QR Code

DO NOT REMOVE

SMARTSAT COOPERATIVE RESEARCH CENTRE

Flinders University

CYBER OPS

The cybersecurity of the Australian Space Infrastructure – A legal and policy analysis

Vinicius Guedes Goncalves de Oliveira[1]

Introduction

As space becomes a segment progressively important for defence, industry and civil sectors, the threats to the space infrastructure also proportionally increase. In this context, cyberattacks are particularly relevant since they are a cheaper, easily controllable, and often untraceable, source of attack. Australia is extremely reliant on space services and applications, having most of its critical infrastructure sector underpinned by the space sector. Due to this, through documental analysis, the research assesses if the Australian legal and policy framework is considering the threat posed by cyberattacks on its domestic space infrastructure.

Aims

The three main aims are (1) Identify the main documents that compose the Australian policy framework regarding the cybersecurity of its space infrastructure and the main governmental branches and stakeholders related to it; (2) Analyse the overall maturity and development of the Australian policy framework, verifying if the procedures, policies, and attributions are considered clear and sufficient; and (3) Identify possible gaps, and opportunities in the Australian policy frameworks regarding the topic to assess which points Australia requires more development for further consolidation as an important space power.

Methods

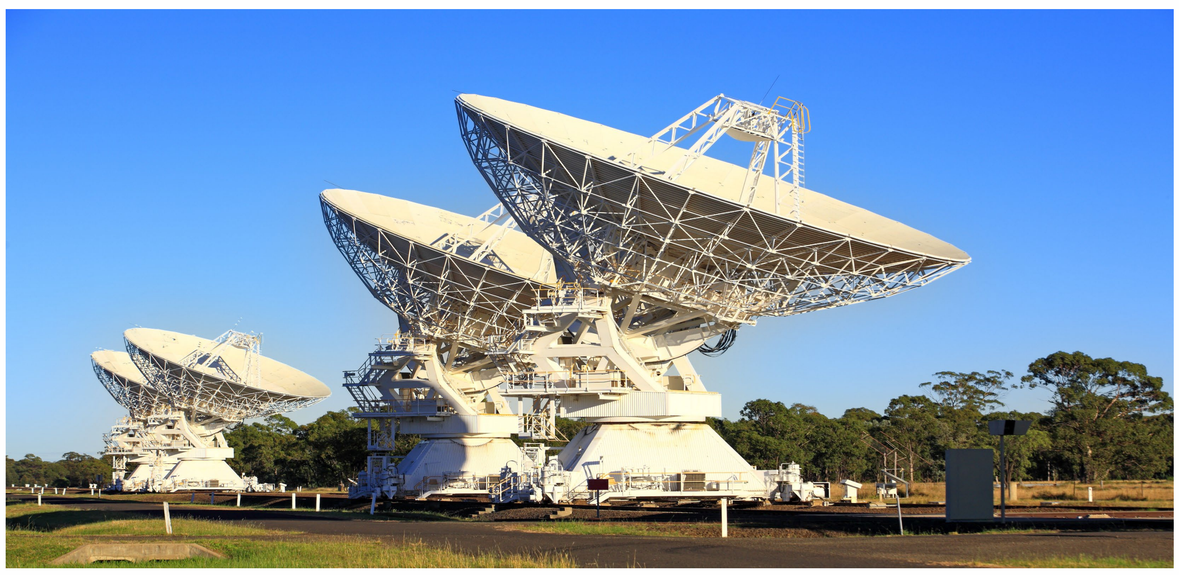
The research performs a qualitative data investigation through a documental analysis. For data collection five clear and explicit criteria of inclusion were established and utilised Furthermore, a series of stakeholder workshops with were organised for the purpose of data collection and validation. For data analysis purposes, the research engages in a structured focused method so that the same broad elements are considered in every individual document analysis.

Results

Government framework: Australia lacks a dedicated governmental branch tasked with overseeing the cybersecurity of its space infrastructure. Instead, this responsibility is dispersed across multiple departments, with a weak link between space and cyber. The cybersecurity of its space infrastructure is not included in any of Australia's military and strategic alliances with significant space-faring nations.

Policy framework: The strategic documents more focused on space at least recognise cyberattacks as a relevant threat to Australia's space infrastructure, however, they do not fully develop the topic. The strategic documents more focused on cyber, in its turn, do not even mention space technology, and only present directions to cyberattacks in a broader environment.

Legal framework: Australia's main space legislation, the Space (Launches and Returns) Act 2018 does not develop the cybersecurity of the space infrastructure in detail. As a result, the topic development is dealt with tangentially by other legislation with broader topics, *e.g.,* telecommunications and critical infrastructure, requiring to transport its obligations, when applicable, to the space domain.



References

STEER, C. 2023. Who is Australia in space? The need for a national space policy. In: MOSS, T. (ed.) The Foundations of Australia's Space Policy. Queensland, Australia: Griffith Asia Institute.

FROEHLICH, A. & SEFFINGA, V. 2018. National Space Legislation: A Comparative and Evaluative Analysis, Cham, Springer International Publishing AG.

1Flinders University – College of Business, Government and Law

Australian Government Department of Industry, Science, Energy and Resources | AusIndustry Cooperative Research Centres Program