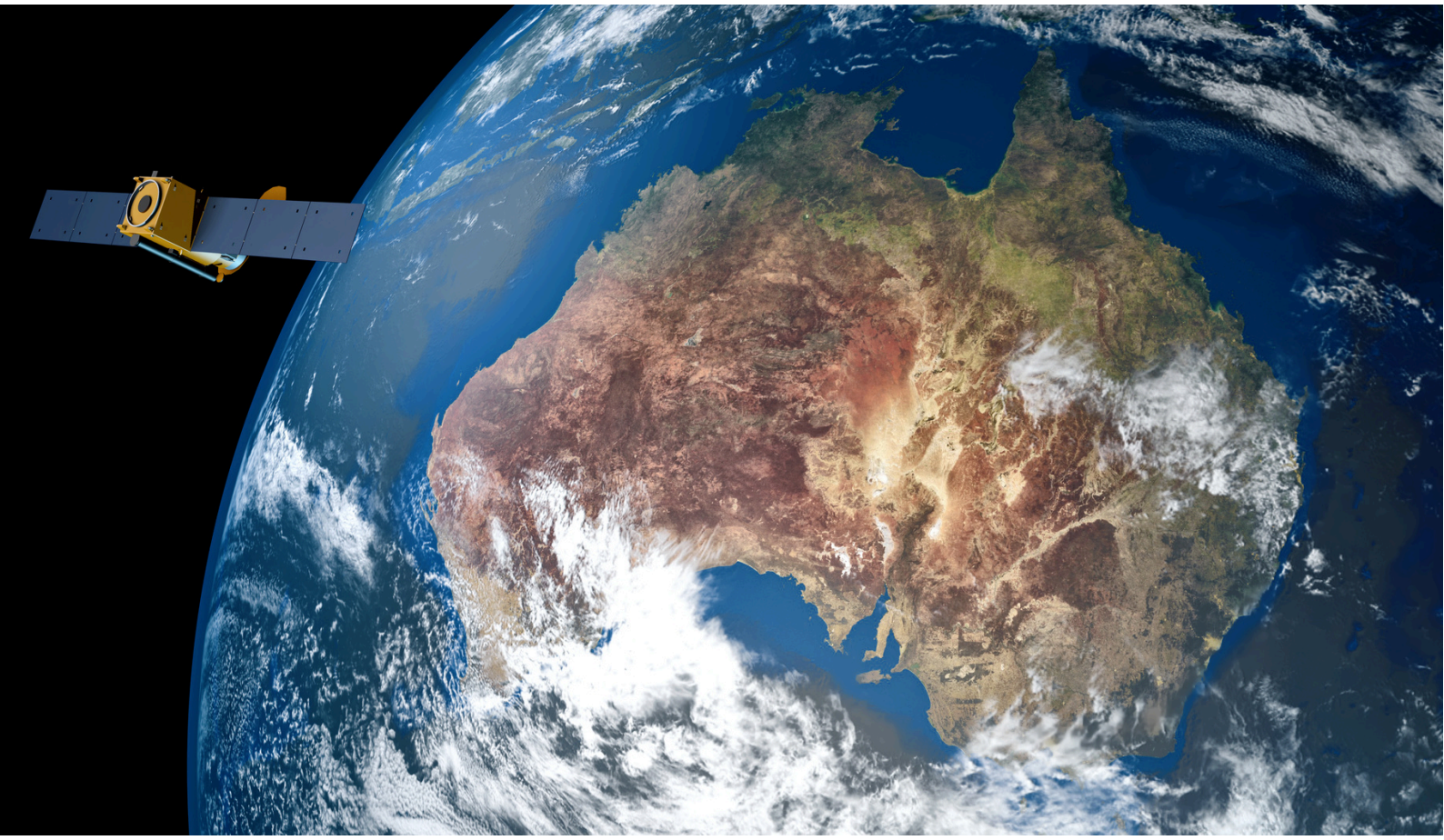
SECURING AUSTRALIA THROUGH SPACE: CYBER SECURITY MEASURES MATTER

VINICIUS GUEDES G. DE OLIVEIRA



ACSG Policy Paper Series
November 2024
www.spacegovcentre.org

ACSG
AUSTRALIAN CENTRE FOR SPACE GOVERNANCE

About the Author

Vinicius Guedes G. de Oliveira is a Researcher and PhD Candidate at Flinders University and a Global Fellow at the European Space Policy Institute.

About the Securing Australia Through Space Policy Papers Series

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

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

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

About the Australian Centre for Space Governance

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

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

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

Citation

Vinicius Guedes G. de Oliveira, ‘Securing Australia Through Space: Cyber Security Measures Matter’, Australian Centre for Space Governance, 2024.

SECURING AUSTRALIA THROUGH SPACE: CYBER SECURITY MEASURES MATTER

Vinicius Guedes G. de Oliveira

Summary

- As Australia is increasingly dependent on space services and applications, the country has a vulnerable space sector and therefore needs to incorporate stronger space cyber security measures.
- Cyberattacks are a key threat to space capabilities because they do not require substantial resources, are available to more actors, and can result in significant and, to a degree, controlled, damage. Additionally, they can provide plausible deniability and stealth for attackers.
- Australia has data protection laws, and cyber security regulations, toolkits and programs. It has also developed civil and defence space strategies and legislation focused on launch activities. Nevertheless, the intersection between cyber and space still requires further maturation and the development of specific tools to safeguard the Australian space infrastructure against cyberattacks.

Policy recommendations

- The Department of Home Affairs should accelerate the process of defining critical infrastructure assets for space technology under the *Security of Critical Infrastructure (SOCI) Act.* It then must assist Australian space companies (and space-related companies) to navigate the new cyber security obligations.
- The Department of Home Affairs and Department of Foreign Affairs and Trade should work together to develop a specific toolkit on space cyber security to clarify how the cyber security strategy applies to the *Space (Launches and Returns) Act*. Presently, the cyber security strategy relies on documents addressed to a broader cyber environment, not tailored to the space sector.
- The Department of Foreign Affairs and Trade should work to include the cyber security of space infrastructure as a priority in Australia's military and strategic alliances with significant space-faring nations, including through AUKUS. Australia could use these alliances to promote rules for the cyber security of space infrastructures and to consider mutual recognition of certifications and technology standards

When it comes to space threats, direct ascent Anti-Satellite (ASAT) capabilities have received most of the attention in media and pop culture, however, their use is unlikely in the current space environment owing to the debris they create. In contrast, cyberattacks do not usually receive much attention from the public, but are a clear and present threat. Although less exciting than a giant pointy missile, space technology is highly vulnerable to cyberattacks, and as space assets progressively incorporate advanced information and communications technologies, the potential entry points for cyberattacks are inevitably expected to multiply.[1] This is particularly relevant for nations such as Australia that do not possess a developed supply chain industry for the space segment and rely on external commercial off-the-shelf (COTS) components or foreign commercial providers. When not properly subjected to standardised testing for cyber resilience, other than tests undertaken by the manufacturer, these components can increase the number of possible entry points for cyberattacks in the space infrastructure.

States are increasingly dependent on space services and applications. Not only is a significant part of the economy directly underpinned by the space segment but most critical sectors such as water, energy, banking and transport also depend on satellite services. Moreover, space technologies influence most modern warfare dynamics and are one of the main variables taken into consideration within military strategies.[2] The loss of service in any of these sectors due to a cyberattack could destabilise Australia's economy on a large scale and have serious implications for national security. It is imperative, therefore, to develop better cyber security measures to safeguard the space sector.

Cost dynamics in cyberattacks as an attack vector

Cyberattacks constitute one of the most accessible means of attack on space services, available to a broad spectrum of actors, including non-state entities. This increased accessibility renders organised criminal networks, terrorist groups, militant organisations, competing commercial entities, political activists and individual hackers capable of disrupting or damaging space infrastructure through cyberattacks.

Illustratively, in 1999, Jonathan James, at the age of 15, successfully installed a backdoor in United States (US) military servers and gained access to the source code of the International Space Station.[3] This demonstrates that substantial resources are not needed for impactful cyberattacks on space infrastructure.

Similarly, a simulated cyberattack was designed by academics targeting space situational awareness data to trick satellites into performing manoeuvres. In the simulation, satellites would collide with debris resulting in total satellite inoperability. This projection, utilising widely available and inexpensive technology, was simulated against over 100 major communications satellites and demonstrated a success rate that exceeded 90% against the targeted entities.[4]

Moreover, from a technological standpoint, engaging in offensive cyber activities is more cost-effective than defensive countermeasures.[5] While defenders have to shield several potential entry points in

the system, attackers only have to find one vulnerability to cause damage. This dynamic introduces the potential for attackers with limited financial means to compromise the space infrastructure of technologically advanced nations.

Cyberattacks as a responsible instrument of warfare

Nonetheless, cyberattacks might be considered a responsible form of targeting space assets. Space is recognised as an operational military domain by Australia and many other nations.[6] Efforts towards achieving space control and security invariably necessitate the integration of both offensive and defensive operations to safeguard freedom of action in space and protect national and allied space systems, as stated in the *Australian Defence Space Command: Space Power eManual*.[7]

However, these offensive and defensive operations must take into consideration the Australian commitment to responsible behaviour in space as an integral aspect of pursuing space control. This is imperative not only for Australia but for any responsible actor in space.

Responsible counterspace capabilities are those that aim to ensure unhindered access to space while also adhering to international security commitments, such as generating predictable effects, mitigating space debris and maintaining the integrity of the space environment.[8] Direct-ascent ASAT kinetic weapons are an example of a counterspace capability contrary to this definition.

Presently, the US, Russia, China and India are the only nations that have empirically demonstrated kinetic ASAT capabilities, each time generating exorbitant amounts of debris that threaten the safe operations of space systems, and some of which remain in orbit for many months or years. Meanwhile, a growing number of nations, including Australia, have unilaterally committed to refrain from testing ASAT capabilities, as it has been recognised that the deliberate creation of debris is irresponsible, making its use more unlikely.

As cyberattacks can be used in a way that do not generate space debris or damage to other space objects, they could offer a more responsible and controlled approach to space operations. One that would align with the desired outcomes of pursuing space control while maintaining the integrity of the space environment.

Stealth and plausible deniability in cyberattacks

An inherent advantage of cyberattacks lies in their capacity to operate stealthily and provide plausible deniability, characteristics not easily achievable through alternative attack vectors. Other forms of attack, including kinetic attacks, are easier to attribute to an actor, which introduces high diplomatic costs that are difficult to navigate within the complex and ever-changing geopolitical landscape.

Cyberattacks offer a concealed alternative that evades immediate detection, owing to the diverse forms and entry points. Cyberattacks are also capable of generating a vast range of effects, such as loss, interception or modification of data, alteration of satellite's orbit, denial of access or service, unauthorised spacecraft control, alteration of power components functions, or even loss of mission. Additionally, the opportunity for the attacker

to concurrently target multiple missions exacerbates the difficulty of attribution, diminishing defensive reaction time.

One factor of added complexity is that, because cyberattacks tend to have temporary, reversible impacts on the space systems that are targeted, it is possible to maintain a cyberattack in the so-called greyzone. In other words, it is not usually the case that these kinds of attacks reach the threshold of use of force, and can therefore be undertaken during times of tension, when there is no open conflict. This means cyber activities may be a defensive tool available to Australia.

At the same time, however, there must be awareness across government and in the private space sector that cyber interference with space capabilities upon which our nation depends are highly likely in times of peace, tension as well as conflict.

Unclear legal and governance frameworks

Cyberattacks operate under an extra layer of furtiveness; the existing international legal and policy frameworks are unclear, making it difficult to identify an appropriate response to an attack.

Both space and cyberspace are conceptualised by many as global commons, denoting their collective ownership by humanity and their exemption from national appropriation. This renders the regulation of cyber activities in the context of the space environment a particularly intricate endeavour, involving the convergence of two global commons.

In the case of space, Articles I and II of the *Outer Space Treaty (OST)* render space beyond national jurisdiction and the province of all.[9] Similarly, the *Declaration of Principles* adopted by the United Nations (UN) mandated World Summit on the Information Society articulates the notion of cyberspace as a global common.[10] This perspective is further echoed in the 2015 report by the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. The report places emphasis on the peaceful use of Information and communication technologies for the common good of [hu]mankind, akin to the principles outlined in the OST.[11]

The shared attribute of common ownership in both space and cyberspace poses a regulatory challenge, particularly as global commons operate beyond national jurisdictions. Consequently, reliance solely on domestic law proves inadequate for establishing a secure regulatory framework for global commons, necessitating broader international agreements among multiple stakeholders.

At the international level, cyber security is subject to two competing frameworks, namely one proposed by a Western bloc, led by the US and Europe, and one proposed by a Sino-Russian bloc, led by China and Russia.

The framework favoured by the Western bloc prioritises the term “cybersecurity” emphasising system integrity, as the safeguarding of networks and critical infrastructure, concurrently advocating for global initiatives to uphold the unimpeded flow of information. In contrast, the Sino-Russian bloc interprets cyber security as the control of content, communication, and interactions in cyberspace. It is primarily focused on preventing activities that could

undermine domestic governance and political stability, exhibiting less appreciation for the free flow of information. For this bloc, the term "information security," is preferred, centring on content integrity.[12]

This lack of a common foundation hinders the development of cohesive obligations, consequences and standards, leaving the space sector vulnerable to cyber threats in the absence of a unified and comprehensive strategy.

Cyber security landscape within the Australian space sector

Australia has recently experienced a rise in both the number and sophistication of cyber threats. At the same time, the country increases its usage and dependence on space for defence, industry and civil uses.

To counter cyber threats, Australia has data protection laws[13] and some cyber security regulations embedded in the protection of critical infrastructure. Australia also possesses national cyber security strategies and develops cyber security programs and toolkits for civil society and industry.[14]

Australia has civil and defence space strategies[15] and legislation focused on launching activities, it has yet to develop specific policies or strategies regarding space cyber security. This is despite recognising cyberattacks as a possible threat to its space infrastructure. Australia also has separate government agencies that oversee cyber security and space — the Australian Cyber Security Centre and the Australian Space Agency (ASA) — with little integration between the two.

Within the legal domestic framework, there is recognition that space assets suffer similar cyber security issues to other industries. However, the specific characteristics of space, such as environmental challenges and operational challenges, mean that a customised space cyber security framework is necessary. Such a framework could take the form of an implementation tool, a strategic document, a chapter of an Act or a governmental program. In all cases, it must cover the intersection of space security and cyber security and be developed by the Australian government in collaboration with Australian space stakeholders.

Australia's main space legislation, the *Space (Launches and Returns) Act*, does not offer comprehensive provisions concerning cyber security. In this sense, the Act requires a cyber security strategy for its licensing process, however, this strategy is based on existent implementation documents, such as the *Strategies to Mitigate Cyber Security Incidents*, the Information Security Manual, and the *Cyber Incidents Response Plan*, which are mainly addressed to a broader cyber environment, and not tailored to the space sector.

While the US employed a sector-specific approach to cyber security regulations,[16] in Australia the topic is fragmented, receiving only tangential attention in scattered documents that primarily address other focal points, such as telecommunication and, especially, critical sectors in the *Security of Critical Infrastructure (SOCI) Act*.

Under the *SOCI Act*, space technology is classified as a critical sector and is therefore subject to the imposition of certain security obligations in Australia.

However, while recent amendments to the *SOCI Act* introduced additional security obligations pertaining to 22 critical infrastructure assets,[17] none of these assets are associated with space technology, making it the only critical sector without a designated critical infrastructure, and, consequently, without further security obligations.

The Department of Home Affairs (Home Affairs), which is responsible for the *SOCI Act*, is currently working on defining assets for space, but in the time it takes for these definitions to be finalised, space remains the least secure sector compared to other critical sectors in Australia. Moreover, Home Affairs and the ASA may need to develop a specific toolkit on space cyber security for private companies, to ensure the *SOCI Act* requirements are fulfilled by those seeking licences under the *Space (Launches and Returns) Act*. Alternatively, given that space technology underpins a significant portion of Australia's critical infrastructure, the *SOCI Act* could reconceptualise space not as another vertical critical infrastructure sector but as a horizontal one. This would allow for the development of a distinct regulatory framework tailored to the unique security requirements of the space sector.

The cyber security of space infrastructure should also be included as a priority in Australia's military and strategic alliances with significant space-faring nations. Australia could use these alliances to not only promote rules for the cyber security of space infrastructures but also to consider mutual recognition of certifications and technology standards based on common, shared principles. For instance, in AUKUS, space technology is not listed in the scope of the partnership, although all three AUKUS states are space powers with bilateral space arrangements between them, sharing similar views on what constitutes responsible behaviour in space.

Conclusion

In the current context, cyberattacks are the most probable source of a significant space attack. Owing to their singular attacking characteristics, cyberattacks are extremely feasible and dangerous to the space sector, with direct defence, industry and civil repercussions.

The increasing dependence on space services and applications, and the vulnerability of space infrastructure to cyberattacks compel all nations to develop a framework to protect their space infrastructure against cyberattacks. In the case of Australia, although there are existing frameworks that can be applicable to improve the cyber security of the Australian space infrastructure, as well as governmental bodies with a degree of influence on the matter, the intersection of space security and cyber security is not yet mature.

To defend itself against cyberattacks, Australia should foster a coherent and efficient governance structure to counter cyberattacks with easy-to-determine responsibilities. It should also develop clear policy and legal frameworks that encompass the cyber security of its space infrastructure to guide industry and government actions and include space cyber security within its alliances and international security partnerships.

It's time for Australia to not only acknowledge this threat but to start developing concrete measures that are tailored to the intersection of space security

and cyber security. This requires a deeper understanding on the part of the Australian government on how to improve cyber security in the space sector while also maintaining its competitiveness as a growing space power.

Endnotes

[1] Vinicius Guedes Goncalves de Oliveira, Clémence Poirier, Marco Aliberti, Rodrigo Praino and Daniel Floreani, 'Cybersecurity of Australia's Space Infrastructure: An Assessment of the Policy and Legal Frameworks', *73rd International Astronautical Congress (IAC)*, Paris, September 2022, accessed 23 October 2024, https://iafastro.directory/iac/paper/id/73118/abstract-pdf/IAC-22,E9,2,1,x73118.brief.pdf?2022-03-29.12:05:24, 2.
[2] Beyza Unal, *Cybersecurity of NATO's Space-based Strategic Assets*, Chatham House, International Security Department, July 2019, accessed 22 November 2024, https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf, 8-11.
[3] Vilius Petkauskas, 'How a Florida teenager hacked NASA's source code', *Cybernews*, 28 July 2023, accessed 22 November 2024, https://cybernews.com/editorial/how-a-florida-teenager-hacked-nasas-source-code/
[4] James Pavur and Ivan Martinovic, *The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space*, *International Conference on Cyber Conflict*, Tallinn, Estonia, 2019, accessed 22 November 2024, https://ora.ox.ac.uk/objects/uuid:6e4194fa-474b-41cb-81fa-dbe5c5e94a68/files/r9c67wn16n, 9-15.
[5] Caroline Baylon, *Challenges at the Intersection of Cyber Security and Space Security*, Chatham House, International Security, December 2014, https://www.chathamhouse.org/sites/default/files/field/field_document/20141229CyberSecuritySpaceSecurityBaylonFinal.pdf, 38-39.
[6] Department of Defence, Space Power eManual: Light-Speed Edition, Commonwealth of Australia, 22 March 2022, accessed 22 November 2024, https://airpower.airforce.gov.au/publications/SPMLink, 25.
[7] Ibid, 15.
[8] Col Charles S. Galbreath, *Building U.S. Space Force Counterspace Capabilities: An Imperative for America's Defense*, Mitchell Institute for Aerospace Studies, 2023, accessed 22 November 2024, https://mitchellaerospacepower.org/wp-content/uploads/2023/06/Building-U.S.-Space-Force-Counterspace-Capabilities-WEB.pdf, 17-22.
[9] Article I of the *Outer Space Treaty* underscores that the utilization of outer space must be conducted for the collective benefit of all nations, constituting the province of all mankind. Article II states outer space and celestial bodies within it are beyond the purview of national appropriation.
[10] World Summit on the Information Society, *Declaration of Principles - Building the Information Society: a global challenge in the new Millennium*, 12 December 2003, accessed 22 November 2024, WSIS-03/GENEVA/DOC/4-E, https://www.itu.int/net/wsis/docs/geneva/official/dop.html
[11] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General,* United Nations Digital Library, 2015, accessed 22 November 2024, https://digitallibrary.un.org/record/786846?ln=en&v=pdf, 12.
[12] Paul Meyer, 'Outer Space and Cyber Space: A Tale of Two Security Realms' in Anna-Maria Osula and Henry Rõigas (Eds.) *International Cyber Norms: Legal, Policy & Industry Perspectives*, NATO CCD COE Publications, Tallinn 2016, accessed 22 November 2024, https://www.thesimonsfoundation.ca/sites/default/files/Outer%20Space%20and%20Cyberspace-A%20Tale%20of%20Two%20Security%20Realms,%20NATO%20CCD%20COE%20Publications%20-%20Chapter%208%20by%20Paul%20Meyer,%20March%202016_1.pdf, 155-169.
[13] A good example is the *Privacy Act (1988)*, Australia's main legislation concerning the protection of personal information of individuals.

[14] *Australia's Cyber Security Strategy 2020*, the *Strategies to Mitigate Cyber Security Incidents*, and the *Defence Industry Security Program* can exemplify this scenario. *Strategies to Mitigate Cyber Security Incidents*, the *Information Security Manual*, and the *Cyber Incidents Response Plan*.
[15] Respectively, the Advancing space: *Australian civil space strategy 2019-2028* and the *Australia's Defence Space Strategy*.
[16] Examples of this approach include sector-specific regulations such as the Health Insurance Portability and Accountability Act Security Rule. More importantly, the US is currently developing its *Satellite Cybersecurity Act*, which addresses cyber security matters related to commercial satellite systems.
[17] *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022.*

Australian Centre for Space Governance

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

ACSG
AUSTRALIAN CENTRE FOR SPACE GOVERNANCE