated to hardware and software fragilities in the space infrastructure. They are also related to the lack of technical knowledge to perform, investigate, or report a certain situation.

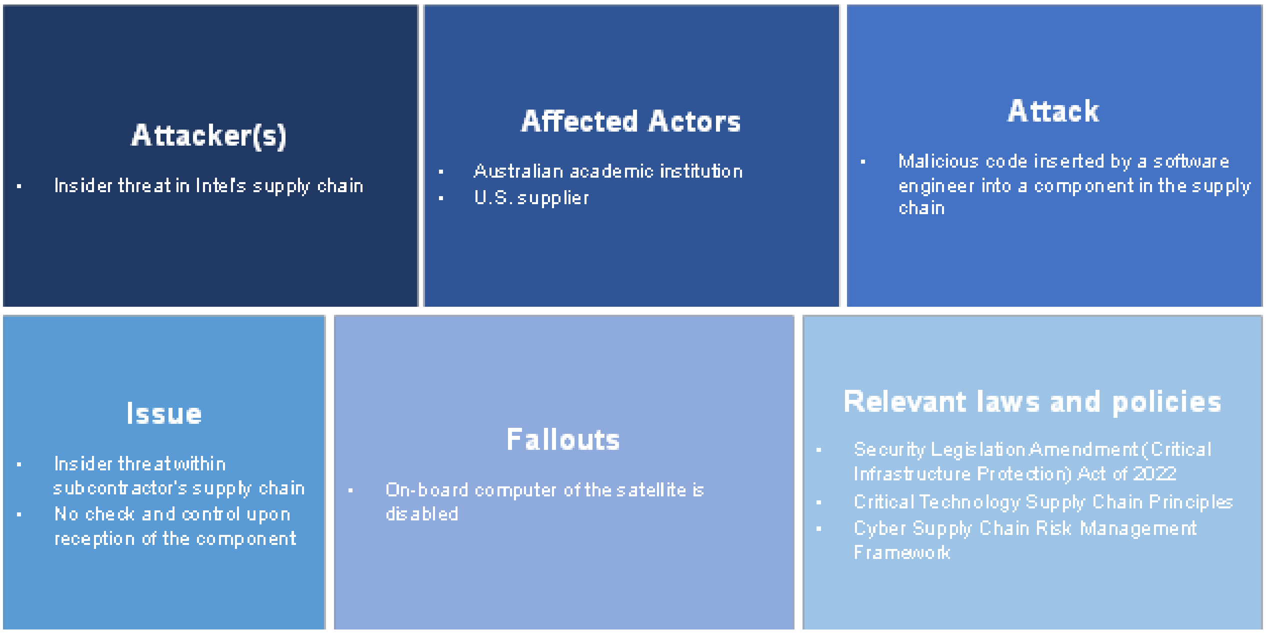
3.2.1 Use Case 1: The Software Supply Chain

An Australian academic institution is developing a nanosatellite for Scientific, Technology, and Education demonstration, relying on COTS components for software, firmware, and hardware. The university orders COTS for the On-Board Computer and decide to use a 220 MHz StrongARM 32-bit SA1100 RISC processor manufactured by Intel, which had its own supply chain compromised. In this compromised supply chain, a software engineer has access privileges within the software development environment and inserts hidden malicious code (e.g., a logic bomb) in the processor during the testing process to prevent any detection. Intel was not able to detect the malicious code. As the nanosatellite is being developed by a university, the university did not have the technical and financial means to further test the processor to detect the malicious code either. While the malicious code does not prevent the basic operations of the nanosatellite, the On-Board Computer provides automatic control of the spacecraft, which are disabled by the malicious code.

Overview

Based on the workshop conducted with Australian industrial stakeholders, attacks on the supply chain represent the most concerning type of attack on the Australian space infrastructure. Key elements of this specific use case are summarised below:

FIGURE 23: MAJOR ELEMENTS OF USE CASE 1



Attacker(s)

- Insider threat in Intel's supply chain

Affected Actors

- Australian academic institution
- U.S. supplier

Attack

- Malicious code inserted by a software engineer into a component in the supply chain

Issue

- Insider threat within subcontractor's supply chain
- No check and control upon reception of the component

Fallouts

- On-board computer of the satellite is disabled

Relevant laws and policies

- Security Legislation Amendment (Critical Infrastructure Protection) Act of 2022
- Critical Technology Supply Chain Principles
- Cyber Supply Chain Risk Management Framework

Relevant Laws and Policies

From a legal perspective, Australia considers space as a critical infrastructure. Therefore, the **Security Legislation Amendment (Critical Infrastructure Protection) Act of 2022**[351] may apply to this case. However, while space technology is considered as a critical infrastructure, it is not clear whether a satellite developed by a university for Scientific, Technology, and Education demonstration fits in the law's definition of a critical infrastructure. The Act defines space technology sector as *'the sector of the Australian economy that involves the commercial provision of space-related services'*, which does not seem to include university demonstration nanosatellites that are not used for commercial services. Furthermore, the Act provides examples of space-related services such as *'position, navigation and timing services in relation to space objects; space situational awareness services; space weather monitoring and forecasting; communications, tracking, telemetry and control in relation to space objects; remote sensing earth observations from space; facilitating access to space.'* As there are listed as examples, it likely suggests that the list is not exhaustive. However, it is unlikely that the university's nanosatellite fits into the scope of the Act. Yet, it does not prevent the university to report the incident on the website of the ACSC.

The Security Legislation Amendment (Critical Infrastructure Protection) Act of 2022 requires responsible entities to create, and follow, a critical infrastructure risk management program to reduce material risks on the critical asset. Entities must consider supply chain risks as part of an 'all-hazard approach' to reduce the risk of disruption, malicious or otherwise, or exploitation of critical supply chains leading to a disruption of the critical infrastructure asset. Yet, it does not seem that space assets, which are not related to defence or broadcasting, must apply this risk management program.

Workshop participants confirmed our assessment and outlined that since it is a CubeSat and that the processor is a non-critical cheap COTS component, no specific legislation would apply.

[351] Department of Home Affairs. (2022). *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022.*

Several stakeholders also pointed out that ISO Standards may apply such as ISO/IEC 27036-3:2013, which provides guidance on product and service acquirers and suppliers in the information and communication technology (ICT) supply chain, into:

- gaining visibility into and managing the information security risks caused by physically dispersed and multi-layered ICT supply chains;
- responding to risks stemming from the global ICT supply chain to ICT products and services that can have an information security impact on the organizations using these products and services. These risks can be related to organizational as well as technical aspects (e.g., insertion of malicious code or presence of the counterfeit information technology (IT) products);
- integrating information security processes and practices into the system and software lifecycle processes, described in ISO/IEC 15288 and ISO/IEC 12207, while supporting information security controls, described in ISO/IEC 27002.

These aspects would have provided guidance to the university regarding the cybersecurity of the supply chain to automatically check received components even if it leads to additional costs.

Moreover, the relevant policy and legal framework, which applies to this case may be found in soft law and best practices case such as the **Critical Technology Supply Chain Principles,**[352] which are non-legally binding principles and intended to be used as a tool to assist governments and businesses in protecting their supply chains.

TABLE 14: CRITICAL TECHNOLOGY SUPPLY CHAIN PRINCIPLES (SOURCE: HOME AFFAIRS)

Agreed Pillars	Agreed Principles
Security-by-Design Security should be a core component of critical technologies. Organisations should ensure they are making decisions that build in security from the ground-up	**1.** Understand what needs to be protected, why it needs to be protected and how it can be protected
	2. Understand the different security risks posed by your supply chain
	3. Build security considerations into all organisational processes, including into contracting processes, that are proportionate to the level of risk (and encourage suppliers to do the same)
	4. Raise awareness of and promote security within your supply chain
Transparency Transparency of technology supply chain is critical, both from a business perspective and a national security perspective	**5.** Know who critical suppliers are and build an understanding of their security measures
	6. Set and communicate minimum transparency requirements consistent with existing standards and international benchmarks for your suppliers and encourage continuous improvement

[352] Australian Government. (2021). *Critical Technology Principles*. https://www.homeaffairs.gov.au/cyber-security-subsite/files/critical-technology-supply-chain-principles.pdf

	7. Encourage suppliers to understand and be transparent in the depth of their supply chains, and be able to provide this information to customers
Autonomy and Integrity Knowing that your suppliers demonstrate integrity and are acting autonomously is fundamental to securing your supply chain	**8.** Seek and consider the available advice and guidance on influence of foreign governments on suppliers and seek to ensure they operate with appropriate levels of autonomy
	9. Consider if suppliers operate ethically, with integrity, and consistently with international law and human rights
	10. Build strategic partnering relationships with critical suppliers

Other tools developed by the Australian Cyber Security Centre may also help the Australian university in this case as the Australian Government provides cybersecurity advice to businesses through initiatives such as the **Cyber Supply Chain Risk Management Framework** or **the Essential Eight Maturity Model**[353] to adopt best practices and cyber hygiene.

More particularly, the **Information Security Manual** focuses on measures that can be applied to protect the supply chain, clearly define responsibility between suppliers and customers, and ensure that suppliers are implementing cybersecurity best practices. With regard to the present case, the implementation of ISM 1790 (applications, ICT equipment and services are delivered in a manner that maintains their integrity.), ISM 1791 (the integrity of applications, ICT equipment and services are assessed as part of acceptance of products and services.), and ISM 1792 (the authenticity of applications, ICT equipment and services are assessed as part of acceptance of products and services.) would have likely mitigated this attack.[354]

However, as they are not compulsory frameworks, the Australian university does not have to implement them and may not be aware that these mechanisms exist to assist its space-related activities as neither the Framework nor the Essential Eight model explicitly mention space.

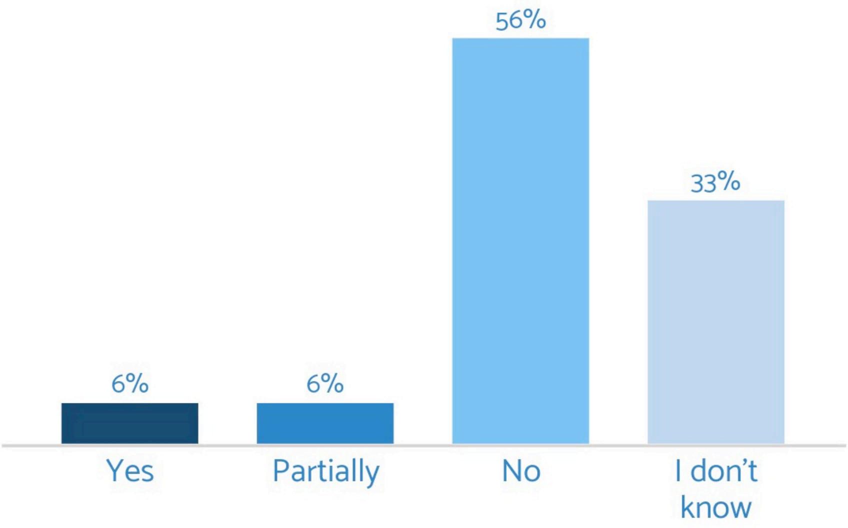
Elements for Consideration and Assessment

Despite some relevant policy and legal instruments, the applicability of current policies and law to this case remains limited. Not surprisingly, 56% of workshop participants considered that current policies and regulations do not address this type of threat. Only 6% of them considered that this type of threat is covered in the policy and legal framework. 33% of respondents did not know, an occurrence suggesting that awareness raising activities may be needed.

[353] Australian Cyber Security Centre. (2022). *Essential Eight Maturity Model*. Commonwealth of Australia. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model

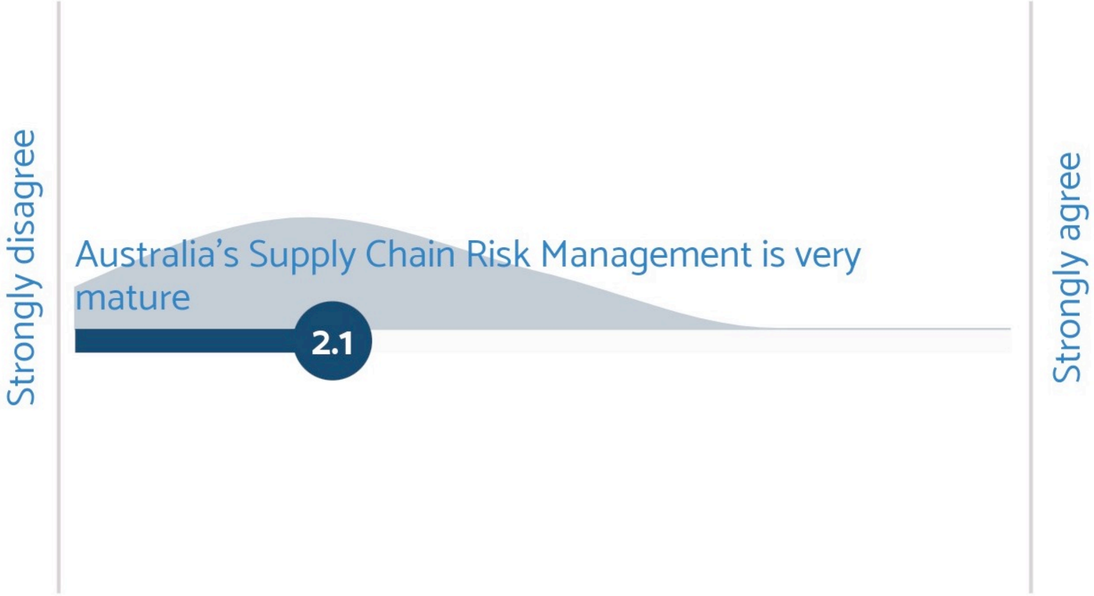
[354] Australian Cyber Security Centre. (2023). *Information Security Manual*. Commonwealth of Australia. p.17. https://www.cyber.gov.au/sites/default/files/2023-09/Information%20Security%20Manual%20%28September%202023%29.pdf

FIGURE 24: ARE CURRENT POLICIES AND REGULATIONS ADDRESSING THIS TYPE OF THREAT?



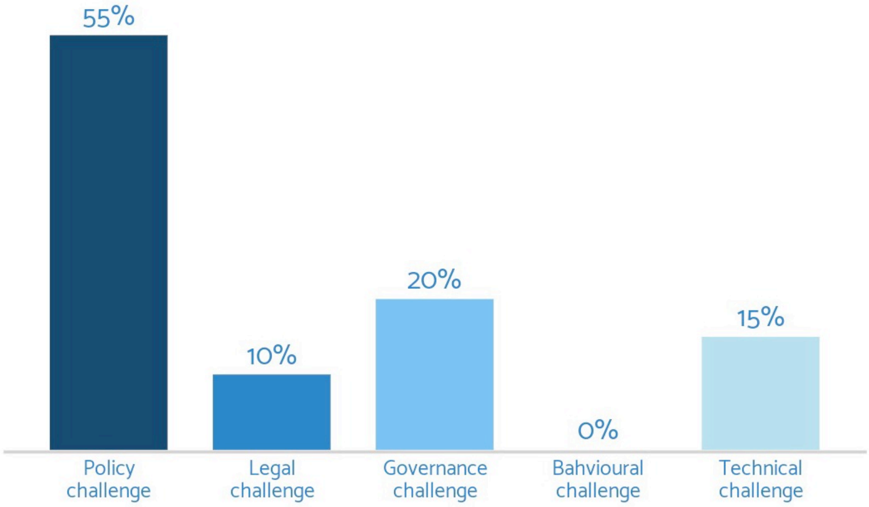
Overall, workshop participants rated the maturity of Australia's supply chain risk management as relatively low (2.1 out of 5).

FIGURE 25: STATEMENT ASSESSMENT



No law compels a university to supply chain risk management and automatic checking of components to screen vulnerabilities and cyber threats, so it can be assessed that there is some sort of legal gap. However, 55% of workshop participants considered that this issue is mostly a policy challenge rather than a legal challenge (10%) or a governance challenge (20%) or a technical challenge (15%). Indeed, while policy documents do provide guidelines on supply chain risks management and supply chain cyber risks, they do not specify best practices for checking non-critical components upon reception that will be used by a university.

FIGURE 26: MOST CRITICAL TYPE OF CHALLENGE ASSOCIATED WITH USE CASE 1



The current legislation does not necessarily cover the specifics of this particular case. However, standards, best practices and frameworks do raise awareness about supply chain cybersecurity and provide guidelines. The biggest issue is that best practices are not compulsory. Nonetheless, it was difficult to find any policy document that would somehow relate to the situation of the use case. While there is a policy and legal gap, there is not necessarily a need to adopt a law for universities on this issue. However, awareness raising on cybersecurity of the space supply chain should be emphasized beyond businesses and government actors as universities are a major part of the Australian space program.

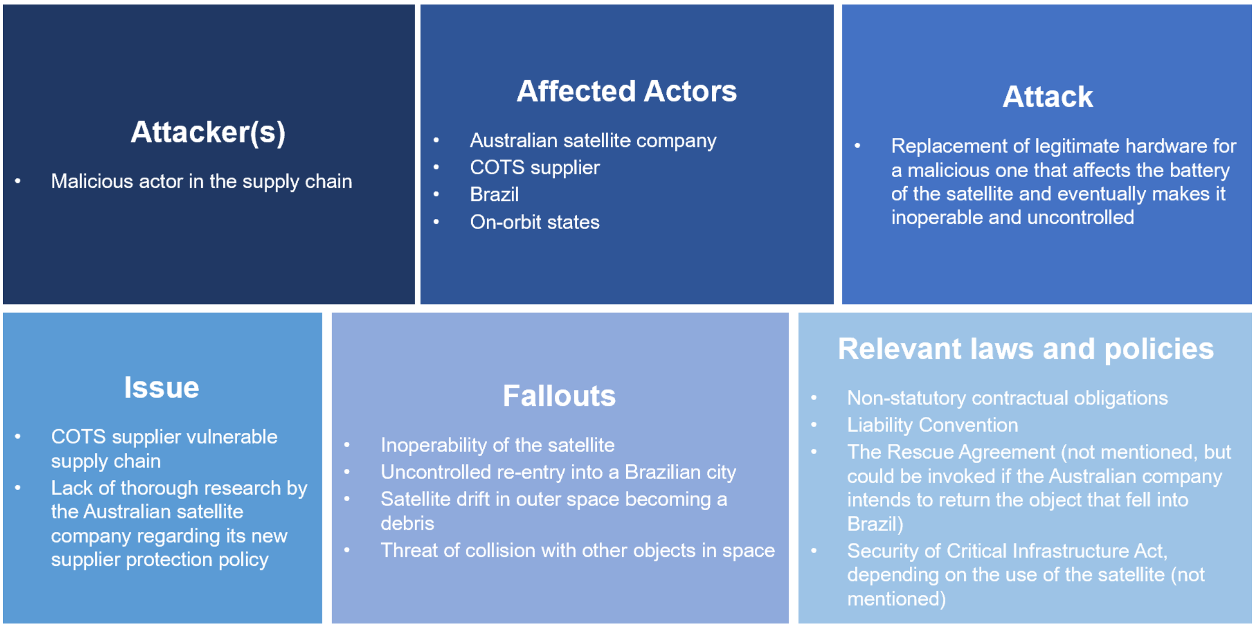
3.2.2 Use Case 2: The Hardware Supply Chain

An Australian company is relying on COTS components for some pieces of hardware. The company orders a CAN micro-controller to include in the power system to measure solar array temperatures and voltages from a trusted and known supplier. Due to supply chain delays following the COVID-19 pandemic and the shortage in semi-conductors, the company decides to change its supplier for another to keep its project on track. However, the Australian satellite company is not aware that this supplier has a less protected supply chain. As a result, a legitimate hardware was replaced by a malicious component in the supply chain by an adversary, who had access to the plant in charge of the welding and therefore had access to the micro-controller. The malicious hardware added to the micro-controller is an additional battery charge regulator, which is supposed to implement maximum-power point tracking, but instead contains a malicious software, which tells the system that is constantly overcharged when it is not. This leads the battery charge regulator, which has a temperature compensated end-of-charge voltage trigger, to be into a constant trickle-charging mode. As a result, the satellite runs out of electric power and becomes inoperable, eventually ending up in an uncontrolled re-entry on a Brazilian city.

Overview

A cyberattack on the hardware supply chain represents a pertinent case study since Australia does not satisfy its supply chain demand within the domestic market and relies for most of its space infrastructure supply chain on international markets, including those relying on commercial-off-the-shelf (COTS) components. Key elements of this specific use case are summarised in the Figure below:

FIGURE 27: MAJOR ELEMENTS OF USE CASE 2



Attacker(s)

- Malicious actor in the supply chain

Affected Actors

- Australian satellite company
- COTS supplier
- Brazil
- On-orbit states

Attack

- Replacement of legitimate hardware for a malicious one that affects the battery of the satellite and eventually makes it inoperable and uncontrolled

Issue

- COTS supplier vulnerable supply chain
- Lack of thorough research by the Australian satellite company regarding its new supplier protection policy

Fallouts

- Inoperability of the satellite
- Uncontrolled re-entry into a Brazilian city
- Satellite drift in outer space becoming a debris
- Threat of collision with other objects in space

Relevant laws and policies

- Non-statutory contractual obligations
- Liability Convention
- The Rescue Agreement (not mentioned, but could be invoked if the Australian company intends to return the object that fell into Brazil)
- Security of Critical Infrastructure Act, depending on the use of the satellite (not mentioned)

Relevant Laws and Policies

Due to the uncontrolled re-entry into a Brazilian city, the case has clear international ramifications, with possibly the application of the **Liability Convention**, requiring it, firstly, an assessment of whether the re-entry caused damage. 'Damage' is narrowly defined by the convention in Article I, letter 'a' as 'loss of life, personal injury or other impairment of health, or loss of or damage to property of States or of persons, natural or juridical, or property of international intergovernmental organizations.

Since the satellite fell in an urban area, it probably did cause damage. However, is important to point out that due to its slender definition, compensatory restitution is not necessarily a certain thing in re-entry situations, and it can be subject to some discussion. The case of soviet satellite Kosmos 954 that crashed into the Canadian territory is a good example.

Letter 'c' of the same article defines the launching state as not only the state that procures the launching (i), but also a state from whose territory or facility the object was launched (ii), while the letter 'd' expands the term space object not only for the object itself, but also to its launch vehicle and parts thereof, in case of damage Australia would be liable if it had accepted to be the launching state.

If Australia were the launching state in this case, firstly the Australian company would have needed to apply for a launch permit under the **Space (Launches and Returns) Act 2018** (Part 3, Division 3) if the object was launched from Australia, or for an overseas payload permit (Part 3, Division 5) if launched from an overseas launching base. By holding this permit, the company would be considered the responsible party by definition. In case of damage, however, Brazil would seek compensation in accordance with the Liability Convention (Section VIII) not to the responsible party but to Australia (the launching state), the responsible party would then be liable to pay the Commonwealth an amount equal to the lesser of the amount of that compensation, or to the insured amount for the permit (Part 4, Division 4).

The case does not provide information on whether Australia would seek the retrieval of its space object. Should the craft be required for internal investigations, for example, Australia could invoke the **Rescue Agreement** for it. The agreement does not limit this imposition of helping and returning only astronauts but extends it to objects launched outer space as well, which was already dictated in the Article VII of the OST.

If the satellite was considered a critical infrastructure asset, **The Security of Critical Infrastructure Act 2018** would be applied. This piece of legislation was amended by the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022, expanding coverage from the previous 4 sectors considered as critical to 11 sectors, which now include communications, data storage or processing, space technology and defence industry. The amendment sought to provide the Government with greater agency in responding to cyberattacks on critical infrastructure. If a cybersecurity incident has a relevant impact on a critical infrastructure asset, the responsible entity for the asset may be required to give a relevant Commonwealth body a report about the incident (Part 2B) and Part 3A authorises Home Affairs to direct and retrieve the data of critical infrastructure industries if a cyberattack has occurred, is occurring, or is deemed to be imminent and prejudices the social and economic stability or defence of Australia. Therefore, the company would immediately need to report to the ACSC within 12 hours as the incident has a significant impact on the availability of the asset.

To support the Australian company, the **Cyber Supply Chain Risk Management** developed by the ACSC, and part of the **Information Security Manual** is a useful document that alerts organisations regarding supply chains' possible threats, it assists in the understanding and identification of cyber supply chain risks by referencing the Identifying Cyber Supply Chain Risks and setting cybersecurity expectations through the Cyber Security Principles and the Essential Eight Maturity Model. The biggest concern is that the adherence to these principles, guidelines and documents is non-mandatory, however, since in this case the object is being considered a critical infrastructure, the Security of Critical Infrastructure Act 2018 grants provision for specific direction to be issued by the Government where national security concerns exist.

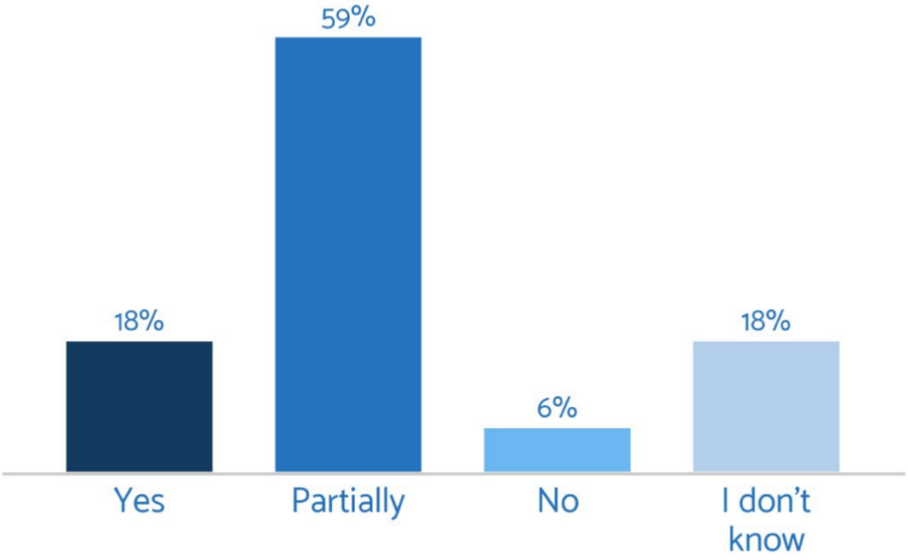
Similar to case 1, the implementation of some security controls of the Information Security Manual such as ISM 1568 (applications, ICT equipment and services are chosen from suppliers that have made a commitment to the security of their products and services.), ISM 1790 (applications, ICT equipment and services are delivered in a manner that maintains their integrity.), ISM 1791 (the integrity of applications, ICT equipment and services are assessed as part of acceptance of products and services.), and ISM 1792 (the authenticity of applications, ICT equipment and services are assessed as part of acceptance of products and services.) would have likely mitigated this attack. However, this Manual is not legally binding and does not compel companies to implement its recommendations.

Finally, different **non-statutory contractual obligations** also come to the fore. The minimum standards stipulated in the contract with the provider would be considered unsatisfactory, making that compensation were pursued from the COTS supplier company.

Elements for Consideration and Assessment

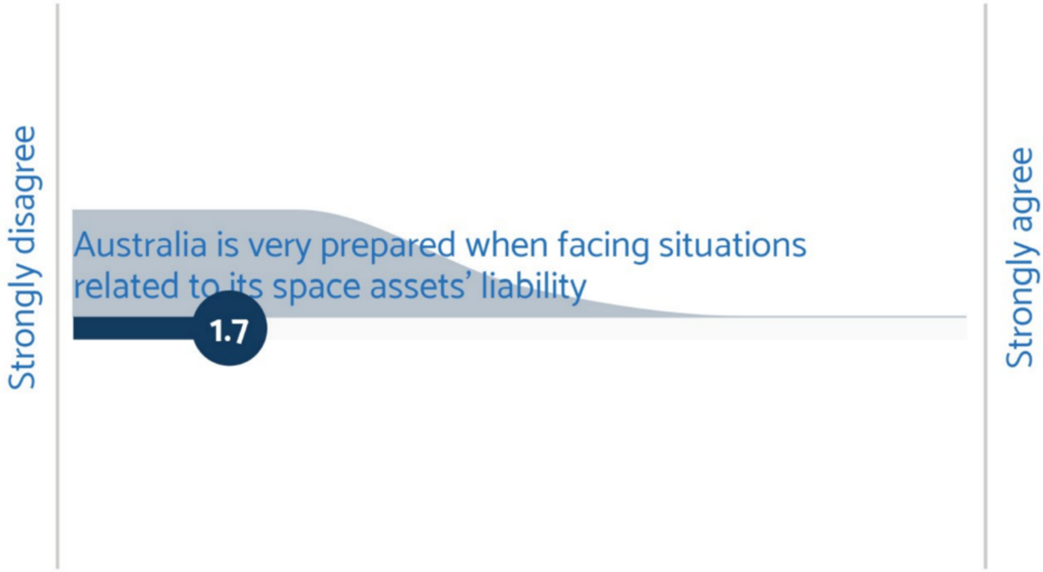
The use case shows non-negligible gaps in Australia's policy and legal framework. This was also confirmed by consulted stakeholders, with only the 6% of them not perceiving any kind of legal and policy gap related to this case.

FIGURE 28: PERCEIVED PRESENCE OF POLICY AND LEGAL GAPS RELATED TO USE CASE 2



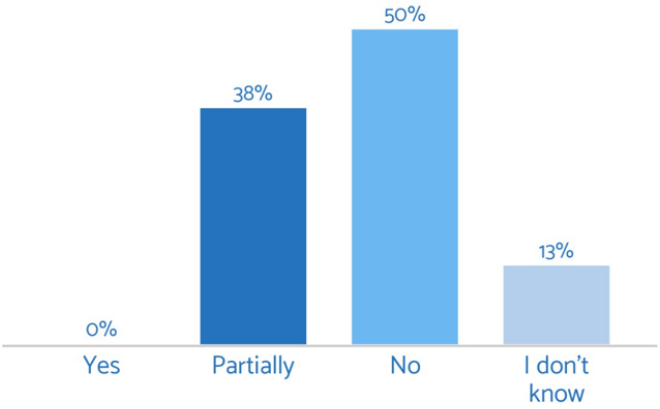
Overall, workshop participants rated the maturity of Australia's supply chain risk management as very poor (1.7 out of 5). This was mostly attributed to the fact that Australia's only immediate directive on the theme is the Liability Convention, while the Launches and Return Act session that covers possible accidents or incidents does not have as a primally purpose the determination of liability.

FIGURE 29: AUSTRALIA'S PREPAREDNESS IN RELATION TO SPACE ASSETS' LIABILITY



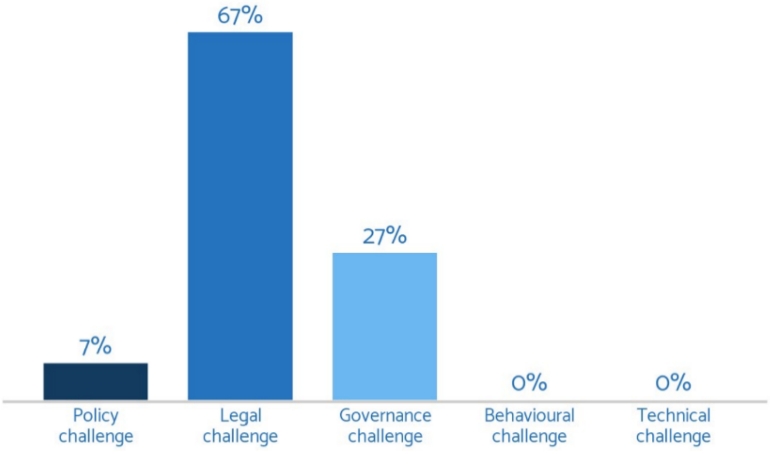
Australia does not seem to be well equipped to address issues related to space assets' liability, not only due to the lack of a specific domestic legislation on the theme, but more broadly because the current international framework is not sufficient to properly address liability issues in the opinion of 88% of the participants. This is an element directly pointing to the necessity of amending the Liability Convention.

FIGURE 30: FITNESS OF THE INTERNATIONAL LEGAL FRAMEWORK TO ADDRESS LIABILITY ISSUES



Among consulted stakeholders, there is a large consensus that the biggest challenge should this case materialise would be legal and governance. This assessment is compatible with the fact that, as already pointed out, the Liability Convention was deemed insufficient for the magnitude of this possible threat, and due to an absence of domestic legislation that directly deals with the theme, governmental roles and procedures in Australia are not clearly defined.

FIGURE 31: MOST CRITICAL TYPE OF CHALLENGE RELATED TO USE CASE 2



The biggest doubt among participants related to the applicability, or not, of the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022. Even though the Act has expanded coverage to the space sector, is still unclear what are the exact usage/elements that would make a structure to be considered a critical infrastructure. Arguably the definition of critical infrastructure asset that the Act provides (Division 2, 9) could be improved to ensure a clearer understanding. Similarly, the definition of the space technology sector as *'the sector of the Australian economy that involves the commercial provision of space-related services.'* remains way too vague and subject to different legal interpretations.

Regarding Australia's liability under the Liability Convention, due to the narrow scope of the definition of damage provided by the document, Australia could contest its compensation obligations with Brazil, this movement could, however, impact its international image.

3.2.3 Use Case 3: The Launch Infrastructure

Australia is developing launch sites in Abbot Point (North Queensland), Nhulunbuy (Northern Territory), and at Whalers Way Orbital Launch Complex (Eyre Peninsula). Australia does not have mature launcher capabilities and mostly launches foreign rockets from its soil.

Australia signs a contract with a new U.S. launcher company to launch a Japanese satellite. In this context, the Australian spaceport in the Eyre Peninsula welcomes staff from both the American and Japanese companies for the launch. The foreign staff is staying in a hotel near the launch site. As the launch is delayed due to adverse weather conditions, the foreign staff work remotely from the hotel and uses the hotel's Wi-Fi.

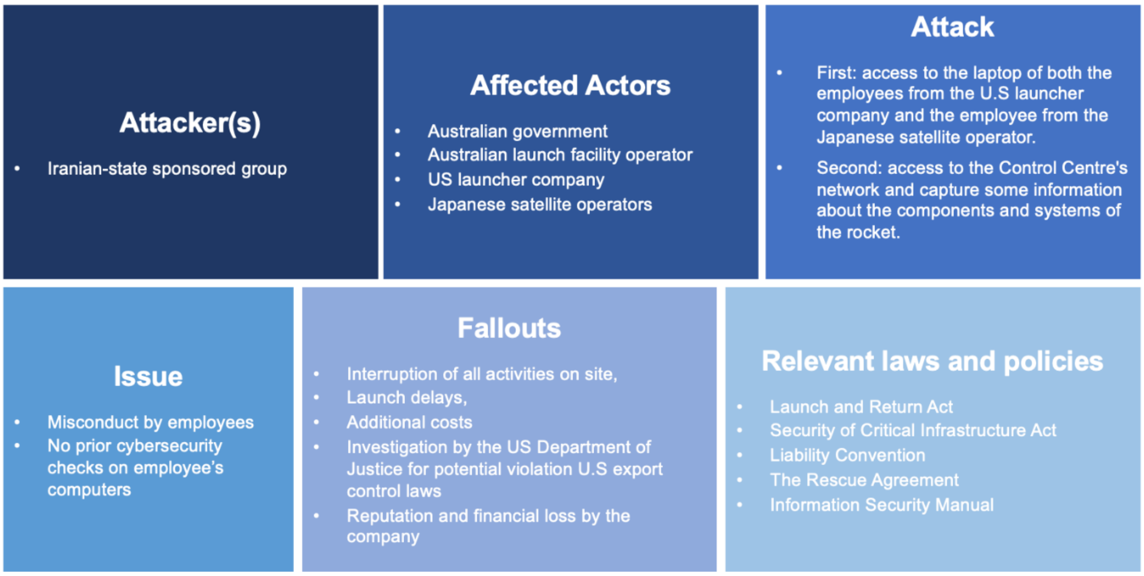
An Iranian state-sponsored group knows that foreign staff which come to the launch site always stay at the same hotel and are targeting this hotel's Wi-Fi to launch a sophisticated attack. The attackers send a malicious email to the hotel's reception, which appears to be a reservation from a well-known hotel booking website. The receptionist clicks on the email, which downloads a backdoor and installs it. The attackers are then able to access the Wi-Fi network of the hotel and can launch attacks on computers and smartphones which connect to the hotel's Wi-Fi network. They use the open-source Responder tool to listen for MBT-NS (UDP/137) broadcasts from devices that are attempting to connect to the Wi-Fi network and collect credentials (login and passwords). The attackers gain access to the laptop of both an employee from the U.S. launcher company and an employee from the Japanese satellite operator. When the launch is about to take place, the two employees travel to the launch site with their laptops and connect to the Wi-Fi network of the Launch Control Centre without any prior cybersecurity check on their computers. As a result, the attackers gain access to the Control Centre's Wi-Fi network and capture all the traffic on the network, including launch tests procedures, revealing some information about the components and systems of the rocket. The attack is detected by the Control Centre, which leads to the interruption of all activities on site, launch delays, additional costs as well as an investigation by the U.S. Department of Justice for potentially violating U.S. export control laws on missile technology. The company is therefore accused of missile proliferation, which affects its reputation and its financial stability due to legal costs.

Overview

Use case #3 – an attack to the launch infrastructure – is becoming more relevant to Australia, which has asserted its intention to rely on commercial providers instead of developing launch capabilities of their own.

The considered use case shows how a simple oversight by the personnel involved in a launch activity (in this case the lack of prior cybersecurity checks on computers of a launcher company employees) can generate far-reaching repercussions, including the temporary interruption of all activities on site with consequent launch delays and additional costs as well as loss of reputation and even and investigation by the U.S. Department of Justice for potentially violating U.S. export control laws on missile technology. Major elements of the considered case are summarised in Figure 29 below.

Figure 32: Major Elements of Use Case 3



Attacker(s)

- Iranian-state sponsored group

Affected Actors

- Australian government
- Australian launch facility operator
- US launcher company
- Japanese satellite operators

Attack

- First: access to the laptop of both the employees from the U.S launcher company and the employee from the Japanese satellite operator.
- Second: access to the Control Centre's network and capture some information about the components and systems of the rocket.

Issue

- Misconduct by employees
- No prior cybersecurity checks on employee's computers

Fallouts

- Interruption of all activities on site,
- Launch delays,
- Additional costs
- Investigation by the US Department of Justice for potential violation U.S export control laws
- Reputation and financial loss by the company

Relevant laws and policies

- Launch and Return Act
- Security of Critical Infrastructure Act
- Liability Convention
- The Rescue Agreement
- Information Security Manual

Relevant Laws and Policies

From a legal perspective, several laws and regulations prove of clear relevance to this case. Given the specifics of the case, the most relevant is the **Space (Launches and Return) Act, 2018** and associated rules. Within this Act, several provisions find applicability to this specific case. In the part on technology safeguard requirements, ss 22, 56, 97 and 102 of the Space (Launches and Returns) (General) Rules 2019 and s 29 of the Space (Launches and Returns) (High Power Rocket) Rules 2019 state that to obtain both a launch facility licence and a launch permit applicants must submit a 'technological security' plan to the Minister for Science and Technology for consideration. This technology plan applies to both launches and returns of space objects. The technological security plan is intended to cover physical risks to launch facilities and vehicles and needs to contemplate cybersecurity.

In explanatory materials accompanying the Space (Launches and Returns) (General) Rules 2019, the Australian Government explained:

Identification of the cybersecurity strategy to be used is important, given the potential for malicious actors to gain access to, and potential control of, the launch facility's [or provider's] network or parts of it. Given the nature of some cyberattacks it may even be difficult to identify if a facility's [or provider's] network has been breached. The defensive measures taken to protect the network are critical for preventing unauthorised access.

The Act also contemplates the possibility to execute investigation reports. Specifically, ss 83, 84, 85, 86 of the Act state that the Minister for Science and Technology can appoint an investigator to examine any launch-related incidents or accidents (see focus box).

Act 87, however, clarifies that by establishing a system of investigating the circumstances surrounding any accident or incident, the object is simply to prevent other accidents and incidents occurring and it is neither the object a) to provide a way of apportioning blame for an accident or incident, nor b) to provide a way of determining the liability of any person in respect of an accident or incident.

Another relevant legislation is the **Security of Critical Infrastructure Act, 2018.** Part 2B of the Security of Critical Infrastructure Act 2018 specifies that critical infrastructure operators are subject to mandatory cyber incident reporting requirements vis-à-vis the Department of Home Affairs and Part 3A authorises Home Affairs to direct and retrieve the data of critical infrastructure industries if a cyberattack has occurred, is occurring, or is deemed to be imminent and prejudices the social and economic stability or defence of Australia.

More specifically, if regulated entities become aware that a critical cybersecurity incident has occurred, or is occurring, and the incident has had, or is having, a significant impact[356] on the availability of their asset, they must notify the Australian Cyber Security Centre (ACSC) within 12 hours (in case of critical cybersecurity incidents) or 72 hours (in case of other cybersecurity incidents) after they become aware of the incident. Should they make the report verbally, then they must make a written record within 84 hours of verbally notifying the ACSC. A form is provided,[357] where it needs to be indicated the reason for reporting (either inform the ACSC and/or request assistance or advice from the ACSC).

Accidents and Incidents for the Space (Launches and Returns) Act

Division 2 Part 7 of the Space (Launches and Returns) Act clarifies the difference between incidents and accidents as follows:

An accident involving a space object or high-power rocket occurs if:

(a) a person dies or suffers serious injury as a result of the operation of the space object or high-power rocket; or

(b) the space object or high-power rocket is destroyed or seriously damaged or causes damage to other property (other than in the circumstances prescribed by the rules).

An incident is an occurrence associated with the operation of a space object or high-power rocket that affects or could affect the safety of the operation of the space object or high power rocket or that involves circumstances indicating that an accident nearly occurred.[355]

From a policy perspective, the various tools developed by the ACSC may have also helped the Australian operators in this case through initiatives such as the **Essential Eight Maturity Model** and the **Information Security Manual** to adopt best practices and cyber hygiene.

Beyond the general cybersecurity principles, the ISM provides several relevant security guidelines, especially those related to enterprise mobility, system hardening and system management, which describe the use and protection of mobile devices like laptops.[358]

[355] Federal Register of Legislation. (2018). *Space (Launches and Returns) Act 2018*. https://www.legislation.gov.au/Details/C2021C00394

[356] A significant impact is one where both the critical infrastructure asset is used in connection with the provision of essential goods and services; and the incident has materially disrupted the availability of those essential goods or services; Australian Cyber Security Centre. (n.d.) *Report Cyber*. https://www.cyber.gov.au/acsc/report

[357] Ibid.

[358] Australian Cyber Security Centre. (2023). *Cyber Security Guidelines*. Commonwealth of Australia. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines

With regard to the present case, the implementation of ISM-0874 (Mobile devices access the internet via a VPN connection to an organisation's internet gateway rather than via a direct connection to the internet) and ISM-0705 (When accessing an organisation's network via a VPN connection, split tunnelling is disabled) would have likely prevented the attack considered in this case.[359] As explained by the ISM, when connecting laptops to the internet, 'best practice involves establishing a Virtual Private Network (VPN) connection to an organisation's internet gateway rather than a direct connection to the internet. In doing so, mobile devices will be protected by additional security functionality, such as web content filtering, provided by an organisation's internet gateway.' In addition, a split tunnel VPN 'can allow access into an organisation's network from other networks, such as the internet. If split tunnelling is not disabled, there is an increased security risk that the VPN connection will be susceptible to intrusions from other networks. An organisation can refer to the relevant ACSC security configuration guidance for mobile devices on how to mitigate this security risk'.

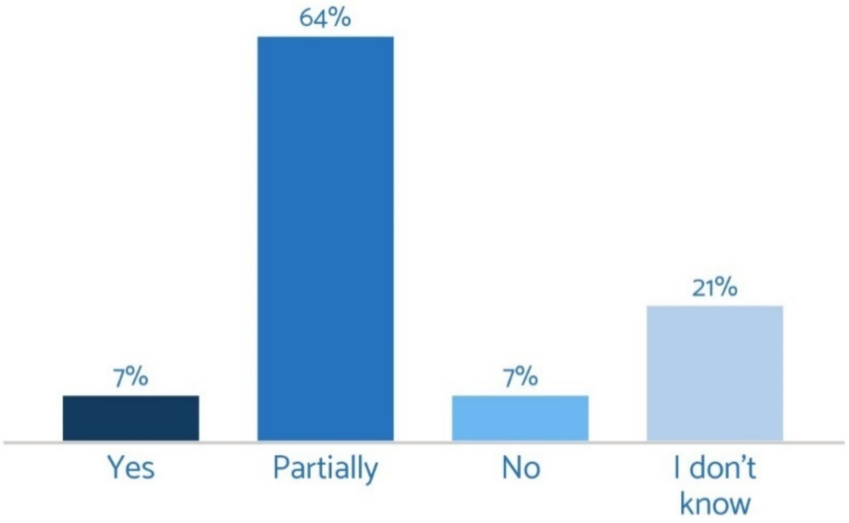
However, as already explained, an organisation is not required by law to comply with the ISM, nor the ISM does override any obligations imposed by legislation or law.

In addition, if there was a national security element to the launch activity or the launch facility operator was a DISP member organisation, then the **Defence Industry Security Program (DISP)** and all its controls, including those related to offsite work, would have applied.[360] As a result, it would have not been permitted to allow computers connected to the hotel Wi-Fi to connect to the launch systems, and the attack would have not occurred.

Elements for Consideration and Assessment

The case shows that cybersecurity accidents can happen even when a policy, legal and regulatory framework do not present visible gaps. As a matter of fact, most stakeholders commented that the attack could have been stopped by standard ICT policy, general good network security and hygiene policy. Only 7% of consulted stakeholders perceive clear policy and regulatory gaps regarding this case.

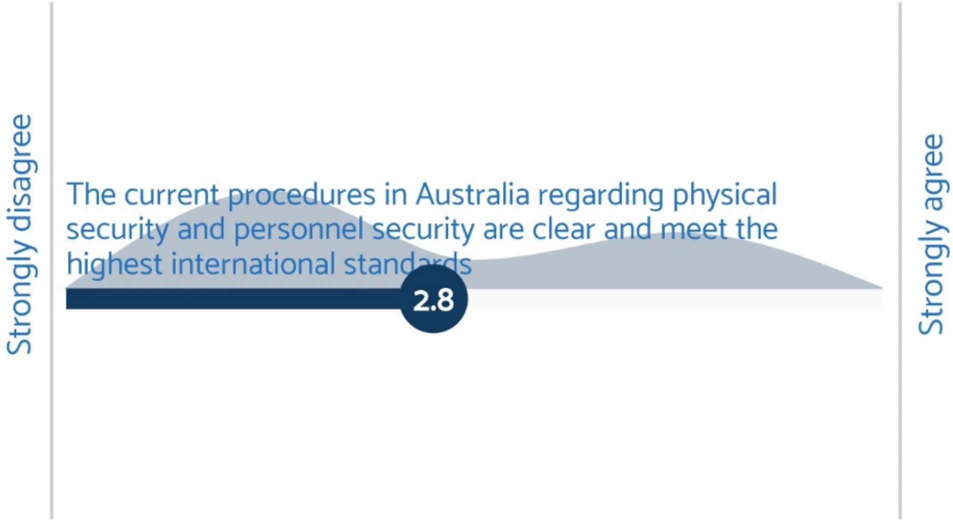
FIGURE 33: PERCEIVED PRESENCE OF POLICY AND LEGAL GAPS RELATED TO USE CASE 3



[359] Australian Cyber Security Centre. (2023). *Information Security Manual*. Commonwealth of Australia. p.17. https://www.cyber.gov.au/sites/default/files/2023-09/Information%20Security%20Manual%20%28September%202023%29.pdf
[360] Department of Defence. (2020). *Defence Security Principles Framework*. https://www.defence.gov.au/sites/default/files/2020-12/DSPF-OFFICIAL.pdf

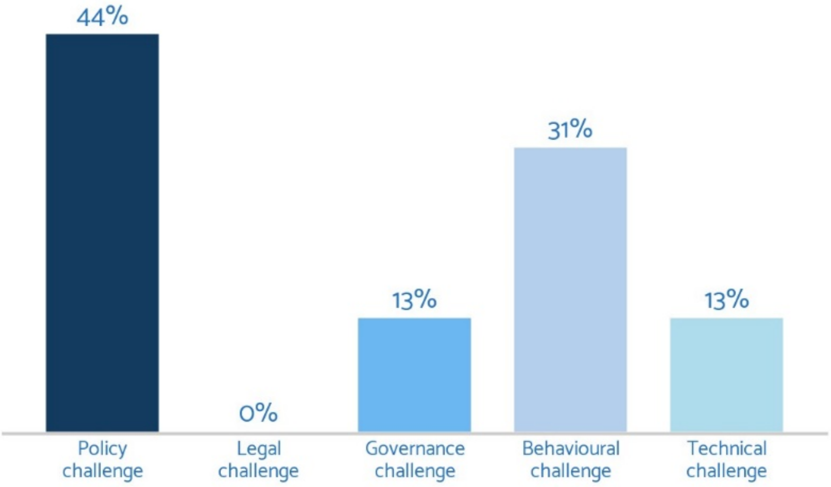
In addition, the current procedures are assumed to be clear and to meet the highest international standards (see Figure 28). What was, however, indicated as critical was the lack of awareness and clear enforcement mechanisms to ensure the full implementation of the procedures already envisaged by the policy framework as well as a baseline hygiene policy in the behaviour of employees. These missing elements can still be conducive to the emergence major cyber incidents.

FIGURE 34: STATEMENT ASSESSMENT



Among consulted stakeholders, there was large consensus that the biggest challenge should this case materialise would be policy and behavioural in nature.

FIGURE 35: MOST CRITICAL TYPE OF CHALLENGE ASSOCIATED WITH USE CASE 3



From a legal and policy perspective, the issue is that current tools focus mostly on preventive measures, but they contain limited guidance during and after attack. As also stressed by de Zwart and Lisk, and '*existing* *legislation seeks to maximise preventative cybersecurity and has only recently addressed contingency plans following breaches of cybersecurity for satellite operators.'*[361]

Policies such as the ISM do instead contain guidance on how to respond to cybersecurity accidents. However, the fact that an organisation is not legally required to comply with the ISM, that the ISM does not override any obligations imposed by legislation or law and that legislation takes precedence over the ISM in case of conflict, make their implementation of general cyber policies more limited.

3.2.4 Use Case 4: The Ground Segment

Australia's space industry has mature capabilities in the manufacture of ground systems and has many ground stations on its soil, which could be the target of cyberattacks. A zero-day vulnerability in the Telemetry, Tracking; Commanding and Monitoring (TTCM) subsystem of an Australian SATCOM ground station located in Adelaide is being exploited by a Russian hacker group. The TTCM enables them to control and monitors the satellite's functions from the ground. The telemetry protocol used by the subsystem contains a vulnerability, which does not implement encryption correctly, enabling the attackers with adjacent short-range access to the ground station to intercept the data, which is in clear text. In addition, the telecommunication satellite, to which the ground station sends commands, is used for telemedicine purposes, which includes personal data and health data. This type of data can then be sold online on the dark net to the highest bidder, resulting in a massive personal data breach because of a vulnerability in a SATCOM ground station, affecting credibility and bankrupting the business.

Note

If the attackers also try to steal any kind of information that possesses national security value, we also have the applicability of the Telecommunication and Other Legislation Act 2017 which imposes some obligations for C/CSPs entities and provides the Secretary of Attorney-General's Department (AGD) an information gathering power to facilitate compliance monitoring and compliance investigation activity in relation to compliance with securities obligations. It also provides the Attorney-General with further directions power to direct a C/CSP to do or not do a specified action.

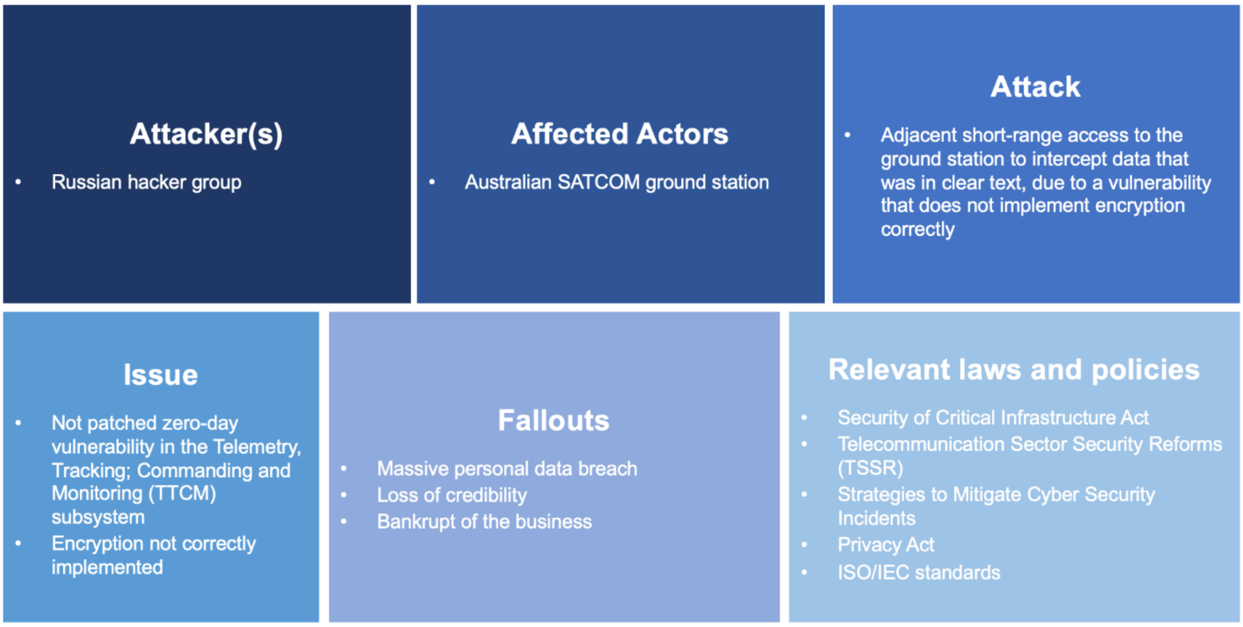
Questions: Is an attack on the ground segment considered as an attack on a space system? Are there legal protocols in place or good practices for the security of the ground segment? Is it considered as a critical infrastructure?

Overview

Use case 4 – a cyberattack on the ground infrastructure – is an increasing concern among institutional and commercial actors alike. As a matter of fact, Australia possesses a strong tradition on its ground centres as an important provider of the segment, with the digitalisation of most stations it becomes an appealing entry point for cyberattacks, that nowadays are more commonly targeting the ground infrastructure than directly at the space segment. For this reason, and for being considered an easier way to gain control over a satellite, it is important for the country to assess the cyber maturity of the current policies and protocols for this kind of attack. Major elements of the considered case are summarised below.

[361] de Zwart, M., & Lisk, J. (2022). *Low Earth Orbit, Satellite Constellations and Regulation*. Flinders University.

FIGURE 36: MAJOR ELEMENTS OF USE CASE 4



Attacker(s)

- Russian hacker group

Affected Actors

- Australian SATCOM ground station

Attack

- Adjacent short-range access to the ground station to intercept data that was in clear text, due to a vulnerability that does not implement encryption correctly

Issue

- Not patched zero-day vulnerability in the Telemetry, Tracking; Commanding and Monitoring (TTCM) subsystem
- Encryption not correctly implemented

Fallouts

- Massive personal data breach
- Loss of credibility
- Bankrupt of the business

Relevant laws and policies

- Security of Critical Infrastructure Act
- Telecommunication Sector Security Reforms (TSSR)
- Strategies to Mitigate Cyber Security Incidents
- Privacy Act
- ISO/IEC standards

Relevant Laws and Policies

Due to involving personal information, there is the applicability of the **Privacy Act** which aim to promote and protect the privacy of individuals and to regulate how Australian Government agencies and organisations, collectively referred to as APP entities, handle personal information. It contains 13 Australian Privacy Principles (APPs), considered the foundation of the privacy protection framework in the Privacy Act that APP entities must comply with (Part 3, Division 2).

In case, the most pertinent APP is the number 11, which dictates that an entity must take reasonable steps to protect personal information it holds from misuse, interference, and loss, and from unauthorised access, modification, or disclosure.

The Privacy Act does not directly include specific cybersecurity protections, it imposes obligations on entities that collect and manage personal information, creating a more secure and responsible domestic data environment, consequently, this legislation can be used to make accountable APP entities that breach APP principles, not taking such reasonable steps to protect personal information, this could be interpreted as not possessing adequate cyber defences and risk management plans, in case of a breach, for example APP 1 requires entities to take reasonable steps to establish and maintain practices, procedures, and systems to ensure compliance with the APPs.

The Act also institutes a scheme for notification for this data breach (Part IIIB, Divisions 2, 3) and brings APP Codes, which is a more concrete materialization of the APP principles, a written code of practice about information privacy, and may impose additional requirements to those enforced by the Australian Privacy Principles.[362]

If any kind of information possesses national security value, there also would have applicability of **The Telecommunication and Other Legislation Act 2017** which imposes some obligations for C/CSPs entities and provides the Secretary of Attorney-General's Department (AGD) an information gathering power to

[362] An App code that is included in the Code Register and in force is a legislative instrument (Part IIIB, Division 2), for this case, the most significant is the Privacy (Australian Government Agencies – Governance) APP Code 2017.

facilitate compliance monitoring and compliance investigation activity in relation to compliance with securities obligations. It also provides the Attorney-General with further direction power to direct a C/CSP to do or not do a specified action.

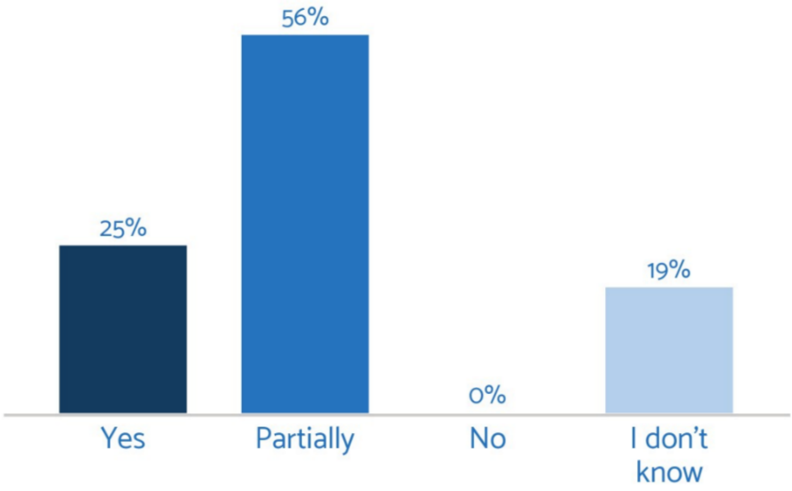
As already mentioned in Case 2, **The Security of Critical Infrastructure Act 2018** was amended by the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022, expanding coverage from the previous 4 sectors considered as critical to 11 sectors, which now include communications and data storage or processing, which can encompass the telecommunication satellite of this case. Considering that the attack targeted an Australian SATCOM ground station, the act can find applicability. Part 2B of the Security of Critical Infrastructure Act 2018 requires critical infrastructure operators to report cybersecurity incidents to the Department of Home Affairs and Part 3A authorises Home Affairs to direct and retrieve the data of critical infrastructure industries if a cyberattack has occurred, is occurring, or is deemed to be imminent and prejudices the social and economic stability or defence of Australia.

From a policy perspective, the **Information Security Manual** provides some guidance for this case. The correct implementation of encryption is highlighted within the document in several sessions, including the Protection Principle seven which dictates the necessity of data being encrypted at rest and in transit between different systems and the fundamentals section of the Guidelines for Cryptography, in which it can be highlighted ISM-0462 (When a user authenticates to the encryption functionality of ICT equipment or media, it is treated in accordance with its original sensitivity or classification until the user de-authenticates from the encryption functionality), ISM-0142 (The compromise or suspected compromise of cryptographic equipment or associated keying material is reported to an organisation’s Chief Information Security Officer, or one of their delegates, as soon as possible after it occurs), and ISM-1091 (Keying material is changed when compromised or suspected of being compromised). Also, the **Strategies to Mitigate Cyber Security Incidents** could assist cybersecurity professionals in all organisations to mitigate cybersecurity incidents after the realization of a solid identification of assets and the completion of a risk assessment to identify the level of protection required from various cyber threats. The most pertinent for the concrete analysed concrete case are the mitigation strategies related to patch applications and operational systems that recommend patching/mitigating computers with ‘extreme risk’ security vulnerabilities within 48 hours and using the latest version of applications and operation systems. Important to emphasize that other implementation guides were also mentioned, highlighting the ISO/IEC 27001:2022 and 27002:2022.

Elements for Consideration and Assessment

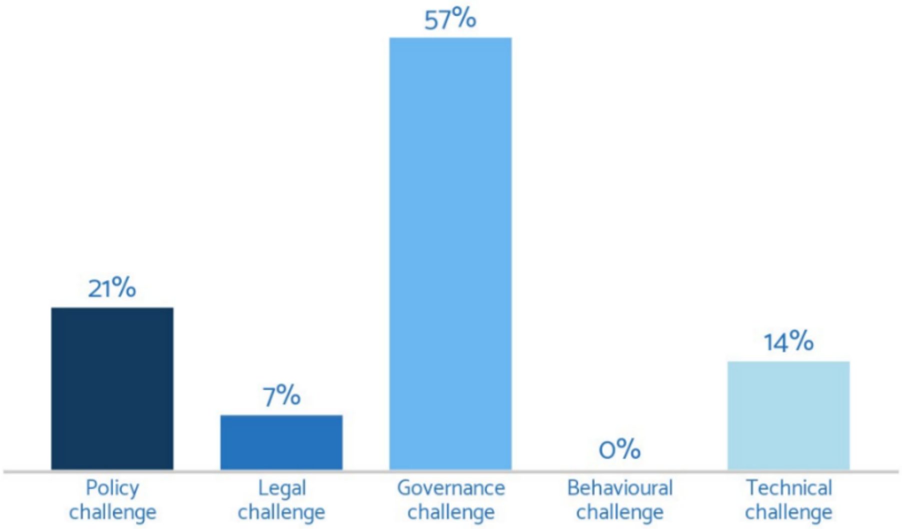
81% of the consulted stakeholders perceived the presence gaps or partial gaps related to this case. This assessment is at odds with the importance that the ground segment possesses in the whole Australian space infrastructure, underscoring the urgent need of developing new policies and legal mechanisms.

Figure 37: Perceived Presence of Policy and Legal Gaps Related to Use Case 4



Although zero-day vulnerabilities are usually associated with the technical segment, only 14% of participants indicated that as the most critical type of challenge, instead, most of the participants considered the biggest challenge would pertain to the governance sphere (57%), what can indicate the recognition of a lack of proper governmental activity to offer policies and programs that aim to mitigate the chance of this kind of attack happening, or, if it happens, the proper identification of governmental roles and procedures to assist in mitigating its damage.

Figure 38: Most Critical Type of Challenge Associated with Use Case 4



Data interception as described in the present case has been a constant problem in the Australian scenario, the Medibank and Optus recent breach demonstrated how devastating the leak of personal information might be. Despite the announced intended efforts by the Prime Minister to overhaul privacy legislation, according to the majority of workshop participants (57%), the problem does not lie on this spectrum, but on governance issues, in the sense of correct attribution of power and responsibilities.

This is coherent with the fact that, depending on the nature of the intercepted information, different departments are empowered to act and, the Telecommunication and Other Legislation Act 2017 provides power to the Secretary of Attorney-General's Department when there is a breach of information that possesses national security value, while the Security of Critical Infrastructure Act 2018 empowers Home affairs if a cyberattack has occurred, is occurring, or is deemed to be imminent and prejudices the social and economic stability or defence of Australia.

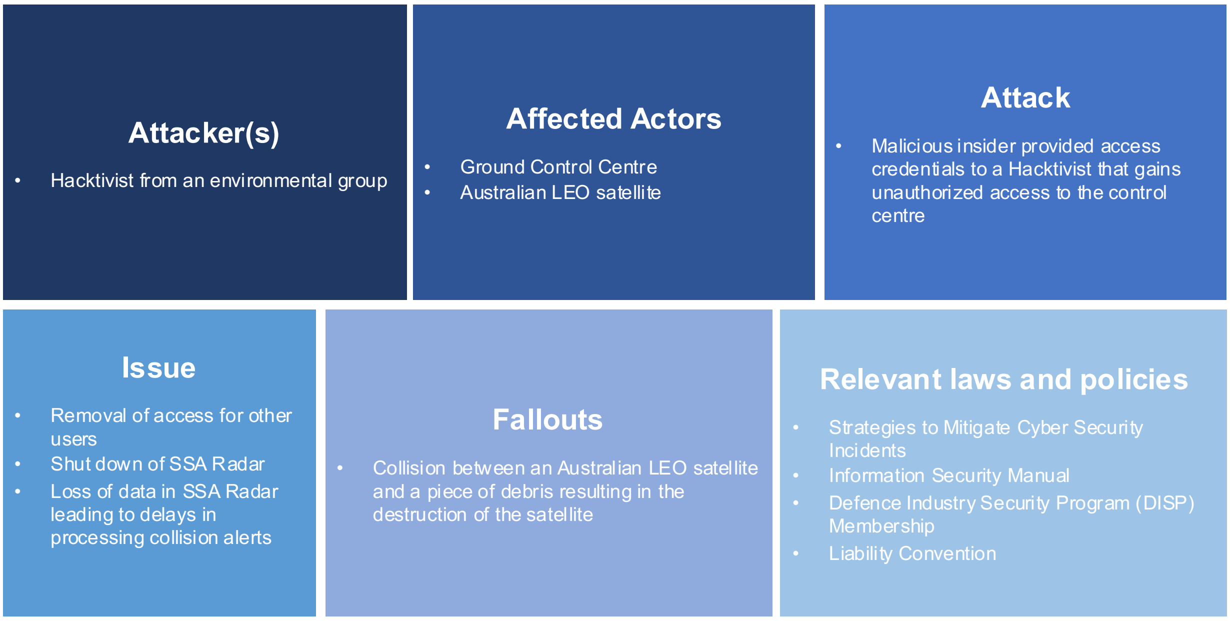
3.2.5 Use Case 5: The Space Situational Awareness Infrastructure

A hacktivist from an environmental group manages to highjack the link between a commercial Space Situational Awareness (SSA) radar located in Australia and a control centre to protest the set-up of the radar near a protected natural area. The environmental group believes that the radiofrequency may harm the natural environment. The hacktivist convinces a frustrated employee of the SSA company of his cause. The employee provides the environmental group with his access credentials (login and passwords) to the Control Centre, which controls the radar. The hacktivist then takes control of the control centre, resets the password, and removes access for other users, making him the only stakeholder with access to the radar. He then shuts down the radar, which led to a loss of data in SSA for several Australian operators, leading to delays in processing collision alerts as operators had to procure additional data elsewhere (e.g., space-track). One collision alert between an Australian LEO satellite and a 50 cm piece of debris is not processed in time and not enough data is available to decide whether to conduct a manoeuvre. As a result, the LEO satellite collides with the debris, destroying a 2-million AUD satellite.

Overview

As already mentioned, Australia has a certain weight when it comes to ground segment services and many policies, laws, and regulations to prevent technical interference have been already developed. However, a man-in-the-middle threat provides the opportunity for a deeper reflection regarding personnel security and physical security. For this, specific segments of manuals, strategies and programs were explored. Major elements of the considered case are summarised in the Figure below.

FIGURE 39: MAJOR ELEMENTS OF USE CASE 5



Attacker(s)

- Hacktivist from an environmental group

Affected Actors

- Ground Control Centre
- Australian LEO satellite

Attack

- Malicious insider provided access credentials to a Hacktivist that gains unauthorized access to the control centre

Issue

- Removal of access for other users
- Shut down of SSA Radar
- Loss of data in SSA Radar leading to delays in processing collision alerts

Fallouts

- Collision between an Australian LEO satellite and a piece of debris resulting in the destruction of the satellite

Relevant laws and policies

- Strategies to Mitigate Cyber Security Incidents
- Information Security Manual
- Defence Industry Security Program (DISP) Membership
- Liability Convention

Relevant Laws and Policies

In the policy sphere, the prior application of the **Strategies to Mitigate Cyber Security Incidents** could be relevant to the case, the document provides several tactics, enlisted by threats, to assist cybersecurity professionals to protect organisations against cyber incidents. On the mitigation details, the most relevant, in case, is the mitigation strategy specific to preventing malicious insiders, dealing with personnel management to assist to avoid employees having, developing, or carrying out malicious intent.

The guidance consists in executing pre-employment screening and ongoing vetting, immediately disabling all accounts, and requiring sanitisation or return of mobile computing devices for departing employees, reminding employees of their security obligations and penalties for violations, creating an appreciation culture to engage employees and to reduce some motivations for employees to become malicious insiders.

Also, for employees who have privileged access to highly classified or other extremely sensitive data, the strategy dictates the performance of psychological assessments by qualified personnel to explore topics including allegiances and beliefs as well as character weaknesses which could be leveraged and manipulated by adversaries.

Another relevant strategy brought by the document is to restrict administrative privileges[363] to reduce the chances of a compromise. An environment with restricted administrative privileges is more predictable and stable, easier to administer as fewer users can make significant changes to their operating environment, either intentionally or unintentionally.

Also, the **Information Security Manual** and the **Defence Industry Security Program Membership (DISP)** could be pertinent to the case. The Information Security Manual (ISM) purpose is to outline a cybersecurity framework that organisations can apply, using their risk management framework, to protect their information and systems from cyber threats, and besides the cybersecurity principles brought by the document, it is significant to highlight in its security guidelines section, the Guidelines for Personnel Security, comprising cybersecurity awareness training and access to systems and their resources, which includes directives regarding system access requirements, and control of Australian systems referencing that some systems should only be accessible from systems under the sole control of the Australian Government that are located within facilities authorised by the Australian Government, what would have avoided the hacktivist access, even with the correct credentials, from a different place. ISM-1565 (Tailored privileged user training is undertaken annually by all privileged users) could also be relevant to the company for a closer approximation of the compromised employee.

In turn, DISP is a program that aims to improve resilience, security and assurance in Australian businesses that engage in Defence projects, contracts, and tenders, addressing risks associated with providing services, products or capabilities and creating a safer environment for the Australian Defence sector, through several measures assessed in four levels of increasing scrutiny.

The program, as defined by the Australian Defence is *essentially security vetting for Australian businesses*, and it is mandated in certain circumstances, including when working on classified information or assets or providing security services for Defence bases or facilities. In case, there are two key categories assessed by DISP that had the potential to alter the outcome of the unauthorised access: information and cybersecurity (i), and personnel security (ii).

Information and cybersecurity involves strengthening the business' cyber capabilities aiming at the identification of, protection from, and remediation of security incidents or attacks on the system,[364] while personnel security includes training, awareness programs, and the institutionalization of policies, procedures, and reporting processes, it might also include, for upholding security clearance, the monitoring

[363] Restricting administrative privileges forms part of the Essential Eight from the Strategies to Mitigate Cyber Security Incidents.

[364] There are four cybersecurity standards the business can choose from depending on the contractual and overall needs; ASD Essential Eight (top 4), NIST SP 800-171, Def Stan 05-138, ISO-27001 and relevant components.

and report of any changes in attitude or behaviour of the sponsored staff, which, along with a more prepared cyber system, could have led to avoiding the problem.

For this case is also interesting to assess liability under the **Liability Convention**, due to the collision between an Australian LEO satellite and a 50 cm piece of debris that resulted in the destruction of the 2-million AUD satellite. The initial point for liability to occur is the existence of damage caused by a space object, in this case, the destruction of a 2-million AUD satellite can be considered as enough damage by the definition of Article I (a), therefore, the next step would be the fault assessment.

According to the convention, liability, when two space objects collide, is fault-based (Article III), so it needs to be established whose fault it was, the discussion lies in the complexity of the scenario.

Prior to this assessment, is important to exclude the commercial ground station liability, as pointed out by some of the participants. Although possessing undeniable importance in the current space scenario, ground stations that assist the operation of space traffic management are not contemplated as liable beings under the Liability Convention. Even in this case, which presents a clear flaw in the operation system of the centre, the liability convention is categorical in indicating only the liability of launching states of space objects that caused damage (Article II), hence, the liability may rest in one of the launching states (Australia and launching state X).

According to Article I (d) of the Convention, component parts of a space object as well as its launch vehicle and parts are also considered space objects for liability purposes. Hence, firstly, the debris would need to be tracked and identified of which space object it was previously a part of, only then is possible to identify what was the launching state of that space object, which is also liable for the debris (launching state X).

On one hand, the satellite launching state, Australia, may track the debris origin and argue that it intercepted the regular trajectory of the satellite, causing the collision and the total satellite destruction, resulting in a loss of a 2-million AUD equipment, claiming compensation under Article VIII, paragraph 1.

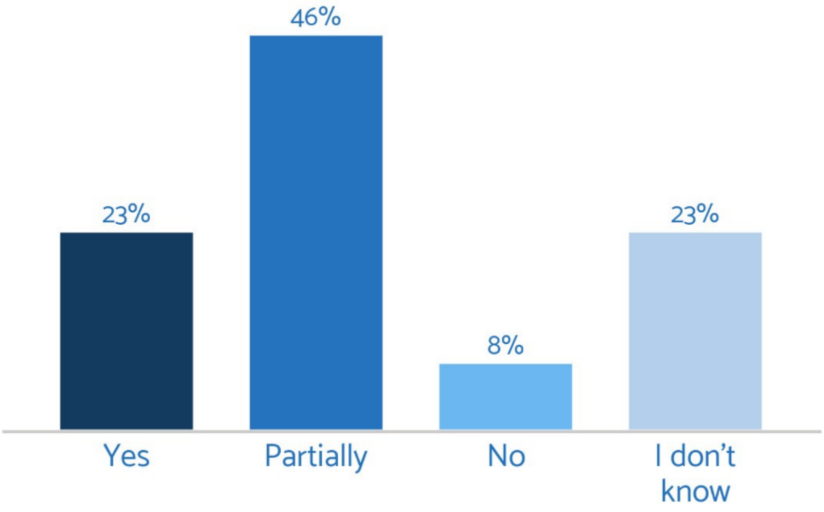
However, on the other hand, the other launching state, responsible for the debris, launching state X, may argue that the debris has no manoeuvring capability and the operators that supposedly could move the satellite were unable due to an internal problem not related to, in any way, with launching state X, concluding that Australia's own omission caused the damage, through a legal systematic interpretation of Article VI, paragraph 1, from absolute liability to fault-based liability. In this sense, the argument would be that, if the damage resulted either wholly or partially from gross negligence or from an act or omission on the part of a claimant State can be exonerated in cases of absolute liability, then, with more reason, it could also be exonerated in cases of faulty liability.

If launching state X's argument prevails, Australia may possibly conduct a regressive action against the commercial ground centre, on a private law basis, but this will not be explored in this section.

Elements for Consideration and Assessment

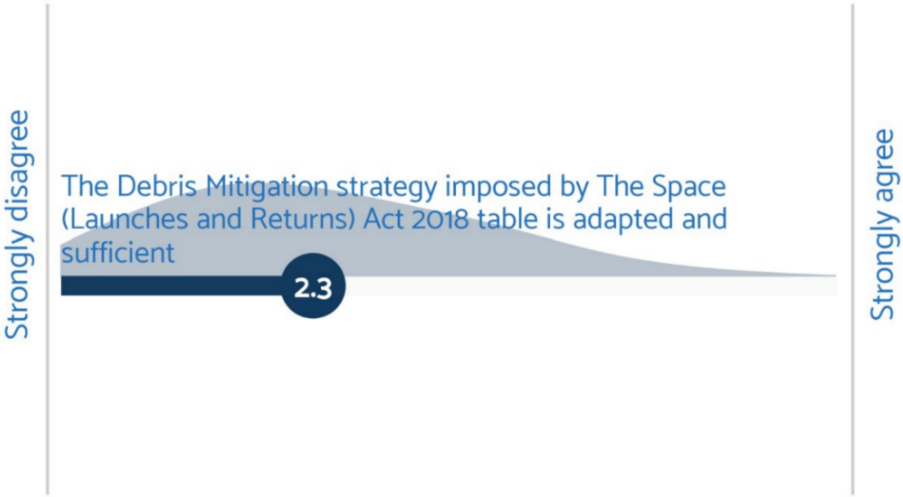
69% of the participants perceive gaps or partial gaps related to this case. According to the participants' discussion, such gaps are mainly associated with the absence of an immediate plan for supporting defective or inoperant ground services and clear procedures regarding personnel security.

FIGURE 40: PERCEIVED PRESENCE OF POLICY AND LEGAL GAPS RELATED TO USE CASE 5



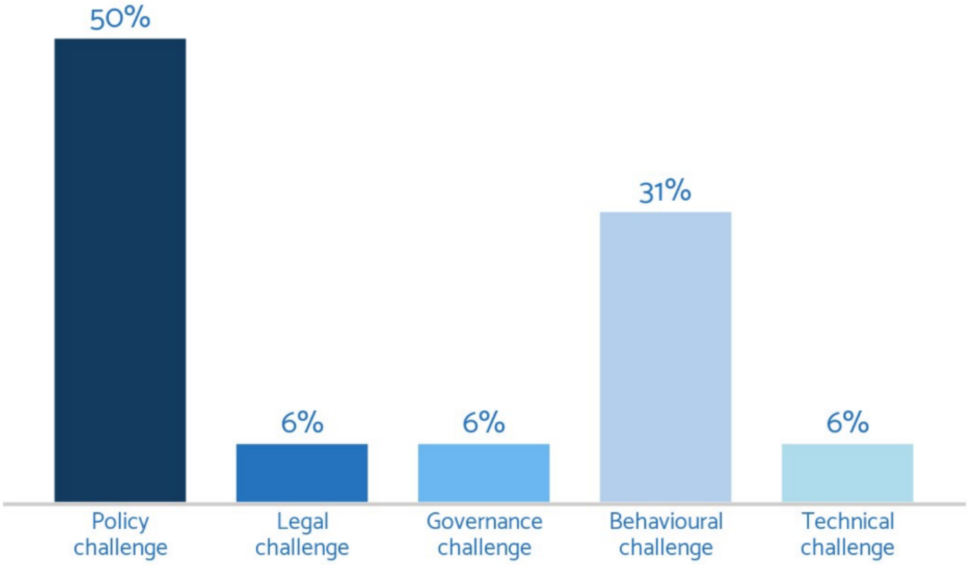
Even if the Debris Mitigation Strategy imposed by the Space (Launches and Returns) Act 2018 requires the use of an internationally recognised guideline or standard for debris mitigation, the description of any mitigation measures planned for orbital debris arising from the proposed launch and an orbital debris assessment, few stakeholders believe that strategy is adapted and sufficient. They however highlighted that the considered issue could be found on the international standard replicated in Australia.

FIGURE 41: STATEMENT ASSESSMENT



The participants agreed that most of the challenges related to this case are policy and behavioural in nature, with 31% of the participants pointing behavioural challenges as the most critical issue. This clearly stems from the role played by human action in this case, despite the existence of procedures, whether they are considered proper or not.

Figure 42: Most Critical Type of Challenge Associated with Use Case 5



The fact that the biggest challenges are associated to policy and behaviour is consistent and coherent with most of the relevant legislations/policies brought into the discussion, focussing on personnel security and malicious insider threats. However, it was raised that although most of the policies presented important preventive measures, they do not possess significant reactive measures.

The SSA situation was also highly debatable, with some participants pointing out that the SSA reliability may never be upon a single sensor, so, in this sense, a thorough international space traffic management, using multiple sensors, could be enough to avoid the situation proposed in this case. Also, participants considered it unclear if SSA is encompassed in the scope of critical structure, which, therefore, made also uncertain the applicability of the Security of Critical Infrastructure Act.

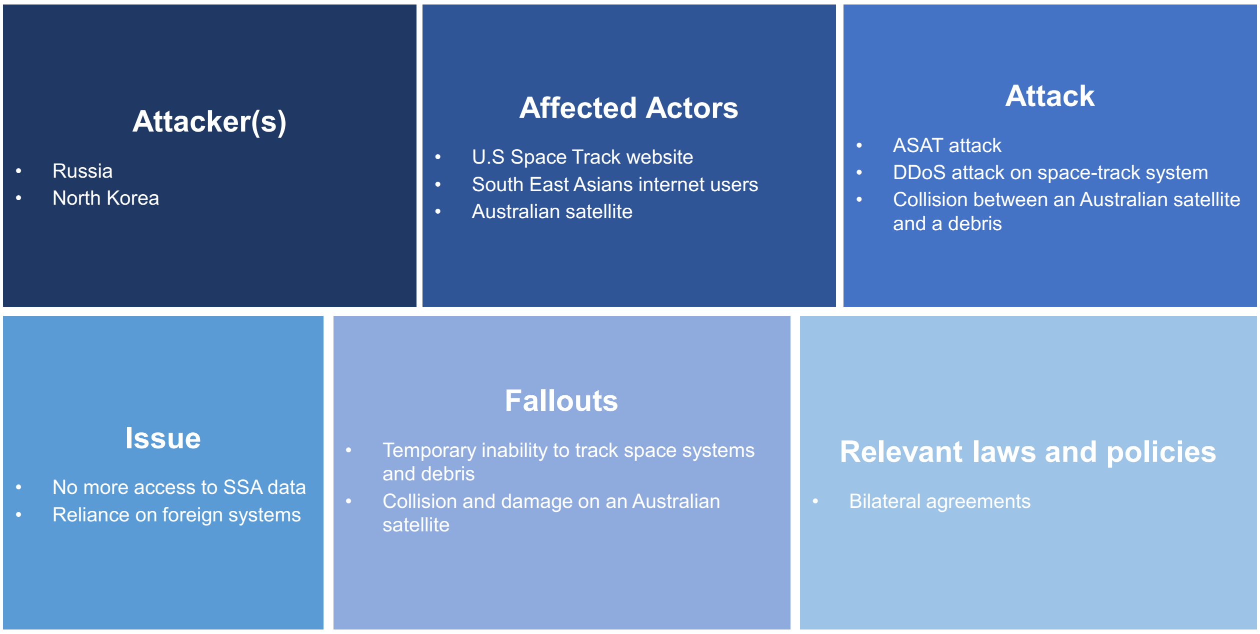
Lastly, another consideration was regarding the insufficiency of the Debris Mitigation Strategy imposed by The Space (Launches and Returns) Act 2018, after an interesting debate regarding the liability situation brought by this case, and highlighting the importance of responsible management of existent debris and the necessity of a sustainable model to minimize the creation of new ones, the participants did not consider the current legislation enough to cover all these necessities in the current space scenario.

3.2.6 Use Case 6: The Space Situational Awareness Infrastructure

Australia is reliant on Space Situational Awareness (SSA) data from the United States' repository space-track.org. Russia decided to launch an ASAT test, creating debris. In parallel and in an uncoordinated way, North Korean hackers decided to launch a DDoS cyberattack on the website of space-track.org by overwhelming the website with millions of illegitimate requests. To do so, North Korean hackers hacked millions of traditional computers in Southeast Asia to turn them into zombie bots to use them to send requests to space-track.org, rendering the website inaccessible. Therefore, the U.S. must share SSA data with Australia in another way, delaying Australia's capacity to monitor the effects and threats of the ASAT test on its satellites, leading to a collision between a satellite and debris.

Overview

Figure 43: Major Elements of Use Case 6



Attacker(s)

- Russia
- North Korea

Affected Actors

- U.S Space Track website
- South East Asians internet users
- Australian satellite

Attack

- ASAT attack
- DDoS attack on space-track system
- Collision between an Australian satellite and a debris

Issue

- No more access to SSA data
- Reliance on foreign systems

Fallouts

- Temporary inability to track space systems and debris
- Collision and damage on an Australian satellite

Relevant laws and policies

- Bilateral agreements

Relevant Laws and Policies

From a legal perspective, Australia considers space as a critical infrastructure. Therefore, the Security Legislation Amendment (Critical Infrastructure Protection) Act of 2022[365] may appear relevant to this case. However, while domestic space infrastructure and technology are considered as a critical infrastructure, it does not apply to foreign systems such as the U.S. SSA system. As a result, the Security Legislation Amendment Act does not apply.

Similarly, it could be assessed that the Cybercrime Legislation Amendment Act applies to this case as any unauthorized access, modification, or impairment of any data is considered an offence, regardless of how it occurs, which also includes DDoS. However, the space-track repository is not an Australian system, therefore the Act does apply.

In that case, the only applicable frameworks for Australia are bilateral agreements such as ANZUS in the field of cybersecurity to ensure coordination and information-sharing in other ways.

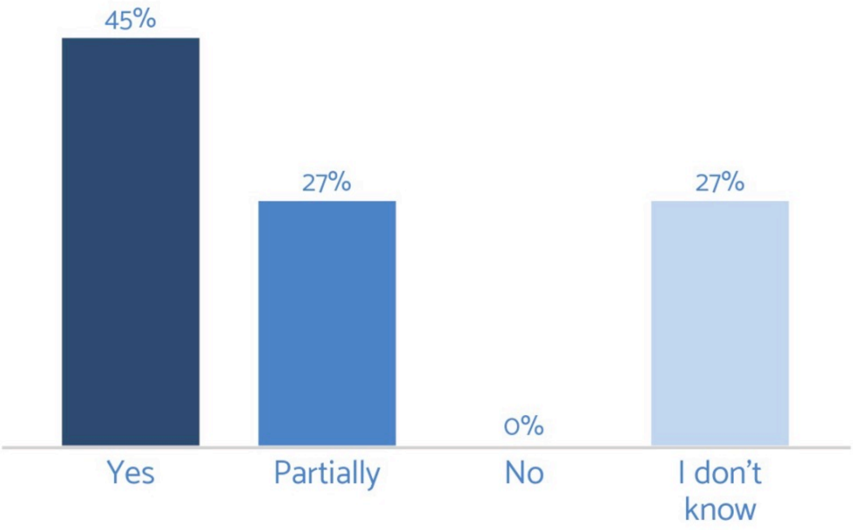
However, the consequences of the attack, that is to say, the collision between a satellite and a debris, are covered by international space law: the Liability Convention. If the debris colliding with the Australian satellite is a debris that comes from the destroyed Russian satellite, which was launched by Russia, then the launching State (Russia) shall be liable to pay compensation for damage caused by its space object on the surface of the earth or to aircraft in flight, regardless of what happened during the cyberattack. To do so, fault must be demonstrated.

Elements for Consideration and Assessment

45% of the workshop's participants considered that there is a policy and legal gap to address this issue. 27% considered that there was only a partial policy and legal gap on that case.

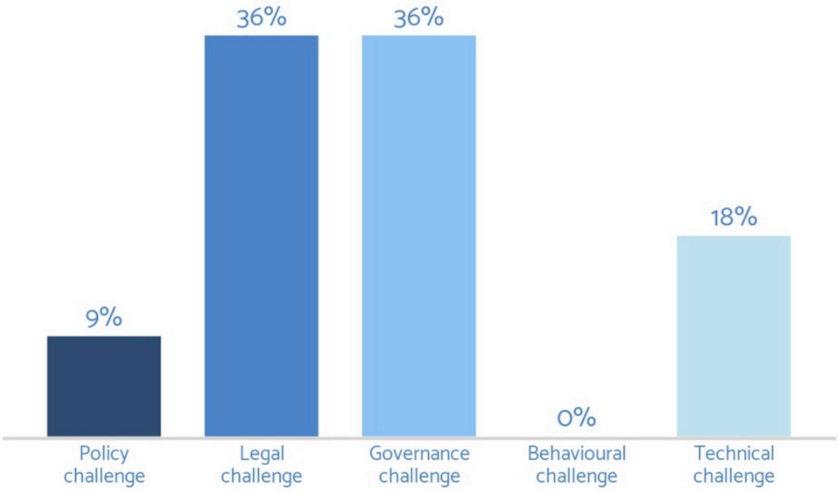
[365] Department of Home Affairs. (2022). *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022.*

FIGURE 44: PERCEIVED PRESENCE OF POLICY AND LEGAL GAPS RELATED TO USE CASE 6



Equally remarkable is that 27% of stakeholder was not aware whether there was a policy or legal gap, an occurrence signalling a low level of awareness with this case.

FIGURE 45: MOST CRITICAL TYPE OF CHALLENGE ASSOCIATED WITH USE CASE 6



36% of workshop participants considered that this case was both a legal and governance challenge. Many participants outlined the issue of reliance on U.S. technology as a policy gap but emphasized that Australia was also well equipped to further develop its SSA infrastructure due to its favourable geographical position.18% of workshop participants considered that it was mostly a technical challenge. 9% of them considered that it was a policy challenge.

This case illustrates that a cyberattack on a foreign system can have ripple effects on an Australian system. An Australian space system can by indirectly impacted by a cyberattack that does not directly target its network or system. This case also demonstrates the issue of inter-dependence and reliance on foreign system. Since space-track is not an Australian system, the Australian ability and capacity to react or adapt its legal and policy framework is limited.

In order to have a clear and adapted framework to this kind of situation, cybersecurity risks and threats should be taken into account when negotiating contracts and/or bilateral agreements with foreign providers. Incident response, coordination, and alternative means of communications should be clearly defined.

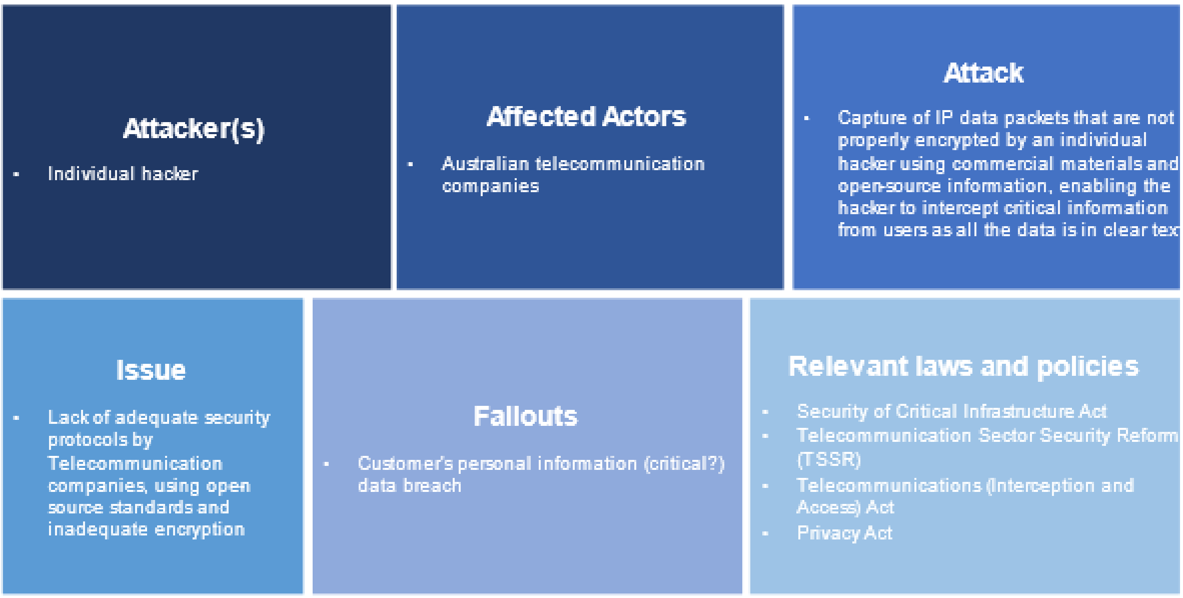
3.2.7 Use Case 7: The Space Segment (Bus)

Considering that Australia mostly has GEO communications satellites, a hacker buys a commercial satellite dish (the one found on the roof of private individuals who have a satellite TV subscription); a DVB board (a circuit board for watching satellite TV on a computer), which costs around $300; a COTS software that allows to search for satellite signals (e.g., EPS Pro) to try to intercept communications' satellites data from Very Small Aperture Terminals (VSAT), which are very present in Australia and used by both commercial and government stakeholders. Then, through Open-Source Intelligence technics, this hacker assembles various information that are readily available on the internet such as the spectrum and radiofrequency bands used by Australian communication satellites, their payloads, and ground stations, as well as their precise positions in orbit. Furthermore, VSAT are using standardized protocols worldwide, which are information available on the internet. The standardisation protocols used for VSAT are the DVB-S and the GSE protocols, which are open-source standards. Then, this hacker writes an algorithm that understands these standards and can find IP data packets to capture. As the communication satellites are not properly encrypted, this method enables the hacker to intercept critical information from users as all the data is in clear text.

Overview

The direct hacking of satellites, although considered unlikely in the past, is now a very concrete threat, especially due to the growing reliance on commercial private companies that do not apply the same standard of protection is use by public stakeholders. The disruption or infiltration of commercial satellites can have a significant impact on the Australian economy as a whole, therefore is important to address the mechanisms that ensure the protection of commercial satellites and the standards that are imposed.

FIGURE 46: MAJOR ELEMENTS OF USE CASE 7



Attacker(s)

- Individual hacker

Affected Actors

- Australian telecommunication companies

Attack

- Capture of IP data packets that are not properly encrypted by an individual hacker using commercial materials and open-source information, enabling the hacker to intercept critical information from users as all the data is in clear tex

Issue

- Lack of adequate security protocols by Telecommunication companies, using open source standards and inadequate encryption

Fallouts

- Customer's personal information (critical?) data breach

Relevant laws and policies

- Security of Critical Infrastructure Act
- Telecommunication Sector Security Reform (TSSR)
- Telecommunications (Interception and Access) Act
- Privacy Act

Considering that Australia mostly has GEO communications satellites, a hacker buys a commercial satellite dish (the one found on the roof of private individuals who have a satellite TV subscription); a DVB board (a circuit board for watching satellite TV on a computer), which costs around $300; a COTS software that allows to search for satellite signals (e.g., EPS Pro) to try to intercept communications' satellites data from Very Small Aperture Terminals (VSAT), which are very present in Australia and used by both commercial and government stakeholders. Then, through Open-Source Intelligence technics, this hacker assembles various information that are readily available on the internet such as the spectrum and radiofrequency bands used by Australian communication satellites such as Optus satellites, their payloads, and ground stations, as well as their precise positions in orbit.77 Furthermore, VSAT are using standardized protocols worldwide, which are information available on the internet. The standardisation protocols used for VSAT are the DVB-S and the GSE protocols, which are open-source standards. Then, this hacker writes an algorithm that understands these standards and can find IP data packets to capture. As the communication satellites are not properly encrypted, this method enables the hacker to intercept critical information from users as all the data is in clear text.

Relevant Laws and Policies

Like case 4, this case also involves the interception of personal information, due to this **The Privacy Act** can be applied. The APP 11 is particularly interesting to the telecommunication company, which dictates that an entity must take reasonable steps to protect personal information it holds from misuse, interference, and loss, and from unauthorised access, modification, or disclosure. The company could be responsible for breaching such principle if were understood that it did not take the necessary preventive measures to protect its customer's data, considering that APP 1 requires entities to take reasonable steps to establish and maintain practices, procedures, and systems to ensure compliance with the APPs.

The Act also institutes a scheme for notification for this data breach (Part IIIB, Divisions 2, 3) and brings APP Codes, which is a more concrete materialization of the APP principles, a written code of practice about information privacy, and may impose additional requirements to those enforced by the Australian Privacy Principles.[366]

The **Telecommunications (Interception and Access Act 1979 (TIA)** protects the privacy of Australians by prohibiting interception of communications and access to stored communications (Part 2.1 and 2.9). Access to such information is only permitted to certain national entities, for certain purposes, such as national security, and after obtaining a warrant,[367] following strict criteria of the Act, only then C/CSPs can legitimately enable a communication passing over their system to be intercepted (Part 2.2 and 2.5), interception performed outside these standards as it was in the present case, is, therefore, according to the act, illicit.

Furthermore, communication is in the list of critical sectors, included by the amendment of the **Security of Critical Infrastructure Act 2018** by the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 which may encompass the telecommunication satellite of this case. In this situation, Part 2B of the Security of Critical Infrastructure Act 2018 requires critical infrastructure operators to report cybersecurity incidents to the Department of Home Affairs and Part 3A authorises Home Affairs to direct and retrieve the data of critical infrastructure industries if a cyberattack has occurred, is occurring, or is deemed to be imminent and prejudices the social and economic stability or defence of Australia.

The security of telecommunications networks and facilities is also contemplated by **The Telecommunication and Other Legislation Act 2017**, which came to strengthen the national security risks of espionage, sabotage and foreign interference to the segment, for this, it brings in Schedule 1, Part 1, security obligations for C/CSPs instituting that they must do their best to protect telecommunications networks and facilities from unauthorised interference or unauthorised access, what include maintaining competent supervision of, and effective control over, telecommunications networks and facilities owned or

[366] An App code that is included in the Code Register and in force is a legislative instrument (Part IIIB, Division 2), for this case, the most significant is the Privacy (Australian Government Agencies – Governance) APP Code 2017.

[367] Agencies can also access communications without a warrant in certain circumstances, such as in an emergency (Part 2-3).

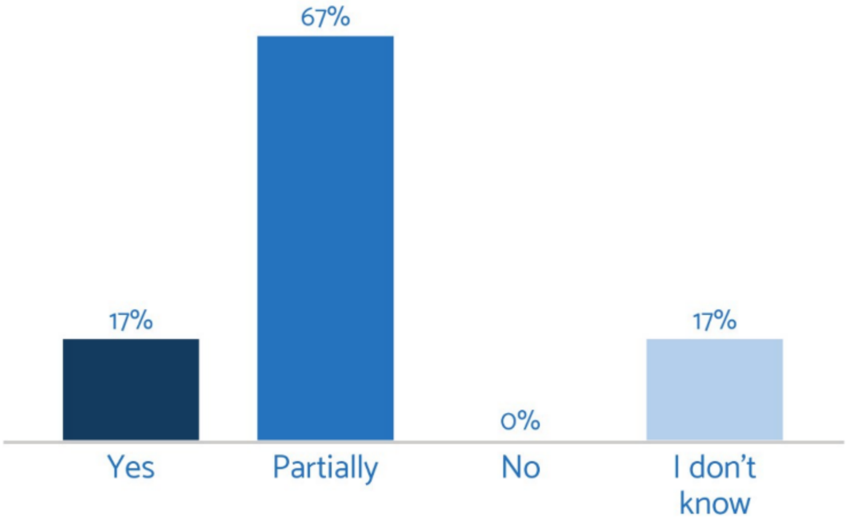
operated by the carrier or provider. In the present case, a such breach could trigger the Secretary of the Attorney-General's Department (AGD) power to obtain information and documents to monitor and investigate their compliance with the security obligation, to seek to evaluate the vulnerabilities in which the interception was based.

From a policy perspective, while the **Information Security Manual** does not directly cover specifically satellites or the space system as a whole, that does not mean that many of its directives are not applicable to the sector, the use of commercial satellites is generally considered less protected for not having the same protection standard as a defence satellite, and, for this reason, the use of security framework developed by the ASCS becomes even more relevant, especially the directives regarding encryption brought on the Guidelines for Cryptography like ISM-0507 (Cryptographic key management processes, and supporting cryptographic key management procedures, are developed, implemented and maintained), and ISM 1080 (An ASD-Approved Cryptographic Algorithm (AACA) or high assurance cryptographic algorithm is used when encrypting media).

Elements for Consideration and Assessment

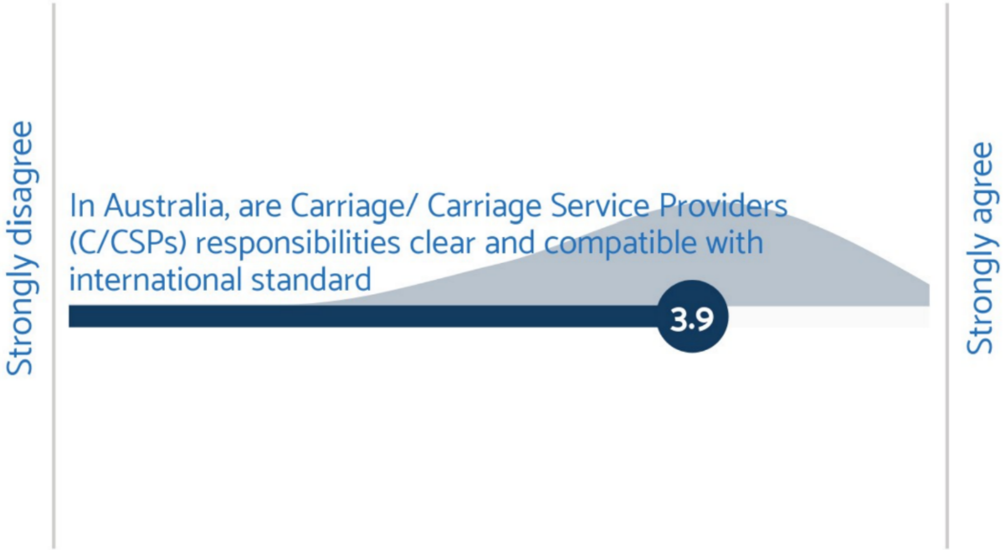
84% of the participants perceive gaps or partial gaps related to this case, with such gaps being related to either the governmental control activity or the internal procedures of commercial space companies that deal with personal data.

FIGURE 47: PERCEIVED PRESENCE OF POLICY AND LEGAL GAPS RELATED TO USE CASE 7



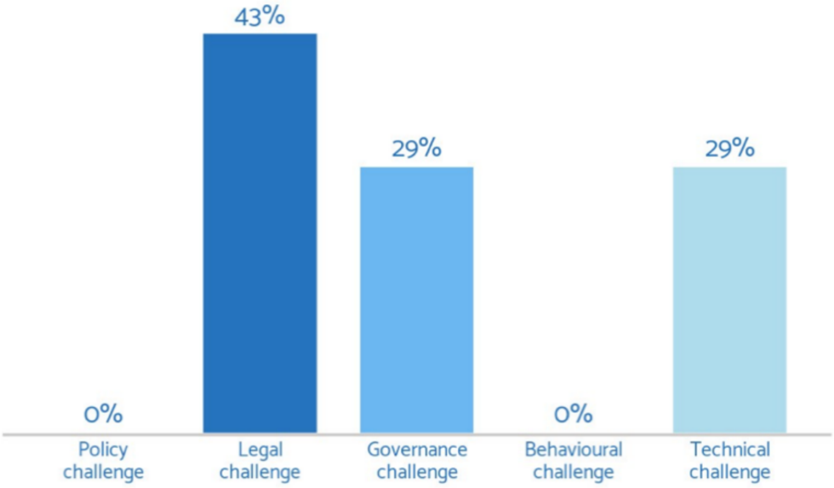
Overall, consulted stakeholders agree that Australia C/CSPs responsibilities are clear and compatible with international standards, this, however, did not prevent approximately 10 million Australians from having their data compromised in a recent hacking scandal on the country's second-largest telecommunications company.

FIGURE 48: STATEMENT ASSESSMENT



Attesting that cyberattacks targeting private companies that deal with private information are a complex and sensitive issue, the participants demonstrated a diverse understanding of what would be the biggest challenge in this case. The majority pointed to legal challenge (43%), with governance challenge and technical challenge relevantly following with 29% each.

FIGURE 49: MOST CRITICAL TYPE OF CHALLENGE ASSOCIATED WITH USE CASE 7



An important point raised during the interaction with the contributors and focused on during a singular interview with one of the participants was regarding what would be the exact illicit character of the act. In general, people assume that the narrated act was a cyberattack, however, the Australian Government defines this kind of attack as a deliberate act through cyberspace to manipulate, disrupt, deny, degrade or destroy computers or networks, or the information resident on them, with the effect of seriously compromising national security, stability or economic prosperity.[368] Through this definition, it is arguable that there was a cyberattack in the present case since none of the illicit tonic verbs was present; manipulate, disrupt, deny, degrade and destroy.

The interception was also questioned on the premises that, since the information was not encrypted it could not be considered intercepted, a parallel with a non-encrypted radio frequency was drawn, in the sense of, if a person made effort to access that frequency, it would be considered or not as an interception. It is relevant to point out that, although some of the participants questioned the existence of the interception act, none of them agreed in considering the possible intercepted information as public information merely due to lack of proper encryption, diverging about what would be the nature of the act in this context.

In this sense, is precious to refer to how interception is defined by the Telecommunications (Interception and Access) Act 1979, as a communication passing over a telecommunications system consists of listening to or recording, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication (Part 1-2. s 6). That is, completely indifferent to the existence, or not, of encryption.

Another debated point was regarding the possibility/necessity of a stronger regulatory framework to hinder obtaining certain equipment/technologies that could be used for interception purposes, not only the prohibition was discussed, but also a necessity to register such equipment in an accessible governmental list.

3.2.8 Use Case 8: The Space Segment (Payload)

An attacker from a state-sponsored (Chinese) hacker group found protocol vulnerabilities in software defined radios. This vulnerability is not patched on the SDR of a commercial customer hosted on an Australia communication satellite and therefore can be exploited. The attacker is using this vulnerability to enter the SDR and infect it with malicious code without being detected. The code aims at making the SDR believe that the frequencies are correct when it should adjust them to establish communication with the ground station. As a result, the SDR stays on the same frequency and cannot communicate with the ground segment anymore, resulting in a denial of access. In addition, the fact that the SDR stays on this same frequency also creates interference with other satellites. The ground station cannot communicate anymore with its satellite but instead send signals, which are received by the neighbouring satellites, creating confusion for all operators.[83] Consequently, the SATCOM service is interrupted for end-users, which lost access to satellite television services.

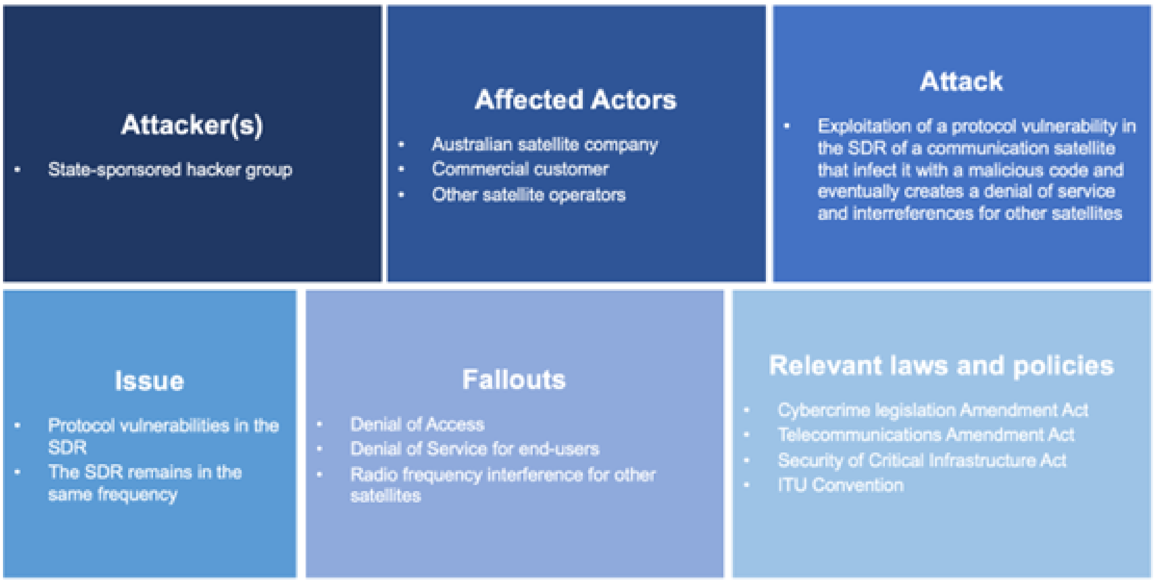
Overview

Considering that Australia's space infrastructure mostly consists of geostationary communication satellites, an attack disrupting the SATCOM service provided by such satellites proves particularly relevant. Furthermore, the specific attack purpose considered in this case – i.e., a denial of information was deemed as the single most likely type of attacks within the Australian context, even though also the least impactful (see section 2.2.2).

At the same time, the considered use case shows that a denial of access and service can generate several additional – and not necessarily premeditated – implications, such as radio-frequency interference for other satellite operators. Major elements of the considered case are summarised below.

[368] Department of Foreign Affairs and Trade. (2017). *Australia's International Cyber Engagement Strategy*. Commonwealth of Australia.

Figure 50: Major Elements of Use Case 8



Attacker(s)

- State-sponsored hacker group

Affected Actors

- Australian satellite company
- Commercial customer
- Other satellite operators

Attack

- Exploitation of a protocol vulnerability in the SDR of a communication satellite that infect it with a malicious code and eventually creates a denial of service and interreferences for other satellites

Issue

- Protocol vulnerabilities in the SDR
- The SDR remains in the same frequency

Fallouts

- Denial of Access
- Denial of Service for end-users
- Radio frequency interference for other satellites

Relevant laws and policies

- Cybercrime legislation Amendment Act
- Telecommunications Amendment Act
- Security of Critical Infrastructure Act
- ITU Convention

Relevant Laws and Policies

From an international legal perspective, several hard law provisions come into consideration. Deliberate interference with broadcast signals constitutes a violation of the international legal regime, including:

- Article 45 of the **ITU Convention**, which states that ‘Member States recognises the necessity of taking all practicable steps to prevent the operation of technical apparatus and installations of all kinds from causing harmful interference to the radio services or communications’.
- Article 9 of the **Outer Space Treaty**, which refers to the necessity for States Parties to avoid any ‘harmful interference’. Jamming can also be considered ‘harmful interference’.
- Article 19 of the **UN Charter**, which states that individuals should have ‘the freedom to seek, receive and impart information and ideas through any media and regardless of frontiers’.
- Article 1 of the **Draft Articles on Responsibility of States for Internationally Wrongful Acts**, which specified that every internationally wrongful act of a state entails the international responsibility of that state.

At the same time, no concrete guidelines exist concerning how to prevent politically intentional jamming (and, for that matter, other intentional interference with space assets) and how to proceed when they occur.

Despite the ability to attribute technically the jamming source to a territory, there are no enforcement mechanism have been envisaged to sanction who is causing harmful interreference.

From a domestic legal perspective, applicable legislation includes first and foremost the **Radiocommunications Act 1992,** in particular, Part 4.2 and 4.3, which respectively regulate offences relating to radio emissions and the settlements of interferences disputes. According to the Act, interference means:

- in relation to radiocommunications—interference to, or with, radiocommunications that is attributable, whether wholly or partly and whether directly or indirectly, to an emission of electromagnetic energy by equipment; or

- in relation to the uses or functions of equipment—interference to, or with, those uses or functions that is attributable, whether wholly or partly and whether directly or indirectly, to an emission of electromagnetic energy by equipment

Article 197 of the Act specifies that ‘a person must not engage in conduct that will result, or is likely to result, in (a) substantial interference; or (b) substantial disruption; or (c) substantial disturbance to radiocommunications: within Australia; or between a place in Australia and a place outside Australia’.

Another relevant law is the **Security of Critical Infrastructure Act 2018.** Regulated entities under Part 2b of the Security of Critical Infrastructure Act 2018 as well as carriers or service providers under the Telecommunications Act 1997 covered by the Telecommunications Security Information instruments,[369] are subject to mandatory cyber incident reporting requirements.

More specifically, if regulated entities become aware that a critical cybersecurity incident has occurred, or is occurring, and the incident has had, or is having, a significant impact[370] on the availability of their asset, they must notify the Australian Cyber Security Centre (ACSC) within 12 hours (in case of critical cybersecurity incidents) or 72 hours (in case of other cybersecurity incidents) after they become aware of the incident. Should they make the report verbally, then they must make a written record within 84 hours of verbally notifying the ACSC. A form is provided,[371] where it needs to be indicated the reason for reporting (either inform the ACSC and/or request assistance or advice from the ACSC).

As in use case 7 (see Section 3.2.7), the security obligations contained in Schedule 1, Part 1 of the **Telecommunication and Other Legislation Act 2017** (which require C/CSPs to do their best to protect telecommunications networks and facilities from unauthorised interference or unauthorised access) could come into consideration. The attack could also trigger the Secretary of the Attorney-General’s Department (AGD) power to obtain information and documents to monitor and investigate their compliance with the security obligation, to seek to evaluate the vulnerabilities in which the interception was based.

From a policy perspective, the ACSC-released **Information Security Manual** provides several relevant security guidelines, particularly those related to system hardening.

Regarding the present case, the implementation of specific controls contained therein would have likely mitigated the attack considered in this case,[372] including:

- ISM-1743 (Operating systems are chosen from vendors that have made a commitment to secure-by-design principles, secure programming practices and maintaining the security of their products.
- ISM-1034 (A Host-based Intrusion Prevention System (HIPS) is implemented on critical servers and high-value servers.)
- ISM 1791 (the integrity of applications, ICT equipment and services are assessed as part of acceptance of products and services.),

[369] Part 2 of the Telecommunications (Carriage Service Provider—Security Information) Determination 2022 or the Telecommunications (Carrier Licence Conditions—Security Information) Declaration 2022.

[370] A significant impact is one where both the critical infrastructure asset is used in connection with the provision of essential goods and services; and the incident has materially disrupted the availability of those essential goods or services.

[371] Australian Cyber Security Centre. (n.d.) *Report Cyber*. https://www.cyber.gov.au/acsc/report

[372] Australian Cyber Security Centre. (2023). *Information Security Manual*. Commonwealth of Australia. p.17. https://www.cyber.gov.au/sites/default/files/2023-09/Information%20Security%20Manual%20%28September%202023%29.pdf

- ISM 1792 (the authenticity of applications, ICT equipment and services are assessed as part of acceptance of products and services.)

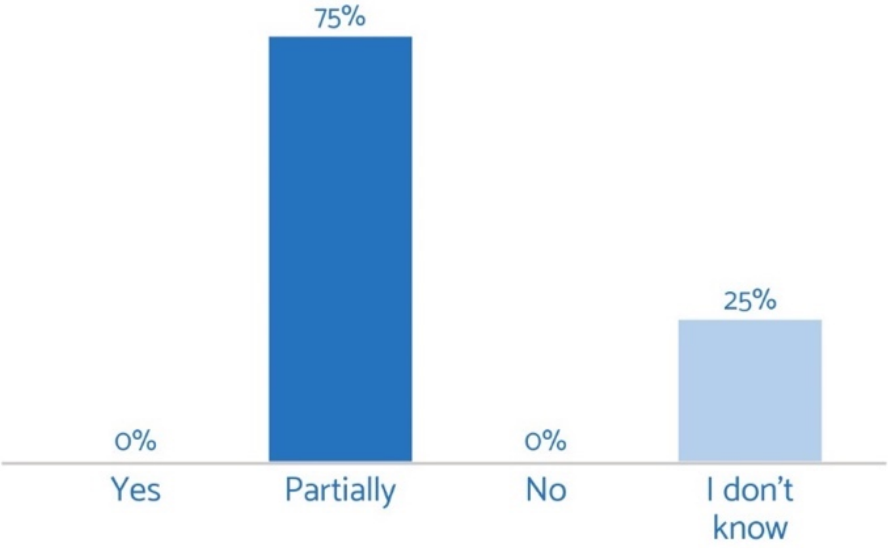
However, as for other cases, an organisation is not required by law to comply with the ISM, nor the ISM does override any obligations imposed by legislation or law.

Still, if there was a national security element to the operations of the satellites or the commercial payload operator was a DISP member organisation, then the **Defence Industry Security Program (DISP)** and all its controls would have applied, and the effect of the attack mitigated.[373]

Elements for Consideration and Assessment

The vast majority of consulted stakeholders recognise the existence of policy and legal gaps related to this specific case, with a significant number of stakeholders (25%) not knowing whether there are gaps.

FIGURE 51: PERCEIVED PRESENCE OF POLICY AND LEGAL GAPS RELATED TO USE CASE 8

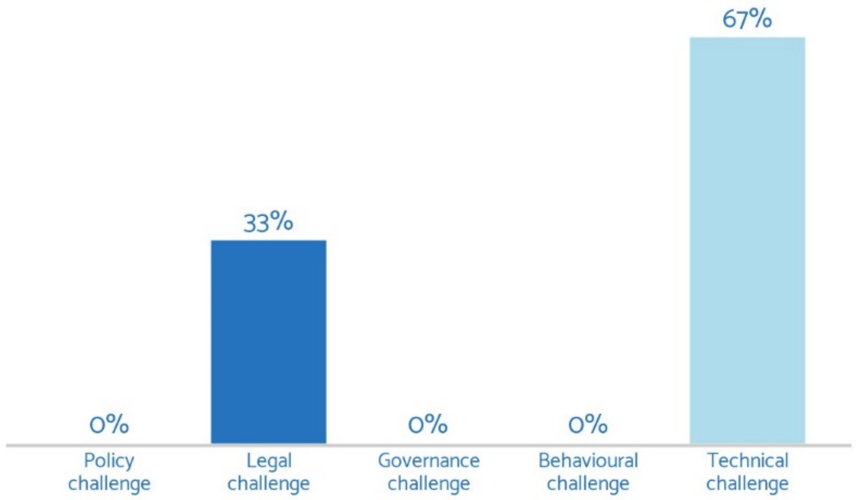


For Australia to be better prepared for this kind of attacks, there was ample consensus on the need to seek new multilateral solutions with international partners, in addition to developing dedicated regulations and best practices tailored for space communication systems.

However, according to consulted stakeholders, this specific use case mostly confronts Australia's space sector with technical challenges. While there some legal improvements may be needed, this type of attacks must be tackled through technical solutions.

[373] Department of Defence. (2020). *Defence Security Principles Framework*. https://www.defence.gov.au/sites/default/files/2020-12/DSPF-OFFICIAL.pdf

FIGURE 52: MOST CRITICAL TYPE OF CHALLENGE ASSOCIATED WITH USE CASE 8

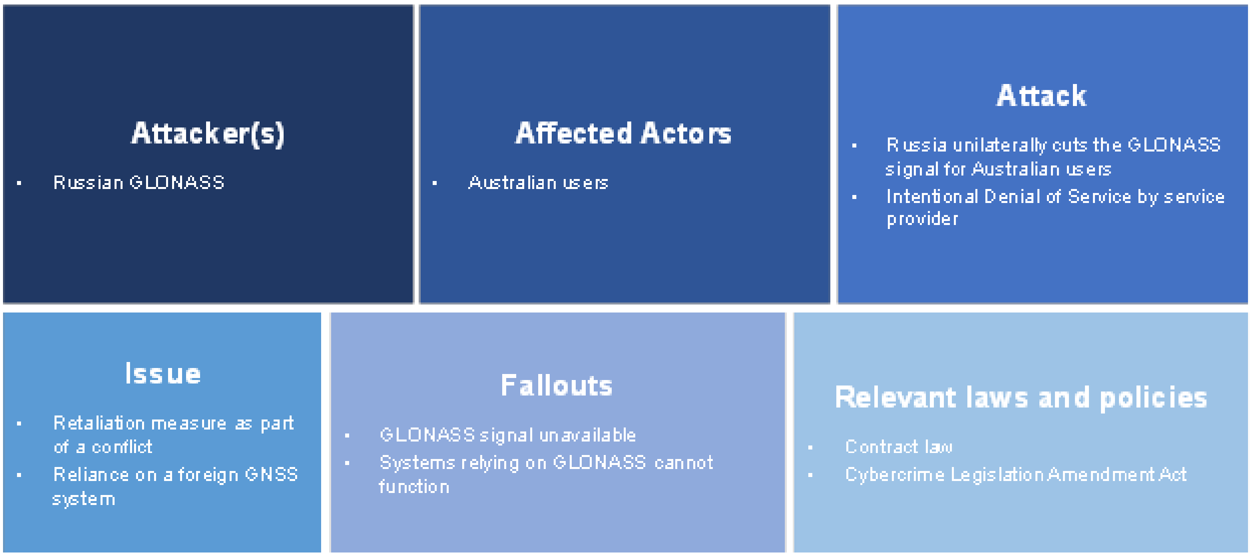


3.2.9 Use Case 9: The User Segment

Overview

Cyber risks can also be seen from the perspective of reliance on foreign systems and services. Indeed, a Deny of Service (DoS) can result from an interruption of service by the service provider of a foreign software or system in case the interests of Australia and a foreign country or an Australian company and ta foreign company are not aligned anymore. In this use case, GNSS such as the GLONASS has been interrupted by the service provider. Key elements of this specific use case are summarised in the following:

FIGURE 53: MAJOR ELEMENTS OF USE CASE 9



Attacker(s)

- Russian GLONASS

Affected Actors

- Australian users

Attack

- Russia unilaterally cuts the GLONASS signal for Australian users
- Intentional Denial of Service by service provider

Issue

- Retaliation measure as part of a conflict
- Reliance on a foreign GNSS system

Fallouts

- GLONASS signal unavailable
- Systems relying on GLONASS cannot function

Relevant laws and policies

- Contract law
- Cybercrime Legislation Amendment Act

Relevant Laws and Policies

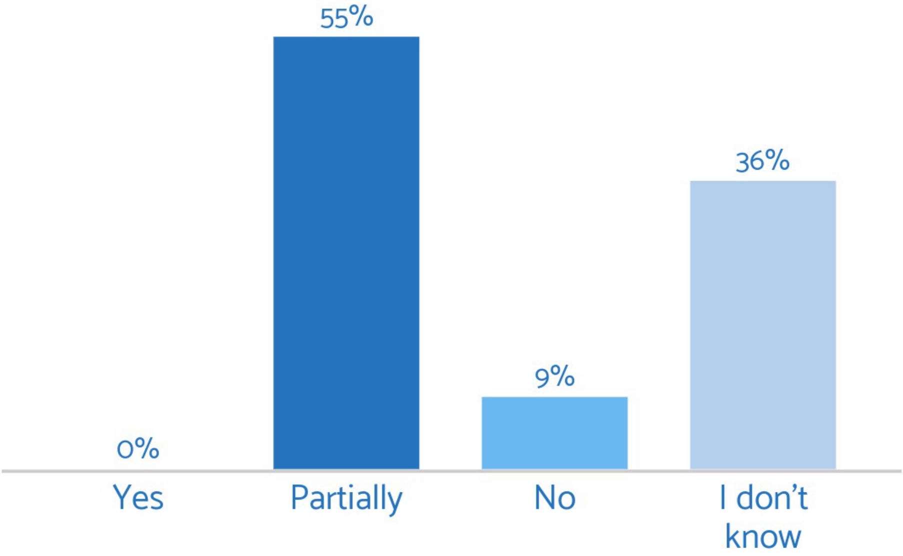
This use case would mostly involve contract law as the provider breaches the contract and unilaterally cuts the signal.

However, it may be argued that the **Cybercrime Legislation Amendment Act** applies to the situation as any unauthorised access, modification, or impairment of any data is considered an offence, including any conduct which diverts or redirects communications, including during a denial-of-service attack.[374] However, here the service provider does not conduct an attack per say where the GNSS is overwhelmed with malicious requests, it simply cuts the service. Therefore, it is not clear whether it could apply.

Elements for Consideration and Assessment

55% of workshop participants considered that there is a partial gap in the Australian's policy and legal framework. 9% of them considered that there is no gap regarding this case. 36% did not know.

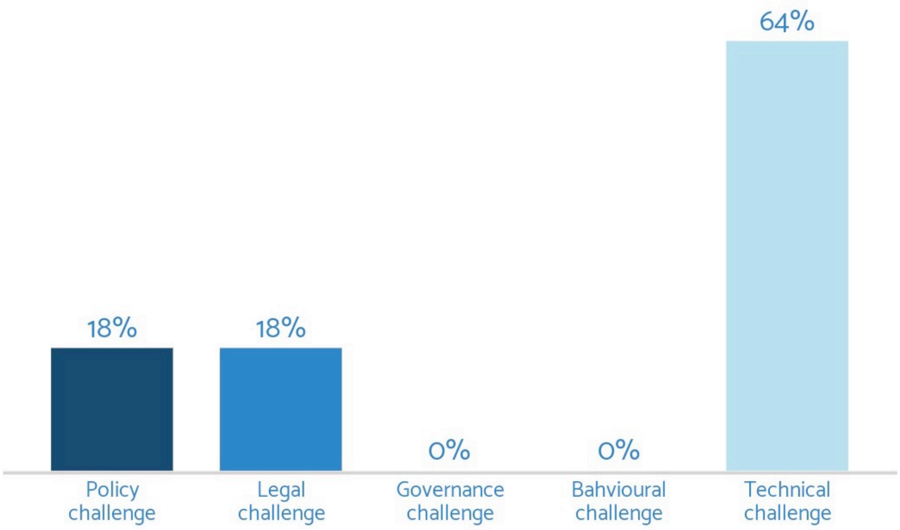
FIGURE 54: PERCEIVED PRESENCE OF POLICY AND LEGAL GAPS RELATED TO USE CASE 9



64% of workshop participants considered the issue as mostly technical, emphasizing that it was about GNSS interoperability and relying on several GNSS constellations and/or developing sovereign PNT to avoid that issue. Workshop participants further emphasized that *'it is almost impossible to stop an entity not providing a service if they choose not to. This is the argument for sovereignty'*. Others pointed that that *'even with useful legislation or agreements in place, the enforcement would be near impossible, especially during war'*.

[374] Swinson, J., et al. (2014) *Australia's Cybercrime Legislation*. King & Wood Mallesons. https://www.lexology.com/library/detail.aspx?g=4ab62fdd-f177-47eb-b02d-e327cf9833a9

FIGURE 55: MOST CRITICAL TYPE OF CHALLENGE ASSOCIATED WITH USE CASE 9



This issue is mostly addressing a policy posture rather than a legal gap, which calls for a diversification of the reliance on GNSS signal as well as increased interoperability between GNSS signals to compensate the loss of one constellation's signal by using another's. In addition, it also calls for the development of sovereign PNT capabilities as a policy measure. From a strategic perspective, it is also about being aware that this kind of retaliation measure can be taken by an adversary as the space sector is increasingly politicised and conflictual.

3.2.10 Use Case 10: The User Segment

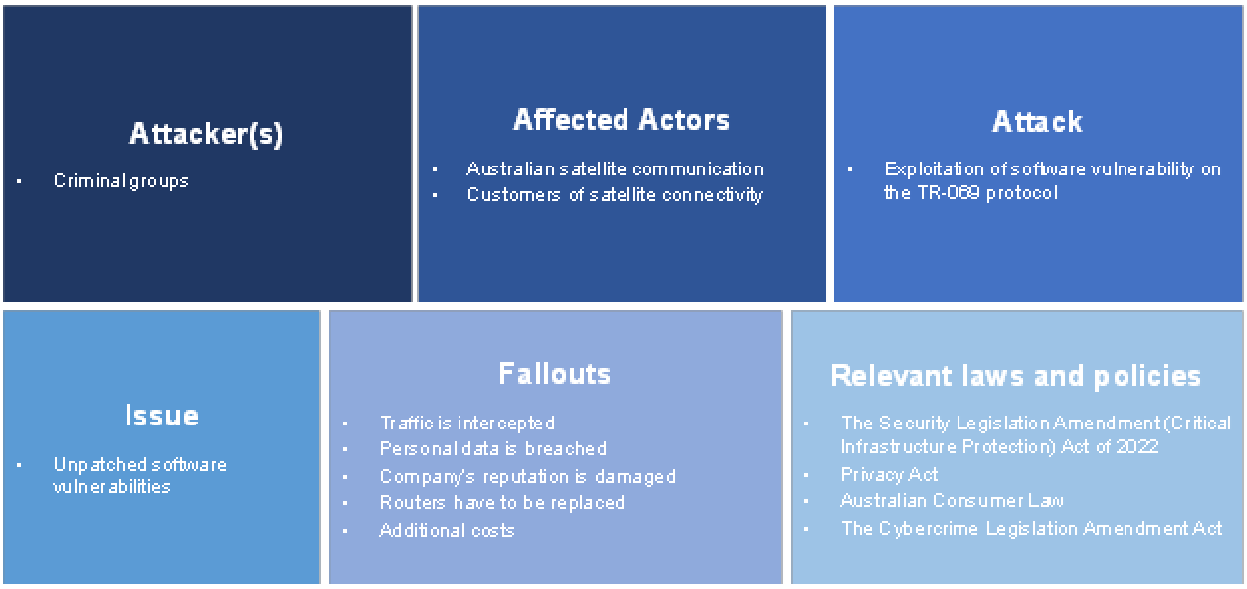
An Australian satellite communication company provides internet broadband to users. Users connect to the satellite broadband through a router provided by the company. The router uses the TR-069 remote management protocol to enable the satellite company to remotely update the router of all its customers and perform diagnostics as well as other remote tasks. However, this protocol has software vulnerabilities, which are exploited by several criminal groups. The satellite company did not set up the router to use HTTPS and simply kept the use of HTTP between its Access Control Service (ACS) and the users' satellite routers. Additionally, the software used by the company's ACS to enable the remote management of their customers' TR-069-enabled routers contains vulnerabilities, enabling several remote code executions. As a result, the criminal groups are retrieving all the internet traffic of the customers, which is in clear text, and contains bank account credentials and credit card numbers used for online shopping, enabling them to steal money. Following this attack, the company's reputation is damaged, and all the routers must be replaced as the company did not enable end-users to access the management settings of the routers to disable the TR-069 protocol, leading to additional costs.[375]

Overview

Key elements of this specific use case are summarised in the following:

[375] Jackson, M. (2014). *Millions of Routers Supplied by Broadband ISPs Vulnerable to TR-069 Hackers*. ISP Review. https://www.ispreview.co.uk/index.php/2014/08/routers-supplied-broadband-isps-vulnerable-tr-069-hackers.html

FIGURE 56: MAJOR ELEMENTS OF USE CASE 10



Attacker(s)

- Criminal groups

Affected Actors

- Australian satellite communication
- Customers of satellite connectivity

Attack

- Exploitation of software vulnerability on the TR-069 protocol

Issue

- Unpatched software vulnerabilities

Fallouts

- Traffic is intercepted
- Personal data is breached
- Company's reputation is damaged
- Routers have to be replaced
- Additional costs

Relevant laws and policies

- The Security Legislation Amendment (Critical Infrastructure Protection) Act of 2022
- Privacy Act
- Australian Consumer Law
- The Cybercrime Legislation Amendment Act

Relevant Laws and Policies

The Security Legislation Amendment (Critical Infrastructure Protection) Act of 2022 likely applies to the case. Indeed, the Act defines space technology sector as *'the sector of the Australian economy that involves the commercial provision of space-related services'*, which seems to include satellite user terminals of the SATCOM provider. The Act provides examples of space-related services such as *'position, navigation and timing services in relation to space objects; space situational awareness services; space weather monitoring and forecasting; communications, tracking, telemetry and control in relation to space objects; remote sensing earth observations from space; facilitating access to space.'* Therefore, the Act likely applies even though the attack did not target the satellite itself. The satellite company must report the cyber incident to the ACSC within 72 hours.

In addition, **the Cybercrime Legislation Amendment Act** may apply to the situation as any unauthorised access, modification, or impairment of any data is considered an offence, regardless of how it occurs, which suggests that it also includes the exploitation of software vulnerabilities.

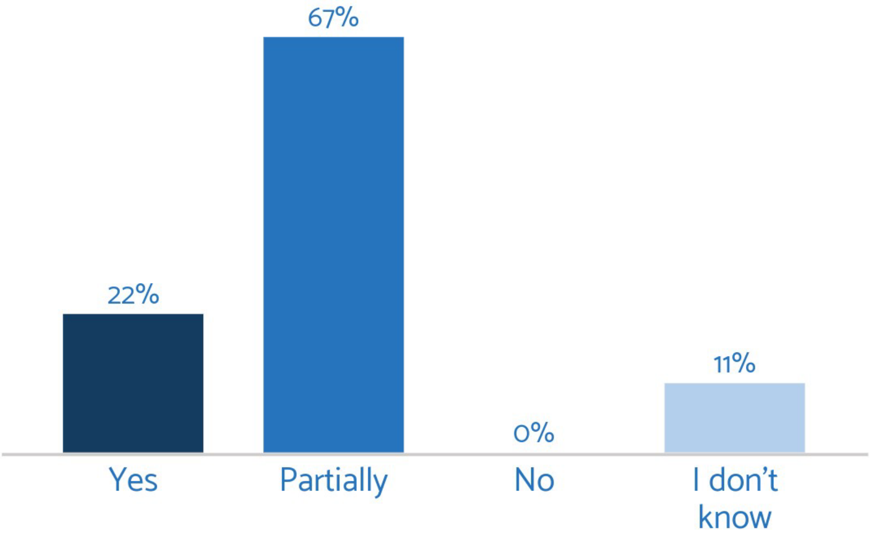
As personal data was breached, accessed, and maliciously used, **the Privacy Act** likely applies. In the case that the satellite company has an annual turnover of $3 million, the Australian Privacy Principles apply to that company. First, the Notifiable Data Breaches scheme applies to the case and requires that affected users and the Office of the Australian Information Commissioner (OAIC) are notified of the breach. The Privacy Act also enables the user of the SATCOM service to seek damages from the SATCOM company for the exploitation of their personal data. The user can make a claim to the Privacy Commissioner, which will investigate the case, determine whether privacy was breached and require the SATCOM company to pay damages.

The user may also have claims for the data privacy breach based on breach of contract, negligence or contravention of the Australian Consumer Law if personal data protection and/or cybersecurity is mentioned in the contract between the SATCOM provider and the user.

Elements for Consideration and Assessment

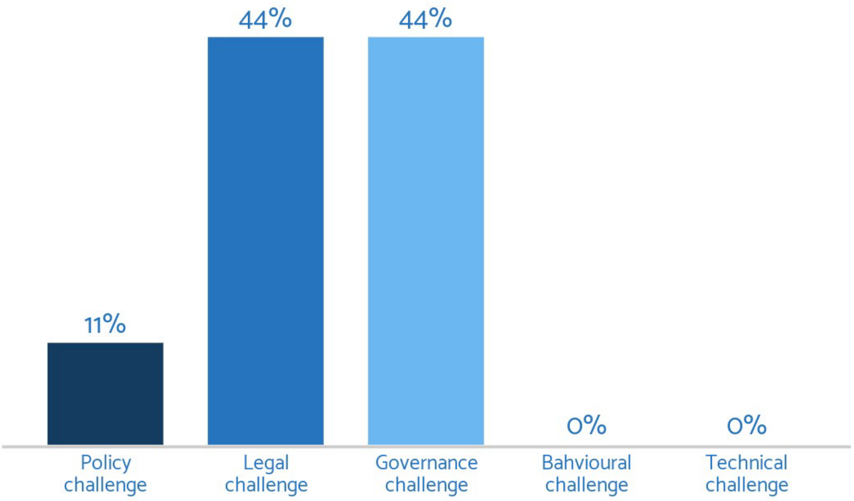
67% of workshop participants consider that there is a partial policy and legal gap regarding this case. 22% of them consider that there is a policy and legal gap. 11% did not know.

FIGURE 57: PERCEIVED PRESENCE OF POLICY AND LEGAL GAPS RELATED TO USE CASE 10



Most workshop participants considered that this case would mostly be a legal and a governance challenge should it happen to their organisation. None of the participants considered this case as a behavioural or technical challenge.

FIGURE 58: MOST CRITICAL TYPE OF CHALLENGE ASSOCIATED WITH USE CASE 10



The Australian legal framework is adapted to the case when it comes to the end-users, who are victims of the cyberattack. However, when it comes to ensuring the cybersecurity of the satellite user terminals, the Australian policy and legal framework seems more limited.

Gap Analysis and Security Measures

This section provides a gap analysis regarding the commitment and maturity of the Australian policy, legal and governance frameworks regarding space cybersecurity. Subsequently, based on the policy and legal assessment as well as the case studies, several recommendations are outlined to improve the overall cybersecurity of the Australian space infrastructure.

4.1. Gap Analysis

4.1.1 A Comparative Assessment of Australia's Commitment to Space Cybersecurity

The ITU's Global Cybersecurity Index, which measures the commitment and level of cybersecurity of 193 UN Member States and the State of Palestine to identify areas of improvement, identify gaps, and encourage the adoption of additional cybersecurity measures in the field of cyber law, technical aspects, organisational aspects, capacity development, and cooperation. The Index is based on a questionnaire of 82 questions, which measures 20 indicators and 5 pillars, which are then cross-referenced and cross-checked with open-source information. Each question is assigned a score, which is then aggregated to provide an overall assessment of the state of cybersecurity measures in each country.

In the Global Cybersecurity Index, Australia is ranked 12th with an overall score of 97.47 out of 100, which demonstrates a high level of commitment for cybersecurity and the adoption of the relevant policy, legal, and organisational framework to tackle cyber threats. Australia is relatively strong in the fields of legal measures and capacity development measures. The ITU notes that organisational measures may be an area for future improvement.

Should this general cybersecurity assessment be transposed to space cybersecurity measures, the commitment to space cybersecurity measures is more scattered, unclear, and limited. The table below provides a comparative overview:

TABLE 15: COMPARATIVE ANALYSIS OF GENERAL CYBERSECURITY MATURITY AND SPACE CYBERSECURITY MATURITY IN AUSTRALIA

Legal				
Measuring the laws and regulations on cybercrime and cybersecurity	Some form of cybersecurity legislation	✓	Some form of dedicated space cybersecurity legislation	✗
	Data Protection Regulations	✓	Data Protection Regulations mention or cover space-based data	✗
	Critical Infrastructure Regulations	✓	Space is considered as a critical infrastructure	✓*
Technical				
Measuring the implementation of	Active CIRTS	✓	CIRTS integrate attacks and risks on the space infrastructure	?

technical capabilities through national and sector specific agencies	Engaged in a regional CIRT	✓	Engaged in a regional CIRT where space in covered	?
	Child Online Protection Reporting mechanism	✓	Clear and identified space infrastructure's cyber incident reporting mechanism	?
Organisational				
Measuring the national strategies and organisations implementing cybersecurity	National Cybersecurity Strategies	✓	Dedicated Space Cybersecurity Strategies	✗
	Cybersecurity Agencies	✓	Space Cybersecurity Agencies or National Agencies with a clear mandate on space cybersecurity	✓
	Child Online Protection strategies and initiatives reported	✓		
Capacity Development				
Measuring awareness campaigns training, education, and incentives for cybersecurity capacity development	Cyber awareness initiatives	✓	Space cybersecurity awareness initiatives	✓
	Cybersecurity R&D programs	✓	Space cybersecurity R&D programs	✓*
	Cybersecurity industries	✓	Space cybersecurity industries	?
Cooperation				
Measuring partnerships between agencies, firms, and countries	Cyber PPP	✓	Space Cybersecurity PPP	✓
	Cyber bilateral agreements	✓	Space Cybersecurity bilateral agreements	?
	Cyber multilateral agreements	✓	Space Cybersecurity multilateral agreements	?

The table above demonstrates the high level of commitment of Australia to general cybersecurity measures. However, many areas of improvement remain regarding measures dedicated to the cybersecurity of the space infrastructure. Still, Australia's policy and legal framework is not devoid of measures that can be applicable to cyberattacks against space systems and many efforts were conducted or launched in 2022.

Indeed, it should be noted that while Australia does not have a space cybersecurity law, several Australian legislations can be applied in the case of a cyberattack against an Australian space system (e.g., the Security Legislation Amendment Act, the Cybercrime Legislation Act, the Telecommunication Act, etc.). Additionally, the recognition of space as a critical infrastructure enables better protection and response to cyber incidents.

The reform extends obligations to various participants in the space supply chain including 'responsible entities', 'reporting entities', 'direct interest holders', 'managed service providers' and 'operators.' However, as the Act is recent, no specific space assets are listed as critical infrastructure, and several uncertainties remain regarding the specific positive obligations responsible entities have to comply with (see below).

In terms of capacity development, R&D activities are nascent in Australia. However, it must be noted that some initiatives are being carried out by universities such as the University of Adelaide, the University of New South Wales. SmartSat CRC and the University of South Australia are also initiating R&D in space cybersecurity. A space cybersecurity industry or ecosystem is has not yet emerged.

At the policy level, while Australia does not have a space cybersecurity strategy, cyber threats are acknowledged in the newly released Space Defence Strategy and both space and cyberspace are recognized as warfighting domains by the Department of Defence.

Nonetheless, specific measures are rather rare, space is very rarely mentioned in Australian cybersecurity policies as illustrated below:

TABLE 16: REFERENCES TO SPACE AND CYBERSECURITY IN THE POLICY FRAMEWORK

Cybersecurity Policies	References to Space
Australia's Cyber Security Strategy 2020	✗
International Cyber and Critical Technology Engagement Strategy	✓
2016 Defence White Paper	✓
2020 Defence Strategic Update	✓
Information Security Manual	✗
Strategies to Mitigate Cyber Security Incidents	✗
2022 National Plan to Combat Cybercrime	✗
Digital Economy Strategy: A Leading Digital Economy and Society by 2030	✓
Cyber Incidents Response Plan	✗
Ransomware Action Plan	✗
Cyber Legislations	

Privacy Act 1988	✗
The Cybercrime Legislation Amendment Act	✗
Telecommunications and Other Legislation Amendment Act	✗
Security Legislation Amendment (Critical Infrastructure Protection) Act 2021	✓
Telecommunications and Other Legislation Amendment (Assistance and Access) Act	✗
Radiocommunications Act 1992	✓
Space Policies	**References to Cybersecurity**
Australia Civil Space Strategy	✓
Defence Space Strategy	✓
Australia in Space: a Decadal Plan for Australian Space Science 2021-2030	✓
Space Legislations	
The Space Activities Act and the Space Activities Amendment (Launches and Returns) Act	✗
International Treaties	
The Outer Space Treaty (1967)	✗
The Rescue Agreement (1968)	✗
The Liability Convention (1972)	✗
The Registration Convention (1975)	✗
The Moon Agreement (1979)	✗

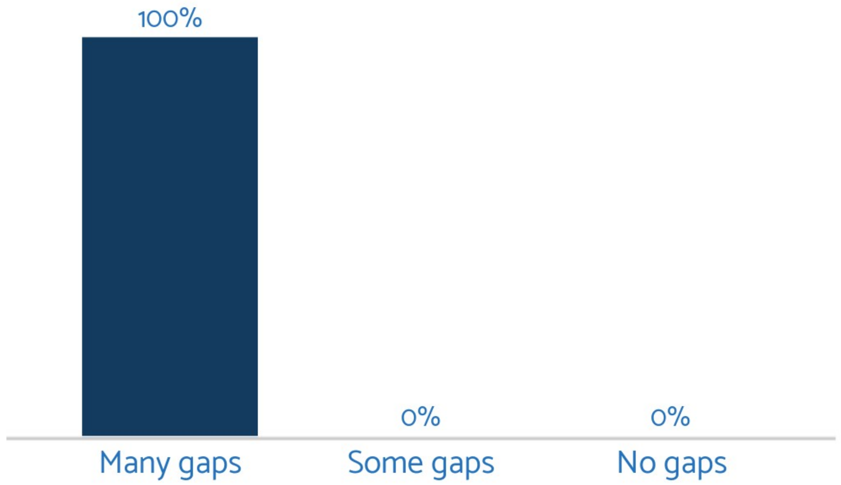
Furthermore, at the organisational level, while Australia does not have a dedicated space cybersecurity agency, the Signals Directorate and the Australian Cyber Security Centre marginally deal with some space cybersecurity issues. At the same time, the Cyber and Infrastructure Security Centre and the Trusted Information Sharing Network (TISN) deal with space cybersecurity threats and engage with space operators as part of the updated critical infrastructure legislation. However, it is not clear to which extent all these entities interact and cooperate to ensure an efficient implementation of cybersecurity measures and incident response and avoid the duplication of efforts and the lack of cross-agencies communications.

As Australia can be considered as an emerging spacefaring nation with a recently established national space agency and space strategy, its progress in space cybersecurity is already significant. The fact that Australia's efforts in the space sector started to mature rather recently is even more of a reason to put a strong focus on space cybersecurity. Cybersecurity must be considered in the design phase of space programs and the cybersecurity strategy has to be established at the beginning to increase efficiency and compliance. Governance, engineering, and laws must be combined to ensure that the Australian space program is ready to face cyber threats.

4.1.2 An Assessment Based on Consulted Stakeholders

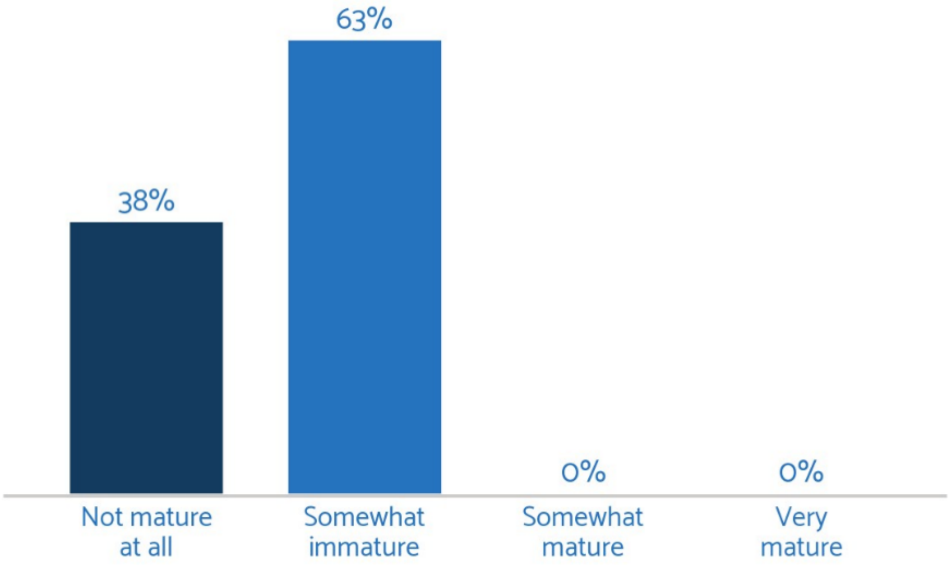
This general assessment was also confirmed by the workshop organised with Australian policy stakeholders. When benchmarking the maturity of the policy and legal framework against cyber threats specific of the space infrastructure, several gaps come to the fore. The figures below present the perception of cyber threats on the Australian space infrastructure and the maturity of the policy and legal framework.

FIGURE 59: PERCEIVED GAPS IN AUSTRALIA'S POLICY AND LEGAL FRAMEWORK



Remarkably, all workshop participants considered that many gaps exist in Australia's policy and legal framework regarding space cybersecurity.

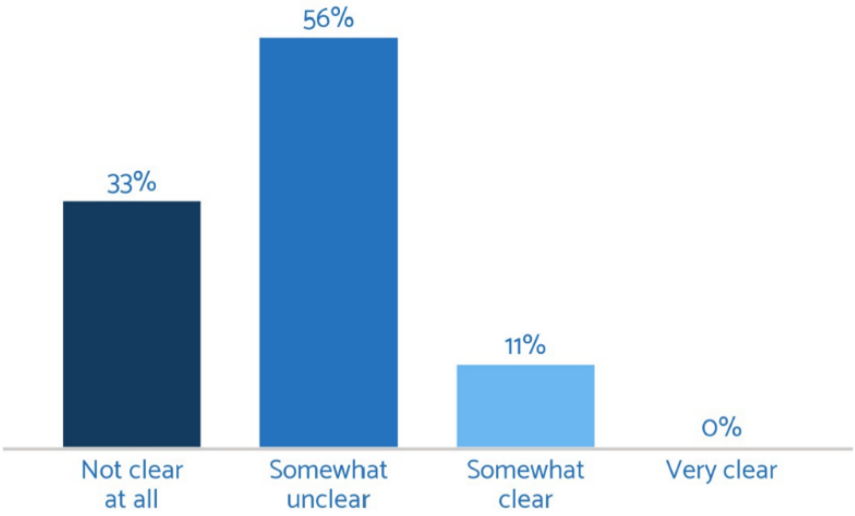
FIGURE 60: ASSESSED MATURITY OF AUSTRALIA'S POLICY AND LEGAL FRAMEWORK



38% of consulted stakeholders perceived the Australian policy and legal framework regarding space cybersecurity as not mature at all, and 63% considered it as somewhat mature. This assessment confirms the gap analysis presented above, but the reasons behind these results may be consistent with two explanations:

- the policy and legal framework is considered as widely immature because it is not adapted to the actual threats, which would stress the need for dedicated policies and legislations;
- the policy and legal framework is rather adapted but consulted stakeholders are not necessarily aware of it or do not know how to implement it, which would stress the need for awareness raising campaigns and training measures.

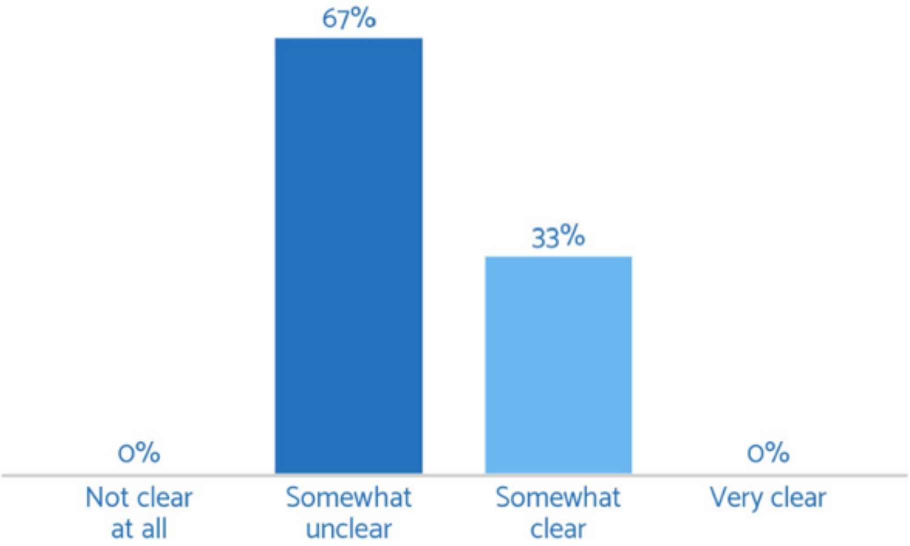
FIGURE 61: CLARITY OF THE POLICY AND REGULATORY FRAMEWORK OF AUSTRALIA'S SPACE SECTOR FOR INDUSTRIAL ORGANISATIONS



Australia does not have dedicated space cybersecurity laws and policies as demonstrated in the gap analysis above. Whereas some of its laws are applicable in case of cyberattacks, 56% of workshop participants considered that the policy and regulatory framework remains rather unclear. 33% of them considered it not clear at all and only 11% of them considered it as somewhat clear.

These results do not necessarily mean that the framework is not adapted, but that implementation in the space sector is rather complex and specific and needs assistance from government organisations. This partly because space systems are increasingly digitalised and subject to the same cyber threats as traditional computers, which prompts operators to adopt traditional cybersecurity measures. However, the hostile nature of the orbital environment and the distance from Earth make many traditional cybersecurity solutions inadequate.

FIGURE 62: CLARITY AND FITNESS OF OFFICIAL PROCEDURES TO SPACE SECTOR NEEDS

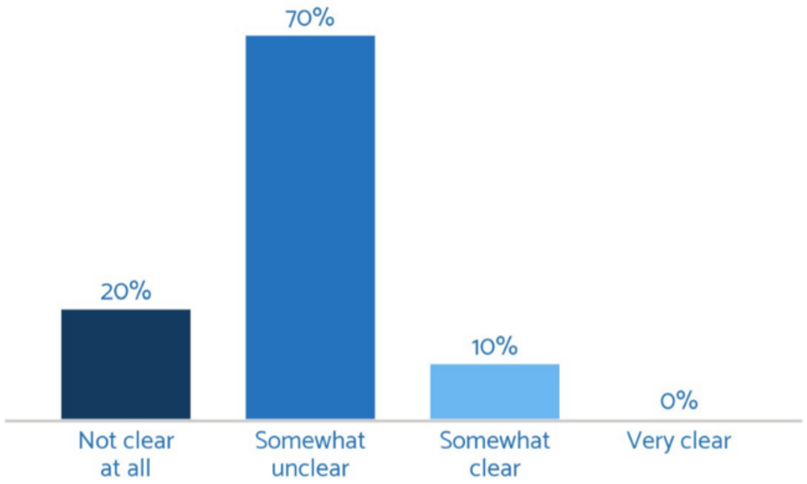


The assessment above is further reinforced by the perception of clarity and fitness of official procedure to the space sector. 67% of workshop participants considered them somewhat unclear. 33% of them considered official procedures somewhat clear. Clarity may be improved through awareness raising and support to industry in policy implementation. Fitness may be improved through cyber exercises, simulation exercises, and space cybersecurity incident response plans.

A specific legal tool where more procedural clarity was reportedly needed is the Security of Critical Infrastructure Act 2018, with several consulted stakeholders viewing the Act as completely unclear. The most serious reported issue associated with the applicability of this legislation is to determine what assets are considered critical, and, therefore, subject to the Act directives. As discussed, assuming that all space systems and services would by default be critical assets is in fact inaccurate, as some of them may be critical and others may not. It would hence be crucial for the government to delineate a clear method to recognize and assess the criticality of a space asset as well as the extant obligations that responsible entities and direct interest holders would have to comply with. Towards this, the Risk Assessment Advisory for Critical Infrastructure Space Technology Sector compiled by the Cyber and Infrastructure Security Centre may be of some utility.[376]

[376] Cyber and Infrastructure and Security Centre. (2021). *Risk Assessment Advisory for Critical Infrastructure Space Technology Sector*. CISC. https://www.cisc.gov.au/critical-infrastructure-centre-subsite/Files/raa-space-technology.pdf

Figure 63: Clarity of the Governmental Sector's Roles, Responsibilities, and Accountability

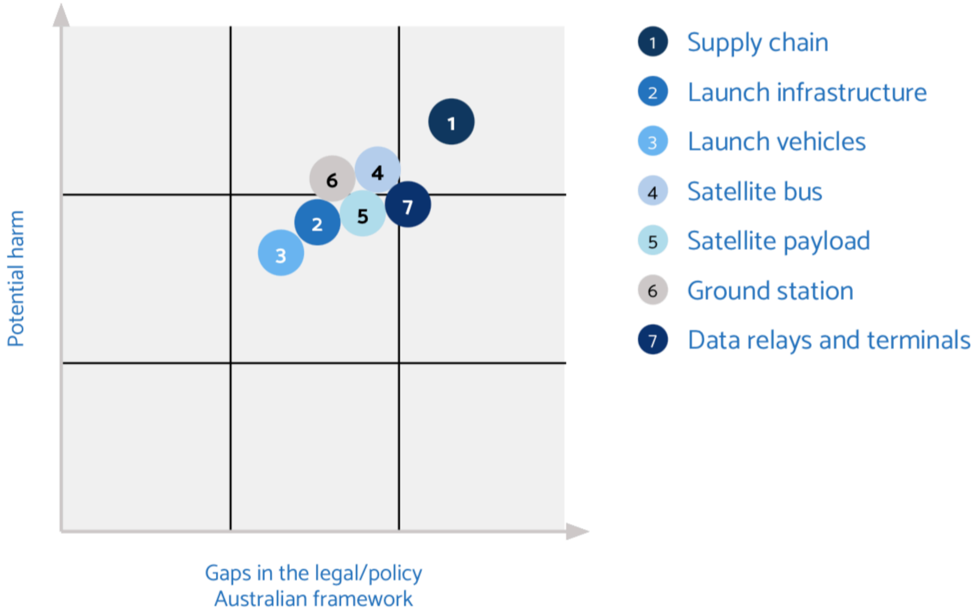


Besides issues related to the clarity and fitness of formal procedures, 70% of workshop participants considered that organisational aspects and responsibilities are somewhat unclear. This is rather normal as the Australian space program was recently restructured with the establishment of several agencies as well as some adaptation in the Department of Defence to face new threats and grey zone operations.

As an example, depending on the nature of the intercepted information, different departments are empowered to act and, the Telecommunication and Other Legislation Act 2017 provides power to the Secretary of Attorney-General's Department when there is a breach of information that possesses national security value, while the Security of Critical Infrastructure Act 2018 empowers Home affairs if a cyberattack has occurred, is occurring, or is deemed to be imminent and prejudices the social and economic stability or defence of Australia, as represented in case 4.

This lack of clarity would require more interactions between governmental organisations and the industry as well as more awareness raising campaigns in order to ensure that operators are aware of who to contact and where to report incidents.

Figure 64: Assessment of Policy/Legal Gaps vs Potential Harm

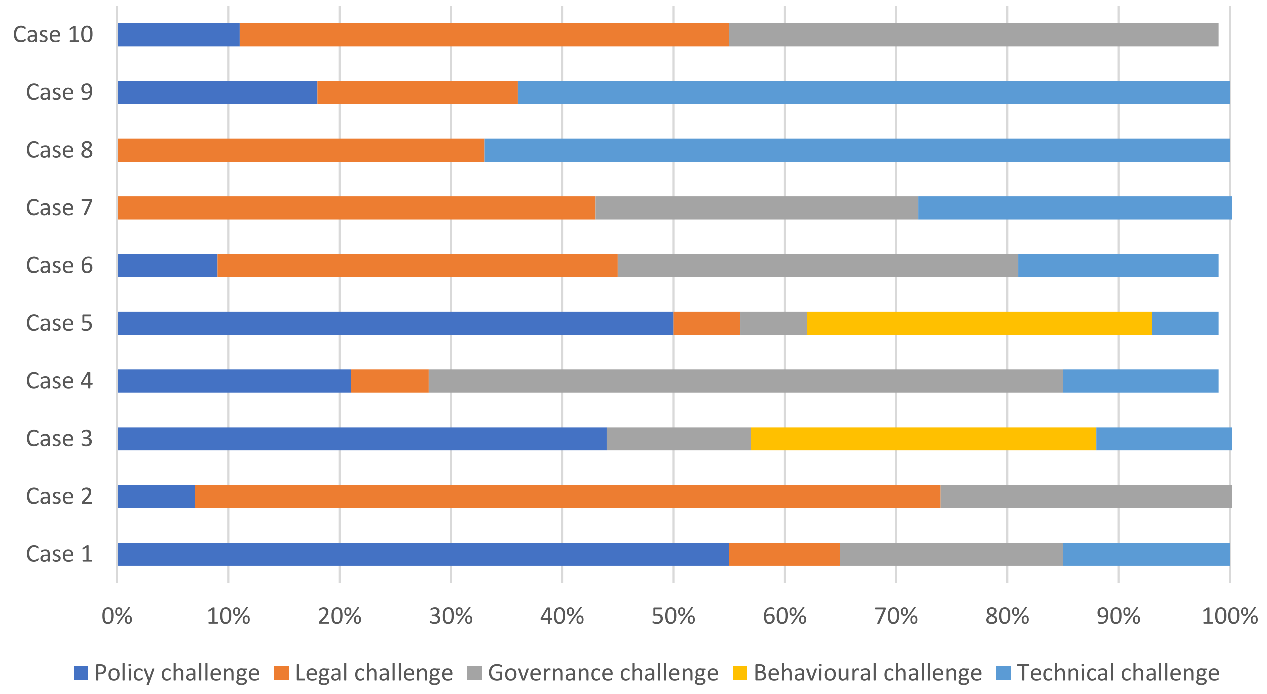


Regarding the maturity of the space cybersecurity maturity of Australian legal and policy framework, workshop participants ranked that the most immature laws and policies pertained to risks regarding the supply chain, data relays and terminals, and satellite buses, which are also the areas where Australia is the more at risk. The higher the risk in Australia, the higher the gaps seem to be. This stresses the need to have better policies and awareness measures for supply chain issues in particular.

Moreover, workshop participants also perceived significant gaps and potential harm regarding cyber threats on the launch infrastructure. The result denotes coherence with the fact that Australia does not yet have a strong upstream segment (manufacturing of spacecraft and launch vehicles) and greatly relies on outsourcing most systems, subsystems, and components. This was clearly reflected in use Cases 1 and 2, which addressed both potential software and hardware supply chain issues, demonstrating Australia's dependence on COTS.

The Table below provides an overview of the types of challenges that the Australian space infrastructure may face in case of an attack:

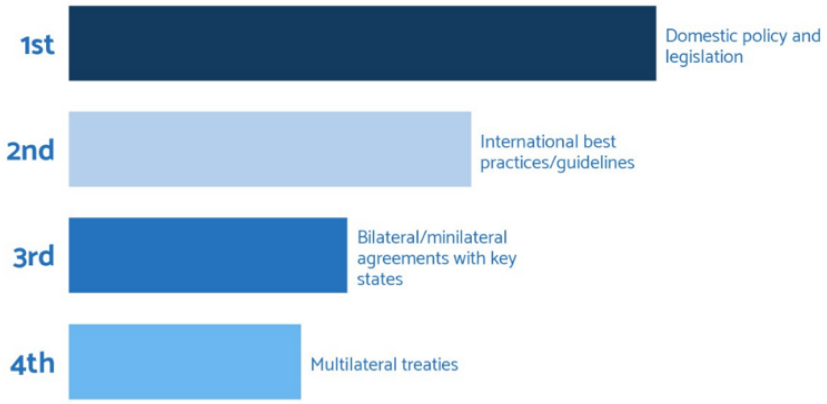
FIGURE 65: CHALLENGES TO CASE STUDIES PRESENTED DURING THE WORKSHOP



Behavioural challenges, which are associated to relevant human action, an incorrect human act that can lead to an undesired situation, despite the existence of proper technical, governance, legal and policy procedures, were the least perceived during the case analysis – only in Cases 3 and 5, in which an existing procedure was disregarded by internal actors, accidentally in Case 3 and purposely in Case 5.

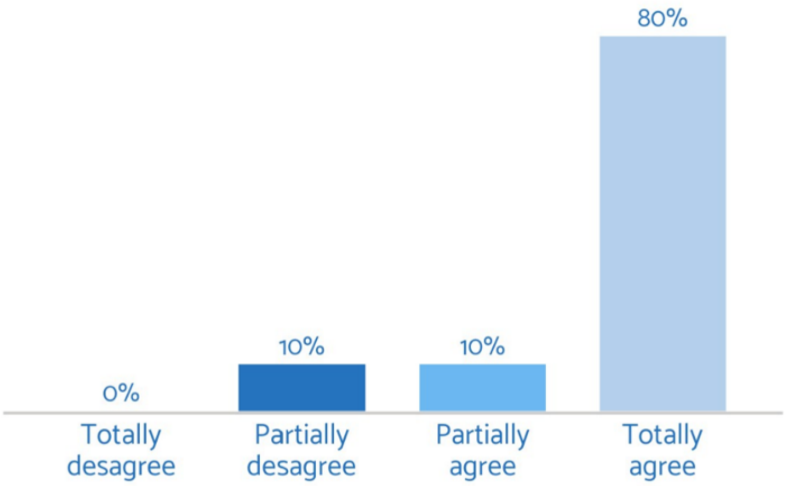
However, all the considered case present governance challenges, in addition to policy and legal ones. Organisational aspects and responsibilities remain indeed somewhat unclear. This lack of clarity would require more interactions between governmental organisations and the industry as well as more awareness raising campaigns to ensure that operators are aware of who to contact and where to report incidents.

FIGURE 66: PROPOSED SOLUTIONS TO ADDRESS GAPS IN AUSTRALIA'S POLICY AND LEGAL FRAMEWORK



Beyond the assessment of the maturity of Australia's space cybersecurity policies and laws, workshop participants were also consulted regarding solutions that they would see fit to fill these gaps. Based on the case studies presented, most of them considered that domestic policy and legislation was the best way to improve space cybersecurity, in particular regarding supply chain issues.

FIGURE 67: ASSESSED NEED TO CREATE NEW LEGAL AND POLICY MECHANISMS TO ADDRESS SPACE CYBER ISSUES



80% of workshop participants considered that there is a need to create new legal and policy mechanisms to address space cybersecurity issues. This proves the appetite for more regulations in this field in the space community, the cyber community, and the defence community, which composed most of the consulted stakeholders.

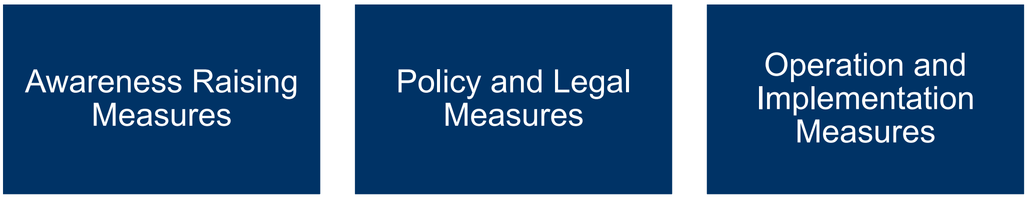
As result, based on the two hypotheses outlined, it can be assessed that the policy and legal framework is rather adapted, with many areas for improvement for supply chain cybersecurity and at the organisational level. However, consulted stakeholders in the policy and industrial communities are not necessarily aware of it or do not know how to implement it, which would stress the need for awareness raising campaigns and training measures. In addition, there is an appetite from the policy community to welcome policies and regulations addressing cybersecurity issues, which would demonstrate Australia's commitment to cybersecurity in general and to the cybersecurity of the space infrastructure.

4.2 Security Measures – Recommended Actions

Based on the policy and legal mapping, as well as the case studies, several recommendations have been outlined to improve the overall cybersecurity of the Australian space infrastructure.

Security measures have been segmented into three main typologies, as shown in Figure below.

FIGURE 68: TYPOLOGIES OF SECURITY MEASURES



Awareness Raising Measures

Policy and Legal Measures

Operation and Implementation Measures

4.2.1 Security Measures Informing Awareness Raising Measures

The need for awareness raising was clearly identified in the workshop. While some stakeholders had a clear of somewhat clear idea about the applicable policies and laws, others did not have a clear view of the applicable legislations and policies. The Table below provides an overview of consulted stakeholders' awareness of legislations applicable to the Use Cases:

TABLE 17: LACK OF AWARENESS OF APPLICABLE POLICY AND LEGAL FRAMEWORK TO USE CASES

Are Current Policies and Regulations Addressing this Type of Threat?	Percentage of Participants that 'Did Not Know'
Use Case 1	33%
Use Case 2	18%
Use Case 3	21%
Use Case 4	19%
Use Case 5	23%
Use Case 6	27%
Use Case 7	17%
Use Case 8	25%
Use Case 9	36%
Use Case 10	11%

Conduct Awareness Raising Campaigns for Space Cybersecurity

The workshops with both industrial and policy stakeholders demonstrated that the level of awareness regarding space cybersecurity was rather heterogenous and limited. In addition, relevant laws, policies, and incident response mechanisms are not clearly identified by space stakeholders at large. While the Australian

Cyber Security Centre is frequently monitoring cybersecurity news and informs Australian organisations to improve their security, this is not sufficient to mitigate the increasing level of cyber threats. For instance, in 2022, the ACSC reshared the U.S. CISA and FBI joint cybersecurity advisory regarding cyber threats on SATCOM user terminals amid the War in Ukraine and urged space companies to follow their guidelines.[377] While this is a good practice, which should be continued, it is not sufficient to raise awareness about space cybersecurity issues, which are rather complex. Awareness raising measures can include dedicated workshops and trainings, assistance to companies in the implementation of new cybersecurity legislation, held desks, official documentations.

Release a Space Cybersecurity Toolkit for the Space Industry

Australia's approach to the cybersecurity of space is characterized by fragmentation across multiple cybersecurity policies, legislations, and governmental branches that only tangentially address the space industry. This fragmentation on the cybersecurity of the space infrastructure in Australia can result in a lack of cohesion, which could introduce a significant risk of confusion and contradictory requirements potentially leading to regulatory overlaps and gaps that explains the fact that the workshops illustrated a low level of awareness for relevant laws and mechanisms in place in this blurry scenario.

As a result, 90% of the participants agreed that Australia needs to create new legal and policy mechanisms specifically to address cyber issues in space (Figure 68). Also, when confronted with options to address gaps in Australia’s policy and legal framework, the most selected option was to develop domestic policy and legislation (Figure 67).

Due to this, to increase the level of awareness and compliance with cybersecurity measures, Australia may take inspiration from the UK Space Agency by releasing a Space Cybersecurity Toolkit[378] for the Space Industry, which provides general information regarding potential cyber threats to space systems, how to conduct impact assessment as well as which general cybersecurity standards to adopt. More importantly, the Toolkit outlines relevant authorities and their mandate for reporting different types of cyber incident as well as an overview of some processes in case of an attack. This toolkit is a short document that does not outline detailed procedures but provides a clear outlook on how to report cyberattacks and to which organisations, which was considered as a main area of confusion by consulted stakeholders. This type of informative documentation can be used by start-ups, established industries, universities, and government stakeholders to increase their awareness, adopt good practices and responsible behaviours. This toolkit can also be used to base the cybersecurity strategy required by the Space (Launches and Returns) Act, that is currently based on two cybersecurity implementation documents that are not space specific.

Provide Space Cybersecurity Training for Professionals and Students

As demonstrated in Use Case 1, Australian universities are deeply involved in the development of Australia’s space program; and cyberattacks on education and demonstration satellites developed by students can lead to ripple effects and create major issues. There is a need to provide space cybersecurity training for both students and professionals to ensure capacity building in Australian institutions and industries. This may take different forms at different stages:

- Before entering the workforce:

[377] Australian Cyber Security Centre. (2022). *Australian Organisations Should Urgently Adopt an Enhanced Cyber Security Posture*. Commonwealth of Australia. https://www.cyber.gov.au/about-us/advisories/2022-02-australian-organisations-should-urgently-adopt-enhanced-cyber-security-posture

[378] United Kingdom Space Agency. (2020). *Cyber Security Toolkit (Version 2).* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/885869/Space_cyber_toolkit_final_v4.pdf

- Academic program: there is a need to create academic programs which integrate space cybersecurity courses to better understand space cyber threats and eventually foster interactions and research between the space and cyber community. In addition, there is a need to integrate cybersecurity in space engineering courses and projects to ensure that new talents have the right skillsets and automatism when they enter the workforce.
- Academic activities: activities and projects related to space cybersecurity may also be conducted as part of the Cyber Security Skills Partnership Innovation Fund, which funds innovative projects carried out by industry and education providers to grow a skilled workforce for cybersecurity.[379]
- Career choice and orientation: the Australian Space Discovery Centre seems to be involved in raising awareness about the types of careers and jobs that exist in the Australian space sector, therefore there would be merit in involving ASA, CyberOps, and ACSC in these activities.[380]

- In the workforce:
    - Continuous and tailored training for professionals: tailored training and workshop on space cybersecurity for different types of professions (e.g., engineers, regulators, strategy, human resources, IT, management, etc.) in the space sector would enable to raise awareness about specific cyber risks and ensure compliance with best practices. These activities would enable to ensure that non-tech professionals get to understand cybersecurity for their own activities. This is key to ensure that institutions such as ASA can gradually build-up in-house expertise instead of relying on external stakeholders.
    - Retaining talent and expertise: it is also key to ensure that the training is being retained and shared in the organisation so that when individual workers switch job or retire, the know-how remains within the institution and is passed on to new generations.

Create a Recurring Space Cybersecurity Event in Australia

To further raise awareness about space cybersecurity in the Australian space sector and beyond, an annual conference dedicated to space cybersecurity would gather stakeholders from the space, cyber, and defence communities to regularly exchange ideas and better understand the topic from an interdisciplinary perspective. This aspect was underlined during the workshop, which also shows the willingness of both policy and industrial actors to better understand this topic.

In Europe, the topic of space cybersecurity used to be rather overlooked in the strategic debate as well as in policy documents, and there was no recurring major event or conference on this topic. However, the Swiss company CYSEC decided to establish the CYSAT conference in 2021 to "t*ogether the space and IT security communities to build a European ecosystem capable to respond to the current and future challenges faced by the European space industry*"[381] and provides speeches, panel discussions, hackathons, and technical demonstrations. While there are also other factors to consider, it partly contributed to awareness raising across the entire space sector and brought the issue to the highest level of space policy and decision making.

[379] Australian Government. (2023). *Funding to Deliver Innovating Projects to Improve the Quality or Availability of Cyber Security Professionals in Australia*. https://business.gov.au/grants-and-programs/cyber-security-skills-partnership-innovation-fund

[380] Australian Government. (n.d.) *Australian Space Discovery Centre, Cyber Security Specialist*. Australian Space Agency. https://www.industry.gov.au/australian-space-discovery-centre/pathways-career-space/cyber-security-specialist

[381] CYSAT. (2023) *About Us*. CYSEC. https://cysat.eu/

4.2.2 Security Measures Informing Policy and Legal Measures

Update the Space Act of 2018 to Enhance Cybersecurity

The Space (Launches and Returns) Act 2018 establishes a system for regulating space activities in Australia or by Australian nationals outside Australia. To improve the state of cybersecurity, compliance with cybersecurity best practices, and clarity of the legal framework for operators, there would be merit in integrating more specific cybersecurity obligations in the Space Act as well as to transpose aspects discussed within UNCOPUOS related to general space security. Since the cybersecurity strategy imposed to obtain some licenses is based on documents not specifically catered to the space environment, integrating cybersecurity obligations on an appropriate space cyber toolkit would also be key to face today's threats. The update may also refer to other legislations and measures such as the Security Legislation Amendment (Critical Infrastructure) Act to clarify the applicable rules for operators depending on the nature and purpose of their assets, clarifying the whole legal scenario, and avoiding space stakeholders to inadvertently adhere to inappropriate standards, resulting in unnecessary costs, reduced competitiveness, and inadequate attention to security issues specific to space activities.

Streamline Incident Reporting Processes

Consulted stakeholders have mainly outline one confusing element regardless of their background: the incident reporting system. As many changes occur in the past few years in Australia, several new organisations were created (e.g., ASA) and others changed status (e.g., ASD). Therefore, it is not clear for operators when, how, and to which organisations they must report an attack based on the type of attack, the type of system targeted, the type of consequences, and the potential type of attacker. There would be merit in raising awareness about it but also in streamlining such processes to avoid confusion, ensure smooth coordination with authorities for incident response and attribution, as well as potential retaliation, which remains the sole domain of governments.

Develop Bilateral and Multilateral Agreements for Managing Cyberattacks on Space Infrastructure

Use Case 6 demonstrated that the reliance on foreign systems and services means that national policy and legal mechanisms are often inadequate in the event of a cyberattack. To respond to an attack and its direct or indirect consequences, it may have merit to increase bilateral and multilateral agreements in the field of space cybersecurity or automatically include clear incident response mechanisms, alternatives, and processes in case of outage or unavailability of a system or service to better coordinate with allies in case of an attack and avoid panic or risky behaviours from operators.

Adapt Procurement Practices

The workshop with industrial stakeholders demonstrated that the supply chain was the part of the attack surface that was the most likely to be targeted on the Australian space infrastructure. Attacks on the smallest and insignificant components can have disastrous consequences and ripples effects on the Australian space infrastructure as demonstrated in Use Case 1 and 2. As a result, procurement practices for Defence, industries, and start-ups should be strengthen.

As demonstrated in Use Case 1, many measures and best practices exist in Australian public documents but are not legally-binding and compulsory for operators. Therefore, making some of the supply chain security controls of the Information Security Manual mandatory would likely help operators better protect their supply chain. As supply chain risks are the most important, compliance may then be measured by a general audit of the Australian National Audit Office or another institution.

4.2.3 Security Measures Informing Operational and Implementation Measures

The workshops and consultations demonstrated that solutions are often political and legal to ensure the protection of the space infrastructure, however, many cases and issues remain technical and behavioural. To complement the policy and awareness raising measures, protecting space systems against cyber threats also calls for operational measures that can enable to better understand the threats, have a better prospective and anticipatory look at adversaries, and ensure coordination between actors in order not to duplicate efforts and wisely use public resources. Some of the measures described below may prove helpful for both public institutions and the industry:

Have a Clear and Active Information Sharing and Analysis Centre (ISAC) or Process for Space Cyber Threats

To improve the state of space cybersecurity in Australia, it is essential to ensure information sharing regarding cyber threats on space systems, sending alerts regarding current threats, conducting cyber intelligence, and gathering news about cyber events as well as resources to support response and mitigation. In Australia, organisations such as CyberOps have joined the U.S.-based organisation Space ISAC, which “serves to facilitate collaboration across the global space industry to enhance our ability to prepare for and respond to vulnerabilities, incidents, and threats; to disseminate timely and actionable information among member entities; and to serve as the primary communications channel for the sector with respect to this information”.[382] In addition, many initiatives in this realm have been kick-started in the past few years in Australia, which is a very positive sign and indicates the appetite to create a dedicated and integrated governance framework for space cybersecurity issues.

However, it seems that several organisations are being set up, which may be confusing for operators and may unnecessarily duplicate efforts. Several public or private organisations were established such as (1) TISN, which established sector groups, including a Space Sector Group, to enable operators to share information on threats and vulnerabilities. Nevertheless, despite appearing as an excellent tool to enhance the awareness of the space sector regarding cyber threats, it does not seem that TISN and the Space Sector Group are active.[383] Additionally, (2) CI-ISAC Australia is a not-for-profit organisation set up in Queensland to share critical cyber threat intelligence for critical infrastructures in line with Australia’s cybersecurity strategy and critical infrastructure’s legislation. Yet, it is not clear how space cybersecurity and the space sector is integrated into CI-ISAC.[384] Moreover, (3) CERT Australia[385] and (4) AustCERT can also facilitate threat information sharing and monitoring, but it is not clear whether space cybersecurity is covered in these two organisations. There is also the Australian Signals Directorate's Australian Cyber Security Partnership Program, aimed at drawing on collective understanding, experience, skills and capability to lift cyber resilience across the Australian economy,[386] however, the program is not tailored to the space sector and its unique technical and environmental singularities. Therefore, there would be merit in clarifying the governance, avoid duplications, and have a transparent active information sharing and analysis centre or processes for such activities in Australia.

[382] Space Information Sharing and Analysis Center. (2023). *About Space ISAC*. https://s-isac.org/about-us/

[383] Cyber and Infrastructure Security Centre. (2023). *TISN Sectors*. Commonwealth of Australia. https://www.cisc.gov.au/engagement/trusted-information-sharing-network/tisn-sectors

[384] CI-ISAC. (2023). *Cyber Threat Intelligence Sharing*. https://ci-isac.com.au/about-sharing.html

[385] Australian Cyber Security Centre. (2023). *Glossary, CERT Australia*. Commonwealth of Australia. https://www.cyber.gov.au/learn-basics/view-resources/glossary

[386] Australian Signals Directorate. (2023). *Australian Signals Directorate’s Cyber Security Partnership Program*. https://www.cyber.gov.au/resources-business-and-government/partner-hub/asd-cyber-security-partnership-program

Further Understanding the Reliance on Space Applications and Services

Use Cases 6 and 9 demonstrated that there is a pervasive reliance on space systems, which is not always understood by end-users and governments. While the reliance is acknowledged, the socio-economic costs of the unavailability of space-based applications and services is not well-known for specific regions and economic sectors. There would be merit in further researching the consequences of cyberattacks on space applications and services used by Australian users. It may take the form of studies or consultations between the space industry, the policy community, the space community, and the cyber community, which are rarely interacting with one another.

Further Developing Domestic Space Systems and Ensuring Redundancy and Substitution

Use Cases 6 and 9 illustrated that reliance on foreign space systems may have cyber-related consequences, which also call for a capability response. Australia should better include redundancy, which is the capacity to immediately compensate for the loss or unavailability of some functionality or component in case of an attack through the duplication of components on a satellite or the integration of various components that can perform similar function. Australia should also better include substitution, which is the capacity to replace a non-functioning system by a system of a different nature but providing similar capabilities through the ability to temporarily replace an EO satellite with a drone, aircraft, or HAPS, or to have interoperability between various GNSS providers.

Make Cybersecurity Tests Compulsory Before Launching a Satellite

Use Cases 1 and Case 4 demonstrated that satellites can be crippled with vulnerabilities and that launching or operating a satellite or space service without running a cybersecurity test can have a significant negative impact. Hardware tests are always conducted to ensure that the system is operational and can be safely launched. However, it is not always the case for software components. Therefore, it is crucial that operators (industrial and institutional) also make cyber tests and run cyber vulnerability scans on their systems prior to operating a satellite. Once the satellite is in orbit, the system cannot be physically accessed to be repaired and some cyber vulnerabilities cannot always be patched remotely. To ensure efficiency and avoid damaging the satellite, tests can be done through virtual simulators or digital twins. Some initial efforts are conducted in this regard in Australia with the development of a space cyber simulator.

Encouraging the Space Industry to Establish Bug Bounty Programs

As demonstrated in Use Case 4, cyber threats on space systems are increasing and satellites can contain vulnerabilities, which are unknown but may be exploited by malicious actors. While no legislation or policy can protect against this type of threats, it should be encouraged that Australian organisation establish Bug Bounty Programs and work with white hat hackers that may have access to their hardware or software to look for unknown vulnerabilities and find potential patches before they are exploited. Ethical hackers may be financially rewarded in exchange. This type of program has been widely adopted in other sectors such as banking to secure systems against Zero Days vulnerabilities.

In the space segment, bug bounty programs may seem dangerous and counterproductive since trying to conduct attacks and exploit vulnerabilities on satellites currently in orbit may lead to unpredicting ripple effects on the systems, disable functions without being able to repair or restore, or even lose control of the satellite, which becomes a debris. However, progress in AI and data processing now enable to create digital twins of satellites, which means it is possible to create exact replicas of space systems, including their networks, points of connection, vulnerabilities, and flaws, so that ethical hackers can conduct penetration testing and check the system for vulnerabilities in total safety.

Organise Cyber Exercises and War Gaming Scenarios to Train Space Operators to Better React to Cyber Incidents

The digitisation of space systems makes them more vulnerable to traditional cyber threats, which usually prompts to adopt traditional cybersecurity measures; but the unique nature of the space environment often renders traditional cybersecurity inadequate.[387] National and international recommendations often include many measures that must be adapted to the nature of the space missions and the technology on-board.[388]

To increase the adoption and compliance of cybersecurity best practices, cyber exercises can be organised to ensure that all operators know and understand processes and mechanisms in place. Exercises can be used to identify gaps and improve incident response. Additionally, war gaming scenarios can be organised at all management levels (e.g., operators, executives, policymakers, industry, defence, universities, etc.) to have an interdisciplinary and integrated prospective look on cyber threats against space systems, assess how planning and official postures (e.g., cyber diplomacy, offensive or defensive actions, attribution capabilities, institutional coordination, applicability of international law to cyberattack on space systems, etc.) apply in various cases and how to react to adversaries' behaviours. Australia has initiated efforts in this realm in the field of Space Domain Awareness (SDA) to create or/and test cyber response plans and introduce cyber issues to SDA professionals, which should be extended to the Australian space sector at large.

[387] Pavur, J., & Martinovic, I. (2022). *Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight*. Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac008. https://academic.oup.com/cybersecurity/article/8/1/tyac008/6611670#406985581

[388] Targett, E. (2022). *U.S. agencies urge 'Independent Encryption' for Satellite Communications across satellite coms. It's not that easy.* The Stack. https://thestack.technology/satellite-communications-encryption-cisa-satcom-cybersecurity/

Bibliography

Aerospace Corporation. (2022). *Space Attack Research & Tactic Analysis (SPARTA).* https://sparta.aerospace.org/

Aliberti, M., et al. (2020). *Emerging Spacefaring Nations*. European Space Policy Institute.

Australian Academy of Science. (2021). *Australia in Space: a Decadal Plan for Australian Space Science 2021-2030*

Australian Cyber Security Centre. (2022). *Australian Organisations Should Urgently Adopt an Enhanced Cyber Security Posture.* Commonwealth of Australia. https://www.cyber.gov.au/about-us/advisories/2022-02-australian-organisations-should-urgently-adopt-enhanced-cyber-security-posture

Australian Cyber Security Centre. (2022). *Essential Eight Maturity Model*. Commonwealth of Australia. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model

Australian Cyber Security Centre. (2023). *Cyber Security Guidelines*. Commonwealth of Australia. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines

Australian Cyber Security Centre. (2023). Glossary, CERT Australia. Commonwealth of Australia. https://www.cyber.gov.au/learn-basics/view-resources/glossary

Australian Cyber Security Centre. (2023). *Glossary, Cyber Attack*. Commonwealth of Australia. https://www.cyber.gov.au/learn-basics/view-resources/glossary

Australian Cyber Security Centre. (2023). *Information Security Manual*. Commonwealth of Australia. p.17. https://www.cyber.gov.au/sites/default/files/2023-09/Information%20Security%20Manual%20%28September%202023%29.pdf

Australian Cyber Security Centre. (n.d.) *Critical Infrastructure Uplift Program (CI-up).* https://www.cyber.gov.au/acsc/view-all-content/programs/critical-infrastructure-uplift-program-ciup

Australian Cyber Security Centre. (n.d.) *Report Cyber*. https://www.cyber.gov.au/acsc/report

Australian Government. (2010). *Australian Information Commissioner Act 2010, No.52.*

Australian Government. (2017). *Strategies to Mitigate Cyber Security Incidents.* https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/strategies-mitigate-cyber-security-incidents/strategies-mitigate-cyber-security-incidents

Australian Government. (2020). *Australian Signals Directorate Annual Report 2020-2021*. https://www.transparency.gov.au/annual-reports/australian-signals-directorate/reporting-year/2020-21-41

Australian Government. (2020). *Defence Science and Technology Group*. https://www.dst.defence.gov.au/discover-dst

Australian Government. (2021). *Australia's International Cyber and Critical Tech Engagement Strategy 2021.*

Australian Government. (2021). Critical Technology Principles. https://www.homeaffairs.gov.au/cyber-security-subsite/files/critical-technology-supply-chain-principles.pdf

Australian Government. (2022). *Cyber and Critical Technology Diplomacy | Australia's International Cyber and Critical Tech Engagement*. https://www.internationalcybertech.gov.au/our-work/cyber-and-critical-technology-diplomacy

Australian Government. (2022). *Multilateral Engagement | Australia's International Cyber and Critical Tech Engagement*. https://www.internationalcybertech.gov.au/about/multilateral-engagement

Australian Government. (2022). *Partnerships and Agreements, Australia's International Cyber and Critical Tech Engagement*. https://www.internationalcybertech.gov.au/about/partnerships-and-agreements

Australian Government. (2023). *Funding to Deliver Innovating Projects to Improve the Quality or Availability of Cyber Security Professionals in Australia*. https://business.gov.au/grants-and-programs/cyber-security-skills-partnership-innovation-fund

Australian Government. (n.d.) *Australian Space Discovery Centre, Cyber Security Specialist.* Australian Space Agency. https://www.industry.gov.au/australian-space-discovery-centre/pathways-career-space/cyber-security-specialist

Australian Journal of Emergency Management. (2012). *COMMUNIQUÉ: Standing Council on Police and Emergency Management*. Australian Journal of Emergency Management. 29 June 2012, Vol. 27, Issue 3

Australian Signals Directorate. (2022). *Information Security Manual*.

Australian Signals Directorate. (2023). *Australian Signals Directorate's Cyber Security Partnership Program*. https://www.cyber.gov.au/resources-business-and-government/partner-hub/asd-cyber-security-partnership-program

Australian Signals Directorate. (n.d.) *Central Bureau formed*. Australian Government. https://www.asd.gov.au/75th-anniversary/timeline/173-1942-central-bureau-formed

Australian Signals Directorate. (n.d.) *Cyber Security*. Commonwealth of Australia. https://www.asd.gov.au/cyber-security

Australian Signals Directorate. (n.d.) *REDSPICE*. Commonwealth of Australia. https://www.asd.gov.au/about/redspice

Australian Space Agency. (2019). *Advancing Space: Australian Civil Space Strategy 2019-28*.

Australian Space Agency. (2022). *Launch Facility License Applications Guidelines*. Commonwealth of Australia. https://www.space.gov.au/sites/default/files/2023-11/launch_facility_licence_-_guidelines.pdf

Australian Space Agency. (2022). *Overseas Payload Permit Application Guidelines*. Commonwealth of Australia. https://www.space.gov.au/sites/default/files/2023-11/overseas_payload_permit_-_guidelines.pdf

Australian Space Agency. (2023). High Power Rocket Permit Application Guidelines. Commonwealth of Australia. https://www.space.gov.au/sites/default/files/2023-11/high-power-rocket-permit-application-guidelines.pdf

Bailey, B. (2019). *Defending Spacecraft in the Cyber Domain*. Aerospace Corporation.

Baram, G., & Wechsler, O. (2020). *Cyber Threats to Space Systems*. JAPCC. https://www.japcc.org/cyber-threats-to-space-systems/

Bardin, J. (2014). *Satellite Cyber Attack Search and Destroy*. Cyber Security and IT Infrastructure Protection. Elsevier.

Baylon, C. (2014). *Challenges at the Intersection of Cyber Security and Space Security*. Chatham House.

Bedi, R., et al. (2020). *Australian Space Outlook 2020*. Faircount Media Group, 13, p.13.

Becht, O., & Trompille, S. (2019). *Rapport d'information sur le secteur spatial de défense*. Assemblée Nationale.

Blount, P.J. (2017). *Satellites are Just Things on the Internet Of Things*. Air & Space Law v.42.

Boschetti, N., Gordon, N.G., Falco, G. (2022). *Space Cybersecurity Lessons Learned from The ViaSat Cyberattack*. AIAA Ascend 2022. https://arc.aiaa.org/doi/10.2514/6.2022-4380

Bradbury, M., Maple, C., Atmaca, U. I., & Cannizzaro, S. (2020). Identifying *Attack Surfaces in the Evolving Space Industry Using Reference Architectures*. IEEE Aerospace Conference. https://doi.org/10.1109/AERO47225.2020.9172785

Caudill, H. (2020). *Space Domain Awareness, Governance, and Security in Outer Space.* AMC Solutions. Webinar.

CI-ISAC. (2023). Cyber Threat Intelligence Sharing. https://ci-isac.com.au/about-sharing.html

Council of Europe. (2001). *Convention on Cybercrime.*

Council of Europe. (2003). *Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems*.

Council of Europe. (2022). *Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence.*

Cyber and Infrastructure and Security Centre. (2021). *Risk Assessment Advisory for Critical Infrastructure Space Technology Sector*. CISC. https://www.cisc.gov.au/critical-infrastructure-centre-subsite/Files/raa-space-technology.pdf

Cyber and Infrastructure Security Centre. (2023). *TISN Sectors*. Commonwealth of Australia. https://www.cisc.gov.au/engagement/trusted-information-sharing-network/tisn-sectors

CyberOps. (2023). *Australian Space Cyber Framework*. https://www.cyberops.com.au/space-cyber-framework

Cybersecurity & Infrastructure Security Agency. (2023). *Cybersecurity Performance Goals: Sector-Specific Goals*. https://www.cisa.gov/news-events/news/cybersecurity-performance-goals-sector-specific-goals

CYSAT. (2023) *About Us*. CYSEC. https://cysat.eu/

Davies, A., Lewis, J., Herrera-Flanigan, J., & Mulvenon, J. (2012). *ANZUS 2.0: Cybersecurity and Australia–US Relations*. Australian Strategic Policy Institute, Issue 46. https://www.aspi.org.au/report/special-report-issue-46-anzus-20-cybersecurity-and-australia-us-relations de Bruijn, H., & Janssen, M. (2017). *Building Cyber Security Awareness: The Need for Evidence-Based Framing Strategies*. Government Information Quarterly, Volume 34, Issue 1, p 1-7.

de Zwart, M., & Lisk, J. (2022). *Low Earth Orbit, Satellite Constellations and Regulation.* Flinders University.

Defence Science and Technology Group. (2016). *Cyber and Electronic Warfare Division, Strategic Plan 2016-2021*.

Defence Science and Technology Group. (2020). *Our Role*. Commonwealth of Australia. https://www.dst.defence.gov.au/discover-dst/our-role

Defence Science and Technology Group. (2022). *Cyber and Electronic Warfare Division.* Commonwealth of Australia. https://www.dst.defence.gov.au/divisions/cyber-and-electronic-warfare-division

Demidov, O., & Persi Paoli, G. (2020). *Supply Chain Security in the Cyber Age: Sector Trends, Current Threats and Multi-Stakeholder Responses*. United Nations Institute for Disarmament Research. https://unidir.org/wp-content/uploads/2023/05/Supply-Chain-Security-in-the-Cyber-Age-UNIDIR-Report.pdf

Department of Defence. (2016). *2016 Defence White Paper*. Commonwealth of Australia.

Department of Defence. (2020). *Defence Security Principles Framework*. https://www.defence.gov.au/sites/default/files/2020-12/DSPF-OFFICIAL.pdf

Department of Defence. (2020). *Defence Strategic Update.*

Department of Defence. (2020). *Force Structure Plan.*

Department of Defence. (2021). *Defence Space Strategy.*

Department of Foreign Affairs and Trade. (2017). *Australia's International Cyber Engagement Strategy*. Commonwealth of Australia.

Department of Home Affairs. (2013). *National Plan to Combat Cybercrime.*

Department of Home Affairs. (2015). *National Organised Crime Response Plan 2015-18.*

Department of Home Affairs. (2018). *The Assistance and Access Act 2018.* https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-encryption

Department of Home Affairs. (2020). *Australia's Cyber Security Strategy 2020.*

Department of Home Affairs. (2022). *National Organised Crime Response Plan 2022.*

Department of Home Affairs. (2022). *National Plan to Combat Cybercrime 2022.*

Department of Home Affairs. (2022). *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022.*

Department of Home Affairs. (2023). *Assistance and Access: A New Industry Assistance Framework.* Commonwealth of Australia. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/assistance-and-access-industry-assistance-framework

Department of Home Affairs. (2023). *Assistance and Access: Overview.* Commonwealth of Australia. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/assistance-and-access-overview

Department of Home Affairs. (2023) *Cyber Security*. Commonwealth of Australia. https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security

Department of Home Affairs. (2023). *Our Portfolio, National Security*. Commonwealth of Australia. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security

Department of Home Affairs. (n.d.) *Cybercrime and Identity Security*. Commonwealth of Australia. https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/cybercrime-identity-security

Department of Home Affairs. (n.d.) *Cyber Security Industry Advisory Committee*. Commonwealth of Australia. https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/industry-advisory-committee

Department of Home Affairs. (n.d.) *What is the Critical Infrastructure Centre?.* Commonwealth of Australia. https://www.homeaffairs.gov.au/nat-security/files/cic-factsheet-what-is-critical-infrastructure-centre.pdf

Department of Industry, Science, and Resources. (n.d.) *Promoting and protecting critical technologies.* https://www.industry.gov.au/science-technology-and-innovation/technology

Department of Infrastructure, Transport, Regional Development, Communications and the Arts. (2022). *eSafety Commissioner*. Commonwealth of Australia. https://www.infrastructure.gov.au/media-technology-communications/internet/online-safety/esafety-commissioner

Department of the Prime Minister and Cabinet. (2021). *Digital Economy Strategy 2030*. Commonwealth of Australia.

Directory. (2021). *Australian Cyber Security Centre*. Commonwealth of Australia. https://www.directory.gov.au/portfolios/defence/australian-cyber-security-centre

Directory. (2023). *Department of Defence*. Commonwealth of Australia. https://www.directory.gov.au/portfolios/defence/department-defence

Directory. (2022). *eSafety Commissioner*. Commonwealth of Australia. https://www.directory.gov.au/portfolios/infrastructure-transport-regional-development-and-communications/australian-communications-and-media-authority/esafety-commissioner

Directory. (2023). *National Cybercrime Working Group*. Commonwealth of Australia. https://www.directory.gov.au/portfolios/home-affairs/national-cybercrime-working-group

Defence Science and Technology Group. (2022). *Cyber and Electronic Warfare Division*. Commonwealth of Australia. https://www.dst.defence.gov.au/divisions/cyber-and-electronic-warfare-division

Douzet, F. (2014). *La géopolitique pour comprendre le cyberespace*. Hérodote.

Electronic Frontier Foundation. (n.d.) *Joint Civil Society Response to the Provisional Draft Text of the Second Additional Protocol to the Budapest Convention on Cyber Crime*. https://www.eff.org/document/eff-comments-additions-budapest-protocol-cybercrime

eSafety Commissioner. (n.d.) *Regulatory Schemes*. https://www.esafety.gov.au/about-us/who-we-are/regulatory-schemes

European Space Agency. (2023). *Space Techniques*. https://spaceshield.esa.int/techniques/space

Expert Reference Group for the Review. (2018). *Review of Australia´s Space Industry Capability*. Australian Space Agency. p.70-77.

Fabio, D. (2015). *GNSS, Interference Threats and Countermeasures*. Artech House.

Falco, G. (2018). *Job One For Space Force: Space Asset Cybersecurity*. Harvard.

Falco, G. (2018). *The Vacuum of Space Cyber Security*. Presented at the 2018 American Institute of Aeronautics and Astronautics SPACE and Astronautics Forum and Exposition. https://arc.aiaa.org/doi/abs/10.2514/6.2018-5275

Federal Register of Legislation. (1901). *Customs Act.* https://www.legislation.gov.au/Details/C2022C00061

Federal Register of Legislation. (1914). *Crimes Act.* https://www.legislation.gov.au/Details/C2022C00059

Federal Register of Legislation. (1979). *Telecommunications (Interception and Access) Act 1979.* https://www.legislation.gov.au/Details/C2021C00341

Federal Register of Legislation. (1982). *Freedom of Information Act 1982.* https://www.legislation.gov.au/Details/C2022C00056

Federal Register of Legislation. (1987). *Mutual Assistance in Criminal Matters Act 1987.* https://www.legislation.gov.au/Details/C2021C00426

Federal Register of Legislation. (1988). *Privacy Act.*

Federal Register of Legislation. (1995). *Criminal Code Act 1995.* https://www.legislation.gov.au/Details/C2022C00065

Federal Register of Legislation. (1997). *Telecommunications Act 1997.* https://www.legislation.gov.au/Details/C2019C00104

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

Federal Register of Legislation. (2001). *Intelligence Services Act 2001.* https://www.legislation.gov.au/Details/C2022C00014

Federal Register of Legislation. (2012). *Cybercrime Legislation Amendment Act 2012.* https://www.legislation.gov.au/Details/C2012A00120

Federal Register of Legislation. (2015). *Enhancing Online Safety for Children (Consequential Amendments) Act 2015.*

Federal Register of Legislation. (2017). *Enhancing Online Safety for Children Amendment Act 2017.*

Federal Register of Legislation. (2017). *Telecommunications and Other Legislation Amendment Act 2017.* https://www.legislation.gov.au/Details/C2018C00385

Federal Register of Legislation. (2018) *Security of Critical Infrastructure Act 2018.* www.legislation.gov.au/Details/C2018A00029

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

Federal Register of Legislation. (2021). *Online Safety Act 2021.*

Freeland, S. (2001). *There's a Satellite in My Backyard - Mir and the Convention on International Liability for Damage Caused by Space Objects.* University of New South Wales Law Journal, vol. 24, no. 2, p. 483. HeinOnline.

Fritz, J. (2013). *Satellite hacking: A guide for the perplexed*. Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies: Vol. 10: Iss. 1, Article 3.

Froehlich, A. (2018). *National Space Legislation, Studies in Space Policy,* vol 15. Springer, Cham.

Froehlich, A. (2021). *Outer Space and Cyber Space: Similarities, Interrelations and Legal Perspectives (Vol. 33).* Springer International Publishing AG, pg. 62-63.

Froehlich, A., & Seffinga, V. (2018). *National Space Legislation: A Comparative and Evaluative Analysis*. Studies in Space Policy, vol 15. Springer, Cham.

Gavrilović, A. (2021). *What’s New with Cybersecurity Negotiations? The UN GGE 2021 Report*. Diplo. www.diplomacy.edu/blog/whats-new-with-cybersecurity-negotiations-the-un-gge-2021-report/

Georgescu, A., Gheorghe, A.V., Piso, M., Katina, P.F. (2019). *Critical Space Infrastructures: Risk, Resilience and Complexity*. Springer.

Gibson, W. (1984). *Neuromancer*. Ace Books.

Gillette, A. (2021). *From Supply Chains to Spacecraft: Taking an Integrated Approach to Cybersecurity in Space*. Wilson Center. https://www.wilsoncenter.org/blog-post/supply-chains-spacecraft-taking-integrated-approach-cybersecurity-space

Gini, A. (2014). *Cyber crime – From Cyber Space to Outer Space*. Space Safety Magazine. http://www.spacesafetymagazine.com/aerospace-engineering/cyber-security/cyber-crime-cyber-space-outer-space

Haig, Z. (2015). *Electronic Warfare in Cyberspace*. Security and Defence Quarterly, 2,7, p.22-35.

Harrison, T., Johnson, K., Roberts, T.G., Young, M. (2020). *Space Threat Assessment 2020*. Center for Strategic and International Studies. https://www.csis.org/analysis/space-threat-assessment-2020

Harrison, T., Johnson, K., Young, M., & Wood, N. (2022). *Space Threat Assessment 2022*. Center for Strategic and International Studies. https://www.csis.org/analysis/space-threat-assessment-2022

Hathaway, O. A., Crootof, R., Levitz, P., & Nix, H. (2012). *The Law of Cyber-Attack*. California Law Review 100, no. 4, 817-886.

Housen-Couriel, D. (2016). *Cybersecurity threats to satellite communications: Towards a typology of state actor responses*. Acta Astronautica 128. https://www.researchgate.net/publication/305729153_Cybersecurity_threats_to_satellite_communications_Towards_a_typology_of_state_actor_responses

International Telecommunication Union. (1992). *Final Acts of the Additional Plenipotentiary Conference, Constitution and Convention of the International Telecommunication Union, Optional Protocol Resolutions Recommendation*.

International Telecommunication Union. (n.d.) *Digital Skills Toolkit*. https://academy.itu.int/itu-d/projects-activities/research-publications/digital-skills-toolkit

International Telecommunication Union. (n.d.) Constitution and Convention Collection. https://www.itu.int/en/history/Pages/ConstitutionAndConvention.aspx#

Jackson, M. (2014). *Millions of Routers Supplied by Broadband ISPs Vulnerable to TR-069 Hackers*. ISP Review. https://www.ispreview.co.uk/index.php/2014/08/routers-supplied-broadband-isps-vulnerable-tr-069-hackers.html

Karimi, N., & Gambrell, J. (2019). *Iran Acknowledges Rocket Explosion, Says Test Malfunctioned*. Military Times. https://www.militarytimes.com/news/pentagon-congress/2019/09/02/iran-acknowledges-rocket-explosion-says-test-malfunctioned/

Kempf, O. (2014). *Alliances et mésalliances dans le cyberespace*. Collection Cyberstratégie. Economica.

Levi, R. (2020). *Cybersecurity of Space Assets*. SGAC Webinar.

Limonier, K. (2018). *Ru.Net : Géopolitique Du Cyberespace Russophone*. Les Carnets de l'Observatoire. L'inventaire.

Livingstone, D., & Lewis, P. (2016). *Space, the Final Frontier for Cybersecurity?.* Research paper. Chatham House.

Manulis, M., et al. (2020). *Cybersecurity in New Space*. Springer.

Martinovic, I., & Pavur, J. (2019). *The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space.* 11th International Conference on Cyber Conflicts. NATO Cooperative Cyber Defence Centre of Excellence.

McGill, I., & Ye, C. (2019). *The Launches and Returns Act: one of the most significant updates to the Space Activities Act since its implementation*. Allens. 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/

Miller, J. (2013). *Supply Chain Attack Framework and Attack Patterns*. MITRE.

Moranta, S., et al. (2020). *Towards a European Approach to Space Traffic Management*. ESPI Report 71.

NATO Joint Air Power Competence Centre. (2020). *Cyber Threats to Space Systems*. https://www.japcc.org/essays/cyber-threats-to-space-systems/

Nevill, L. (2018). *Cyber Security Governance in Australia*. Centre for International Governance Innovation.

National Institute of Standards and Technology. (n.d.) *Glossary, Cyberspace*. Computer Security Resource Center. https://csrc.nist.gov/glossary/term/cyberspace

Oakley, J. G. (2020). *Cybersecurity for Space: Protecting the Final Frontier*. Apress L. P.

Office of the Australian Information Commissioner. (2019). *Data Breach Preparation and Response*. https://www.oaic.gov.au/__data/assets/pdf_file/0017/1691/data-breach-preparation-and-response.pdf

Office of the Australian Information Commissioner. (2019). *Part 1: Data Breaches and the Australian Privacy Act*. https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/part-1-data-breaches-and-the-australian-privacy-act

Office of the Australian Information Commissioner. (n.d.) *Australian Privacy Principles*. https://www.oaic.gov.au/privacy/australian-privacy-principles

Office of the Australian Information Commissioner. (n.d.) *The Privacy Act*. https://www.oaic.gov.au/privacy/the-privacy-act

Office of the Australian Information Commissioner. (n.d.) *What We Do*. https://www.oaic.gov.au/about-us/what-we-do

Optus Yes. (2013). *C1 Satellite Payload Information*. https://www.optus.com.au/content/dam/optus/documents/about-us/our-network/Optus_C1_Payload.pdf

Paganini, P. (2013). *Hacking Satellites… Look Up To The Sky*. Infosecinstitute.com. https://resources.infosecinstitute.com/hacking-satellite-look-up-to-the-sky/

Parliament of Australia. (2010). *Government Response – House of Representatives Standing Committee on Communications Report on the Inquiry into Cyber Crime – Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime*.

Parliament of Australia. (2014). *Enhancing Online Safety for Children Bill 2014*.

Parliament of Australia. (2016). *Privacy Amendment (Notifiable Data Breaches) Bill 2016*. https://www.aph.gov.au/parliamentary_business/bills_legislation/bd/bd1617a/17bd052#:~:text=The%20purpose%20of%20the%20Privacy,Government%20agencies%2C%20some%20private%20sector

Parliament of Australia. (2017). *Revised Explanatory Memorandum of the Telecommunications and Other Legislation Amendment Bill 2017*. https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/s1051_ems_37a7641a-7411-409c-82d9-1f5b945486c3/upload_pdf/644130.pdf;fileType=application%2Fpdf

Parliament of Australia. (2017). *Telecommunications and Other Legislation Amendment Bill 2017*. https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=s1051

Parliament of Australia. (2018). *Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*. https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/AmendmentsTOLAAct2018

Pasco, X. (2017). *Le Nouvel Âge Spatial, De La Guerre Froide Au New Space*. CNRS Editions.

Pavur, J. (2020). *Space for the IoT: Between the Race for Connectivity and Cybersecurity Concerns*. SGAC Webinar.

Pavur, J., & Martinovic, I. (2022). *Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight*. Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac008. https://academic.oup.com/cybersecurity/article/8/1/tyac008/6611670#406985581

Plotnek, J. (2022). *A Threat-Driven Resilience Assessment Framework and Security Ontology for Space Systems.* Thesis submitted to the University of South Australia for the degree of Doctor of Philosophy.

Plotnek, J. (2023). *Critical National Infrastructure Supply Chain Dependencies on Space Systems and Satellite Services in the West*.

Plotnek, J., & Slay, J. (2022). *Space Systems Security: A Definition and Knowledge Domain for the Contemporary Context*. Journal of Information Warfare. 21.3: 103-19.

Plotnek., J., & Slay, J. (2023). *COSMOS2: Contemporary Ontology for the Security Management of Space Systems*. International Journal of Critical Infrastructure Protection.

Poirier, C. (2021). *Interdependences Between Space and Cyberspace in a Context of Increasing Militarization and Emerging Weaponization of Outer Space—A French Perspective*. Springer.

Rajagopalan, R.P. (2019). *Electronic and Cyber Warfare in Outer Space*. Space Dossier 3. United Nations Institute for Disarmament Research.

Rives, A. (2019). *Sécurité Des Liaisons Satellites*. CEIS.

Robertson, J., & Riley, M. (2018). *The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies. Bloomberg*. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Ruben, S. (2014). *A Wake-Up Call for SATCOM Security*. IOActive. https://ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf

Sanger, S. & Broad, W. (2019). *U.S. Revives Secret Program To Sabotage Iranian Missiles And Rockets*. New York Times. https://www.nytimes.com/2019/02/13/us/politics/iran-missile-launch-failures.html

Shah, R. (2023). *Getting regulation right – Approaches to improving Australia's cybersecurity*. ASPI.

Shadbolt, L. (2021). *Satellite Cyberattacks and Security*. Technical Study. HDI. https://www.hdi-specialty.com/downloads/_Global/HDIS209_Satellite%20Cyberattack_whitepaper_V8_05JULY21.pdf

SmartSat. (2022). *Satellite Cyber Resilience Whitepaper.* SmartSat. Adelaide, Australia. https://smartsatcrc.lbcdn.io/uploads/Satellite-Cyber-Resilience-Whitepaper-FINAL.pdf

South Australian Space Industry Centre. (n.d.) *Ping Services*. https://sasic.sa.gov.au/industry/industry-directory/ping-services/

Space Information Sharing and Analysis Center. (2023). *About Space ISAC*. https://s-isac.org/about-us/

SpamTitan. (2017). *NSA Exploit Used in Cyberattacks on Hotel WiFi Networks*. https://www.spamtitan.com/blog/nsa-exploit-cyberattacks-on-hotel-wifi-networks/

Swinson, J., Bowe, K., & McKew, A. (2014) *Australia's Cybercrime Legislation*. King & Wood Mallesons. https://www.lexology.com/library/detail.aspx?g=4ab62fdd-f177-47eb-b02d-e327cf9833a9

Targett, E. (2022). *U.S. agencies urge 'Independent Encryption' for Satellite Communications across satellite coms. It's not that easy.* The Stack. https://thestack.technology/satellite-communications-encryption-cisa-satcom-cybersecurity/

The Economist. (2019). *Attacking Satellites is Increasingly Attractive—And Dangerous*. https://www.economist.com/briefing/2019/07/18/attacking-satellites-is-increasingly-attractive-and-dangerous

United Kingdom Space Agency. (2020). *Cyber Security Toolkit* (Version 2). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/885869/Space_cyber_toolkit_final_v4.pdf

Underwood, C., et al. (2001). *SNAP-1: A Low Cost Modular COTS-Based Nano-Satellite – Design, Construction, Launch and Early Operations Phase*. AIAA/USU Conference on Small Satellites. https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=1993&context=smallsat

United Nations. (2013). *Group of Governmental Experts 2013 Final Repo*rt. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf?OpenElement

United Nations. (2021). *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/075/86/PDF/N2107586.pdf?OpenElement

United Nations. (n.d.) *Group of Governmental Experts*. https://www.un.org/disarmament/group-of-governmental-experts/

United Nations Office for Outer Space Affairs. (2023). *Agreement Governing the Activities of States on the Moon and Other Celestial Bodies*. https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/intromoon-agreement.html

United Nations Office for Outer Space Affairs. (2023). *Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space*. https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introrescueagreement.html

United Nations Office for Outer Space Affairs. (2023). *Convention on International Liability for Damage Caused by Space Objects*. https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introliability-convention.html

United Nations Office for Outer Space Affairs. (2023). *Convention on Registration of Objects Launched into Outer Space.* https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introregistration-convention.html

United Nations Office for Outer Space Affairs. (2023). *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*. https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html

United Nations Office for Outer Space Affairs. (n.d.) *Committee on the Peaceful Uses of Outer Space: Membership Evolution*. https://www.unoosa.org/oosa/en/ourwork/copuos/members/evolution.html

Underwood, C., Richardson, G., & Savignol, J. (2001) *SNAP-1: A Low Cost Modular COTS-Based Nano-Satellite – Design, Construction, Launch and Early Operations Phase*. AIAA/USU Conference on Small Satellites. https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=1993&context=smallsat

Valeri, L. (2013). *Countering Threats in Space and Cyberspace: A proposed Combined Approach*. Chatham House, p.3.

Van der Watt, R., & Slay, J. (2021) *Modification of the Lockheed Martin Cyber Kill Chain (LMCKC) for cyber security breaches concerning Low Earth Orbit (LEO) Satellites*. Presented at the 16th International Conference on Cyber Warfare and Security.

Velkovsky, P., et al. (2019). *Satellite Jamming, A Technology Primer*. On the Radar. Center for Strategic and International Studies.

Von der Dunk, F. G. (2003). *The Registration Convention: Background and Historical Context, Space, Cyber, and Telecommunications*. Law Program Faculty Publications.

Weeden, B., & Samson, V. (2020). *Global Counterspace Capabilities: An Open Source Assessment*. Secure World Foundation.

West, J. (2019). *Space Security Index 2019*. Project Ploughshares.

Wheelahan, F., & Lee, K. (2020). Launching a space industry: an overview of Australia's renewed space regulations. https://www.corrs.com.au/insights/launching-a-space-industry-an-overview-of-australias-renewed-space-regulations

Wills, T. (2010). Cyber Crime: *The Net Is Closing in on You*. Bulletin (Law Society of South Australia) 32. no. 6:26.

Zarkan, L. (2020). *Space Domain Awareness, Governance and Security in Outer Space*. AMC Solutions. Webinar.

Zarkan Cesari, L. (2021). *What's in a Word? Notions of 'Security' and 'Safety' in the Space Context*. United Nations Institute for Disarmament Research.

Appendix: List of Acronyms

Appendix A: List of Acronyms

Acronym	Meaning
ACIC	Australian Criminal Intelligence Commission
ACMA	Australian Communications and Media Authority
ACORN	Australian Cybercrime Online Reporting Network
ACS	Access Control Service
ACSC	Australian Cyber Security Centre
ADF	Australian Defence Force
AFP	Australian Federal Police
AGD	Attorney-General Department
AI	Artificial Intelligence
APP	Australian Privacy Principles
APT	Advanced Persistent Threat
ARF	ASEAN Regional Forum
ASA	Australian Space Agency
ASAT	Anti-Satellite Weapon
ASD	Australian Signals Directorate
ASDC	Australian Space Discovery Centre
ASEAN	Association of Southeast Asian Nations
ASIO	Australian Security Intelligence Organisation
AWS	Amazon Web Services
BGAN	Broadband Global Area Network
C/CSP	Carriers and Carriage Service Providers
CAN	Controller Area Network Protocol
CBM	Confidence-Building Measures

CERT	Computer Emergency Response Team
CEWD	Cyber and Electronic Warfare Division
CIA	Central Intelligence Agency
CIAC	Critical Infrastructure Advisory Council
CIC	Critical Infrastructure Centre
CISA	Cybersecurity and Infrastructure Security Agency
CI-UP	Critical Infrastructure Uplift Program
COTS	Commercial Off The Shelf
CRC	Cooperative Research Centre
CSIS	Center for Strategic and International Studies
DDoS	Distributed Denial of Service
DISP	Defence Industry Security Program
DNS	Domain Name System
DoD	Department of Defence
DoS	Denial of Service
DSTG	Defence Science and Technology Group
DVB	Digital Video Broadcasting
EEE	Electrical, Electronic and Electro-mechanical
EO	Earth Observation
ESA	European Space Agency
ESPI	European Space Policy Institute
EU	European Union
FBI	Federal Bureau of Investigation
FOI	Freedom of Information
GEO	Geostationary Orbit
GEOINT	Geospatial Intelligence

GGE	Group of Governmental Experts
GLONASS	Global'naya Navigatsionnaya Sputnikovaya Sistema (Russian)
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GRE	Generic Routing Encapsulation
GRU	Russian Chief Intelligence Office
GSE	Generic Stream Encapsulation
HAPS	High-Altitude Pseudo-Satellite
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICCTES	International Cyber and Critical Technology Engagement Strategy
ICD	Interface Control Documents
ICES	International Cyber Engagement Strategy
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISO	International Organization for Standardization
IST	Information Security Manual
IT	Information Technology
ITU	International Telecommunications Union
JAPCC	Joint Air Power Competence Centre
JCSC	Joint Cyber Security Centres
LEO	Low Earth Orbit
M2M	Machine to Machine
MGMT	Management
MoU	Memorandum of Understanding

NATO	North Atlantic Treaty Organization
NCWG	National Cybercrime Working Group
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OAIC	Office of the Australian Information Commissioner
OEWG	Open-Ended Working Group
OST	Outer Space Treaty
OT	Operational Technology
PNT	Positioning, Navigation, and Timing
PoC	Points of Contact
PSPF	Protective Security Policy Framework
R&D	Research and Development
REDSPICE	Resilience, Effects, Defence, Space, Intelligence, Cyber, Enablers
RF	Radio Frequency
S&T	State and Territory
SATCOM	Satellite Communications
SCArch	Space Cyber Architecture
SCC	Space Coordination Committee
SCPEM	Standing Council on Police and Emergency Management
SDR	Software Defined Radios
SIAA	Space Industry Association of Australia
SME	Small-to-Medium Enterprise
SoNS	Systems of National Significance
SSA	Space Situational Awareness
SST	Space Surveillance and Tracking
STEM	Science, Technology, Engineering and Mathematics

SWF	Secure World Foundation
TCP/IP	Transmission Control Protocol/Internet Protocol
TIA	Telecommunications (Interception and Access)
TISN	Trusted Information Sharing Network
TSSR	Telecommunication Sector Security Reforms
TT&C	Telemetry, Tracking and Command
TTCM	Telemetry, Tracking; Commanding and Monitoring
UN	United Nations
UNCOPUOS	United Nations Committee on the Peaceful Uses of Outer Space
UNIDIR	United Nations Institute for Disarmament Research
UNOOSA	United Nations Office for Outer Space Affairs
VPN	Virtual Private Network
VSAT	Very Small Aperture Terminals

USER INFORMED **INDUSTRY** DRIVEN **RESEARCH** POWERED

SMARTSAT
COOPERATIVE RESEARCH CENTRE

Australia's Premier Space Research Centre

Australian Government
Department of Industry, Science and Resources

AusIndustry
Cooperative Research Centres Program

SmartSat CRC Head Office:
Lot Fourteen, Level 2, McEwin Building
North Terrace, Adelaide, SA

info@smartsatcrc.com
smartsatcrc.com