Need for a Cyber Resilience Framework for Critical Space Infrastructure

Syed Shahzad, Li Qiao and Keith Joiner
School of Engineering and IT, Capability Systems Centre, University of New South Wales, Canberra., Australia
s.shahzad@adfa.edu.au
l.qiao@adfa.edu.au
k.joiner@adfa.edu.au

Abstract: The purpose of this paper is to introduce a case for a standardised comprehensive cyber resilience framework for Critical Space Infrastructure (CSI). Based on structure systematic review and meta-analyses, this paper outlines the needs of a risk-based framework. Space assets are fundamental components of critical national infrastructure (CNI), whose destruction significantly impacts many lives. Moreover, today's digitally connected space infrastructure is exposed to sophisticated and catastrophic cyber-attacks. This paper lays out the research gap to present the need for a comprehensive cyber resilience framework for CSI and future research and collaboration to understand the emergence of a new category of failures related to space-asset-reliance disruption risks.

Keywords: Cyber Resilience Framework for Critical Space Infrastructure, Critical Infrastructure, Cyber Security, Cyber Resilience, Resilience Framework

1. Introduction

Space assets are fundamental components of critical national infrastructure. They are an integral and crucial part of modern navigation, communication, weather, financial services, timing, defence, and science (Gheorghe et al., 2018). Space services enable society's vital functions, and their service offerings are difficult to substitute. The physical, cyber, geographical, and logical aspects of space infrastructure make it a perfect complex system of systems subject to cascading and escalating failures, increasing the impact of damage (Mureșan and Georgescu, 2017). Mureșan et al. (2016) state that space systems are a new type of critical infrastructure, not just a new category. Georgescu et al. (2019) argue that space assets should be described and accepted as critical national infrastructure. Although there has been much research in addressing space infrastructure operational security problems, little effort is made in developing a common means of assessing the resilience of the critical space infrastructure. A critical space infrastructure is a combination of space and ground assets whose disruption or failure would impact other critical infrastructure (Georgescu et al., 2018). A disproportionately small number of studies explicitly investigate the vulnerability of the critical space infrastructure to cyber-attack scenarios and how they could be prevented, mitigated, and made resilient. Few scholars have drawn on systematic research into the cyber resilience framework for critical space infrastructure. Therefore, there is an urgent need to address the resilience for space infrastructure security as a field. As the first step towards the cyber resilience framework, the current paper aims to understand the need for such a framework. Therefore, the overall motivation behind this work is to initiate a discussion for a comprehensive cyber resilience framework for critical space infrastructure. This work is the first known to systematically examine the research in cyber resilience for critical space infrastructure and calls for a comprehensive framework.

2. Background

Much of the research up to now has been limited and focused on one particular domain of space, which is operational security (OT). However, the unique threats for space infrastructure come from four separate attacks and weapons known as anti-satellite weapons, described as "*kinetic physical, non-kinetic physical, electronic, and cyber* (Way, 2021). As most digitised critical infrastructure, space infrastructure is equipped with computers and networked hardware with connectivity for remote analytics, configuration, and upgrades, creating opportunities for cyber-attacks and cyber-defence. Typically, space infrastructure is divided into three main segments: outer space equipment, ground stations, and launch providers. These segments have unique vulnerabilities (Usman et al., 2020). The interdependencies between the three space segments lead to the proliferation of unique space cyber security risks and threats (Georgescu and Bucovețchi, 2017). Despite the importance and known limitations of cyber security for space infrastructure, there has been little focus on cyber resilience for space assets and comprehensive guidance in the form of standards from the technology, ownership, and management perspectives.

This paper focuses on cyber-attacks and work published within the tenants of cyber resilience. The study's goal is to understand better the needs and the performance of the cyber resilience framework. Therefore, this paper motivates the need for such as cyber resilience framework and outline elements of an evaluating cyber resilience framework. To the authors' best knowledge, this study is unique in the discipline since this work is the first to examine the research and calls for establishing a need for a cyber resilience framework for critical space infrastructure. Since the topic crosses multiple domains, it consists of cyber, space and system engineering. In order to fully cover these disciplines' branches, a more advanced reporting system is required to overview the topic. The preferred reporting items for systematic reviews and meta-analyses reporting guidelines (Luhnen et al., 2018) is a comprehensive, explicit, and reproducible method, as documented guidelines by Durach et al. (2017).

The remainder of this paper is organised as follows. Section two presents the background of the study and motivates the need for a cyber resilience framework. Then, section three introduces the method to identify the need for such a framework. The second four discusses the finding, section five outlines the first steps towards a common resilience framework. Finally, Section six concludes the paper and section seven presents the future work.

3. Methodology

In order to assess the need for a cyber resilience framework for critical space infrastructure, the adopted method is the preferred reporting item for systematic reviews and meta-analyses (PRISMA), based on English-language peered reviewed papers published in the last ten years. PRISMA is widely known as an instrument to qualitatively appraise a systematic review of the quality attributes evaluations (Luhnen et al., 2018). The search results are visually represented in Figure 1, following the PRISMA set structure (Moher et al., 2009). The selected search terms (keywords), including the alternate terms used, are listed in Table 1. The search criteria were applied to SCOPUS, Google Scholar, IEEE, and JSTOR databases, and a spreadsheet was developed to construct combinations of keywords to address all research questions. The articles between 2017 and 2021 were shortlisted whose abstracts, titles, or keywords included one of the search terms. Approximately 241,000 documents were published or accepted between 2017 and 2021 (up to and including mid-Oct 2021 at the time of writing) in cyber security, space, systems engineering and space engineering domains. Over 467 articles were finally selected and included in this literature review for screening. Forty-six per cent of the articles screened were excluded based on non-relevance. Another thirty per cent of articles were not retrieved because of record-duplication between databases. The final 115 most applicable and available articles were read carefully to answer, "What frameworks, standards and regulations are developed explicitly for cyber resilience of space infrastructure?".

Most of the literature used was published between 2019-2021, and 68% of the studies go back no more than seven years. USA, China, Romania, and Turkey have 40% contributions and pay attention to critical space infrastructure. There is a significant lack of peer-reviewed work in the area of cyber resilience for space infrastructure.

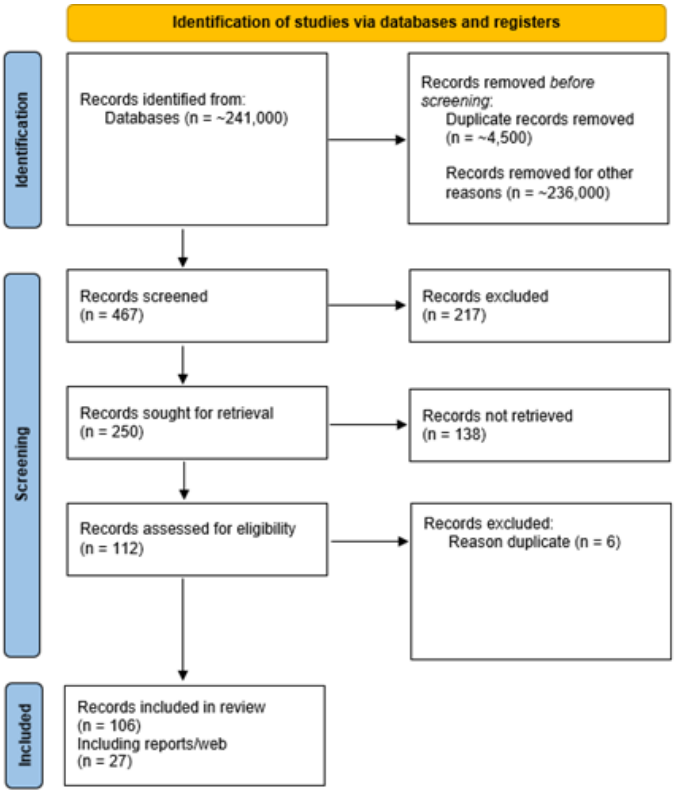

Figure 1: Preferred Reporting Items for Systematic Reviews and Meta-Analyses

Table 1: Search keywords and combinations

Keyword	Condition	Keyword
space assets	or	cybersecurity
critical space infrastructure	or	standards
space systems cybersecurity	and	framework
space assets frameworks	and	cybersecurity
space assets policy	and	cybersecurity
space assets policy	or	cybersecurity
critical space infrastructure	or	cyber resiliency
Space infrastructure	and	cyber resiliency
Space infrastructure	and	cyber
space cyber frameworks	or	assesment
cybersecurity assessment frameworks	and	Space
critical space infrastructure	and	cyber attacks
Space infrastructure	and	governance
Space infrastructure	and	cyber attacks
Space infrastructure	and	kinetic attacks
Space infrastructure	and	attacks
Space infrastructure	and	current threats
cyber vulnerability assessment	or	space
attack vectors	or	critical assets
cyber security threats	and	SCADA or ICS or IoT
cyber security space	and	security models
critical infrastructure	and	attacker behaviour
cyber attack	and	motivation
system engineering	and	cybersecurity (cyber security)
system engineering	and	cyberresiliency (cyber resiliency)
system engineering	and	space
Space system engineering	and	security
system engineering frameworks	and	space
systems engineering	and	business
systems engineering	and	business process / management
systems engineering	and	business framework
systems engineering	and	business management
systems engineering	and	business process modeling
system engineering	and	risk management
regulatory framework	and	cybersecurity (cyber security)
regulatory framework	and	cyber resiliency/resilience
regulatory framework	and	space
business efficiency	and	space
business	and	regulatory framework
cybersecurity	and	risk assessment frameworks
cybersecurity	and	asset classification
cybersecurity	and	risk categorisation
cybersecurity	and	business impact
cybersecurity	and	risk assessment

4. Analysis and Discussion of Findings

The outer space assets are subjected to specific space phenomena, orbital debris, and the harshness of the outer space environment with temperatures and radiation (Mark, C.P. and Kamath, S., 2019). However, deliberate threats to critical space systems come from the state, rogue states, and non-state actors with various access levels to highly capable and affordable anti-satellite weaponry (La Bella, 2020). Egeli (2021) argues that the critical space infrastructure is under new anti-satellite attacks, and adversaries are increasingly developing new cyber threats, perhaps to achieve coordinated cyber-storming within 'grey-zone' tactics short of actual war (Austin, 2020). In addition, the kinetic weapons to destroy satellites in low Earth orbit have been shown to cause a large debris field that threatens other satellites and pollutes the space domain beyond recovery (Egeli, 2021). Bateman (2021) argues that the United States should avoid kinetic anti-satellite. Instead, the US should invest in developing and deploying non-kinetic weapons such as electronic or cyber-attacks against their adversaries' space assets.

In contrast to kinetic weapons, the impact of cyber-attacks in outer space is not well understood. Georgescu et al. (2019) found air-transport infrastructure was virtually dependent on space systems, and the space systems have a high probability of spontaneous malfunction as they operate in the most challenging environments. Johnson and Yepez (2011) analysed the Global Navigation Satellite Systems (GNSS) cyber threats. Their research intends to *provide an integrated, risk-based approach to the identification of attack scenarios that can help assess the resilience of safety cases to security threats*." They also investigated several threats to GNSS infrastructures from denial-of-service attacks on the ground-based infrastructure, data integrity, and vulnerabilities through insider attacks that could affect the services' accuracy, integrity, availability, and continuity. However, their focus was on the safety aspects and did not perform a fuller cyber risk assessment.

The growth in outer space activities is mainly driven by the commercial demand from new satellites for space transportation. This growth is called "Space 2.0", where '*out of new space thinking has come new technologies, new market entrants, new launcher systems, new ways of financing space ventures, new satellite architectures, efficient new small satellite designs, new types of ground antenna systems with electronic tracking, and market shifts toward networked services'* (Logue, T.J. and Pelton, J., 2019). The private sector plays a crucial role in the outer space activities where the public sector once was driving innovation and technology. In 2021, more than 50 countries will operate satellites in space (The Global Nature of Space Activities | Secure World, 2021). The new wave of smaller and more advanced satellites creates the danger of space crowding and signal interference. Safe operations of space assets are not only critical for the owners of those assets but global security and peace, as space assets monitor anti-terrorist activities, surveillance, and coordinate and disaster management (Bhattacherjee et al., 2018). Significant dependency on space infrastructure poses a critical yet under-recognised security predicament for critical infrastructure providers, policymakers, and governments.

Surprisingly, Australia, one of the wealthiest nations, has contributed little to space policy and space in general (Biddington, 2021). Georgescu et al. (2015) point out that governance in the space environment is complex since space has no clear jurisdictional boundaries that inform critical national infrastructure processes on Earth. For example, the European Commission states: '*Space infrastructure is critical infrastructure on which services that are essential to the smooth running of our societies and economies and our citizens' security depend. It must be protected, and that protection is a major issue for the EU which goes far beyond the individual interests of the satellite owners'* (EU., 2008). Therefore, each country currently takes responsibility to identify, designate and protect its specific infrastructure as critical national infrastructure, with no overarching regulatory authority.

Although space technology plays a critical role concerning commerce and security, it can also be seen as a threat to international peace (Rao et al., 2017). Space was the frontier for governments who were the primary sponsor of exorbitant research and development. Hence the International space law does not cover the space activities of today's major player, the private sector. By law, the private sector entities are to be under the supervision of the state of their jurisdiction, and their activities are to be assumed within the framework of relevant national laws and policies. '*There is no national legislation in many states on space-related matters, and many key issues relating to liability, technical safeguards, security, and innovation are not addressed adequately'* (Oltrogge et al., 2020). There is an urgent need for quite a few nations to develop legislation and standardise them with International Law. There has been a drive from the international community to develop "risked-based" frameworks for both public and private sectors (Daniels, and Paté-Cornell, 2017). Despite increasing space

technology advancements with rapid growth, international space lawmakers have not progressed beyond the initial five treaties and non-binding resolutions in the last fifty years.

Unfortunately, the UN treaties on outer space activities do not adequately facilitate commercial space activities (Rao et al., 2017). The current corpus of space law comprises treaties and agreements accepted and adopted by the total signatories. Such non-universal recognition and buy-in have seriously undermined the universal applicability of space law despite its adoption by unanimous approval in the UN General Assembly (Sachdeva, 2017). Oralova (2015) describes the "*Jus Cogens of Space Law*" as the fundamental principles that '*carry unanimous acceptance among the comity of nations as peremptory norms and command invariable adherence from states.*' '*Potential derogation from the principles of non-appropriation of outer space and of freedom of exploration and use of outer space, which is essential for the whole system of international space law is inconsistent with the natural state of outer space and can threaten international space and security*' (Oralova, 2015). These laws state as follows:

- Outer space as a province of humankind
- Freedom of access to all states for exploration and use
- State responsibility to humanity
- Prohibition on the placement of weapons in earth orbit
- Rescue and return of astronauts and space objects

The UNGA Resolution on Legal Principles recognised the risk of outer space weaponisation. However, it did not consider potential digital or, now as we know, cyber threats (UNOOSA, 2021), nor has the resolution been updated to reflect the new challenges. The UNGA authors only considered the possibilities relating to kinetic attacks, such as military activities. The North Atlantic Treaty Organisation (NATO) has facilitated discussions to address cyber related challenges and made series of recommendations (Tatar, U. 2020).

The increasing use of space systems for military reasons and several other conflicting issues make space assets vulnerable to attack. As per the United Nations Office for Outer Space Affairs (UNOOSA), '*State-Parties undertake not to place in orbit around the Earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction, install such weapons on celestial bodies, or station weapons in Outer Space in any other manner* (UNOOS 2, 2021). The Secretary-General of the United Nations Group of Governmental Experts commissioned a study on transparency and confidence-building measures in outer space activities. The study concluded that *the 'World's growing dependence on Space-based systems and technologies and the information they provide requires collaborative efforts to address threats to the sustainability and security of Outer Space activities'* (Murthi, Gopalakrishnan, 2017). Somewhat in contrast to the research literature, governments and industry have begun to address cyber security for space infrastructure. For example, in a recent initiative, the White House released a Space Policy Directive (SPD5) entitled "*Cybersecurity Principals for Space Systems"* (Directive5, 2020) that establishes a broad set of guidelines for space companies in developing their cyber protection approaches. These guidelines include:

- Protection against unauthorised access to critical space vehicle functions;
- Physical protection measures designed to reduce the vulnerabilities of a space vehicle's command, control, and telemetry receiver systems;
- Protection against communications jamming and spoofing;
- Protection of ground systems, operational technology, and information processing systems through adopting deliberate cyber security best practices. This adoption should include practices aligned with the National Institute of Standards and Technology's cyber security framework to reduce the risk of malware infection and malicious access to systems, including from insider threats;
- Adoption of appropriate cyber security hygiene practices, physical security for automated information systems, and intrusion detection methodologies for system elements; and
- Management of supply chain risks that affect space systems' cyber security by tracking manufactured products, requiring sourcing from trusted suppliers; identifying counterfeit, fraudulent, and malicious equipment; and assessing other available risk mitigation measures.

These principles are defined as best practices, but they lack a formal framework and governance toolkit. MITRE has, however, released a recent paper, "*Cyber Best Practices for Small Satellite*", to address some concerns raised by SPD5 (Visner and Kordella, 2020). A new Space Information Sharing and Analysis Centre (ISAC) has also recently been established '*to enable 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 firms, and to serve as the primary communications channel for the sector with respect to this information' (Space ISAC. 2021). ISAC has developed a framework to describe threats in operations, business systems, provider, and communication segments. Besides that, a handful of private organisations have published some work, such as Aerospace Industries Association, published the first National Aerospace Standard NAS9924, citing it as "*Cyber Security Baseline*". Aerospace Industries Association developed baseline controls that focus on cyber security for the supply chain for aerospace and defence supply (Aerospace Industries Association, 2021)

Researchers have also become increasingly interested in anti-satellite cyber threats in recent years as their strategic, legal, and technical implications are not well-understood (Heinl, 2016). Scholars have argued the limitations of the '*non-binding doctrine'* of *jus ad Bellum* to cyber conflicts "Tallinn Manual" (Wallace and Jacobs, 2018) (Schmitt, 2017) (Norris, 2013). Therefore, the significant dependency on space infrastructure poses a critical yet under-recognised security predicament for critical infrastructure providers and policymakers. The threats for critical space infrastructure arise from distinct types of attacks and weapons known as anti-satellite (ASAT) weapons. These weapons are kinetic, non-kinetic, electronic, and cyber. If a significant cyber-attack happens, the resilience of commercial space infrastructure is likely to be fragmented, reduced, and may require expensive replacement, such that key-dependent terrestrial services would be unavailable for long durations. Therefore, a contemporary challenge is developing, mandating, and implementing cyber security and resiliency for a complex and substantial space infrastructure spanning different systems, jurisdictions, and legal frameworks. However, there is generally a lack of peer-reviewed research in cyber security for space infrastructure, and not much work has been done in space reference architecture, governance frameworks, and tools. Thus, the paper suggests a comprehensive cyber resilience framework is needed to regulate the expanding space industry.

5. Towards a Cyber Resilience Framework

This section outlines the needs for the future cyber resilience framework for critical space infrastructure. First, the future framework shall build on a set of risk assessment and management questions. The overarching approach for the suggested framework is based upon Kaplan and Garrick (1991) structured risk analysis employing the following three fundamental risk assessment questions: 'what can go wrong?', 'what is the likelihood?', and 'what are the consequences?' In addition, the future cyber resilience framework shall cover the next triplet of framework-specific questions:

1. What viable options are available?
2. What is the actual cost of risk?
3. What is the return on risk reduction investment?

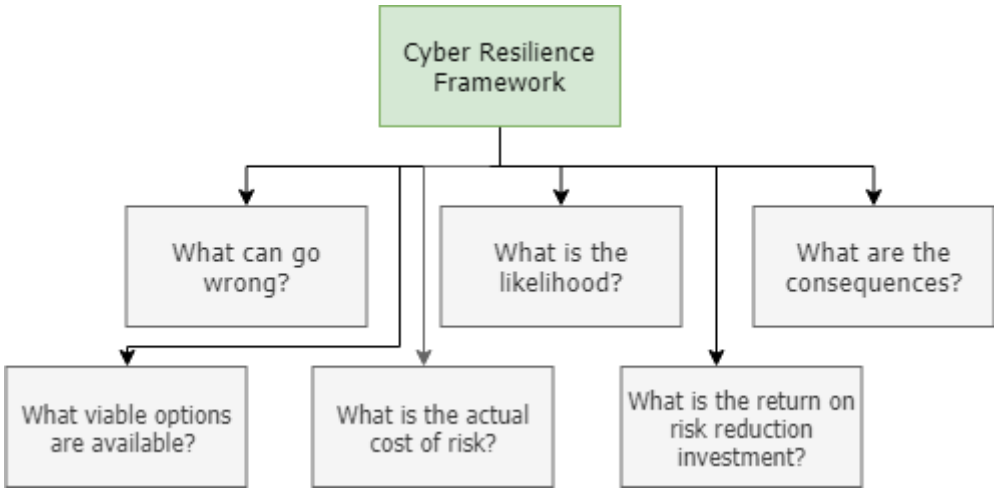

Figure 2: Framework Foundation based on Structured Risk Analysis

Second, the future framework shall be fair and consistent. It assures that the development and integration of a space system (and subsystems) hardware, software and supply chain fully incorporated cyber security and resilience needs appropriate to the contested information environment for which it is intended to operate. The framework employs attack surface management (ASM) for identification, inventory, classification, monitoring

and prioritisation of all digital assets of a space system. Our proposed framework builds on the above risk assessment and management questions, developing a discussion on the current literature on the subject, and compares and highlights the similarities and new possibilities.

Third, the future framework shall consider both tangible and intangible assets. Despite decades of research on cyber security and risk assessment, finding the critical assets (tangible and intangible), and more importantly, the value of "intangibles" has been less than satisfactory. Therefore, asset categorisation, risk identification, risk assessment and decision-making methods are essential for the future cyber security framework to provide business impact assessment.

Fourth, the future framework building shall develop a reliable cyber resilience framework and ontology encompassing many requirements. For example, the framework will need to be risk-based (cyber and business risks), requirements focused, and cost-driven (correct cost estimation for impact analysis). Further, the framework will need to incorporate security by design (cyber security and resilience into design, development, acquisition, operation, and sustainment), be resilient (protect, detect, react, and restore), be controls-based (select, implement, assess, and monitor) and where possible reduce the test and evaluation burden.

6. Conclusion

The critical space infrastructure (CSI) supports vital functions of society to operate its sensitive and crucial services from health, mobility, and security and peace. Despite their importance and increased cyber security risks, threats and attacks, the global community is yet to define, negotiate and mandate a treaty or instrument. At present, there are no agencies or governing bodies that monitor and restrict the use of satellites (Falco, 2018). The lack of overarching governance creates a vacuum in security design and operational cyber resiliency for the private sector that plays a vital role in the outer space activities where the public sector once was driving innovation and technology. Modern space systems are fundamentally dependent upon information technology and networked systems operating in the domain of cyberspace. These systems are inherently interconnected, either directly or indirectly, formatting a complex system of systems whose operations are interdependent and critical to the command, control, and performance of platforms, sensors, and other elements. Although the dependence on cyberspace and the networking of systems is a double-edged sword, enhancing our capabilities yet at the same time introducing numerous potential vulnerabilities. In response to the increasingly pervasive and adaptive threat environment, a consistent and fair cyber security and resilience assessment framework are critical to reduce the risk and provide a layered approach to ensure mission assurance.

7. Future Research

While the concept of a cyber security and resilience framework for space infrastructure is new, it certainly demands the attention of academics from all domains. Comparisons between the commercial space domain and banking and finance can be drawn, where risk criticality and cost are crucial for risk owners. At present, the space industry is like the High Seas and Antarctica, where no single regulatory or governance framework is applicable, instead of a combination of international treaties, commercial contractual frameworks, and national laws only relevant to specific objects and individuals. Remarkably few studies have been designed to study the commercial space assets cyber security and resiliency from a risk-based, cost-benefit approach. As critical space infrastructure is under new anti-satellite attacks and the private sector is increasingly growing, this literature review suggests developing and research a structured cyber-resilience framework for critical space infrastructure with:

- an underpinning cyber-vulnerability ontology for finding the critical digital assets,
- a means to value "intangibles", and
- a governance framework for through-life secure and resilient space operations.

A disproportionately small number of studies explicitly investigate the vulnerability of the critical space infrastructure to cyber-attack scenarios and how they could be prevented, mitigated, and made resilient. Therefore, we suggest that coherent and efficient future collaborative research can be significantly aided by understanding the already proposed cyber resilience frameworks in other domains.

References

Aerospace Industries Association. 2021. AIA Announces First Cyber Security Standard | Aerospace Industries Association. [online] Available at: <https://www.aia-aerospace.org/news/aia-announces-first-cyber-security-standard> [Accessed 13 October 2021].

Austin, G. ed., 2020. National cyber emergencies: The return to civil defence. Routledge.

Bateman, A., 2021. America Can Protect Its Satellites Without Kinetic Space Weapons - War on the Rocks. [online] war on the Rocks. Available at: <https://warontherocks.com/2020/07/america-can-protect-its-satellites-without-kinetic-space-weapons/> [Accessed 13 October 2021].

Bhattacherjee, D., Aqeel, W., Bozkurt, I.N., Aguirre, A., Chandrasekaran, B., Godfrey, P.B., Laughlin, G., Maggs, B. and Singla, A., 2018, November. Gearing up for the 21st century space race. In Proceedings of the 17th ACM Workshop on Hot Topics in Networks (pp. 113-119).

Biddington, B., 2021. Is Australia Really Lost in Space?. Space Policy, 57, p.101431.

Daniels, M.P. and Paté-Cornell, M.E., 2017. Risk-based comparison of consolidated and distributed satellite systems. IEEE Transactions on Engineering Management, 64(3), pp.301-315.

Directive5, 2020. Cybersecurity Principles for Space Systems. National Space Policy.

Egeli, S., 2021. Space-to-Space Warfare and Proximity Operations: The Impact on Nuclear Command, Control, and Communications and Strategic Stability. Journal for Peace and Nuclear Disarmament, 4(1), pp.116-140.

EU., 2008. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A European strategy for data, COM/2020/66 final. [online] Op.europa.eu. Available at: <https://op.europa.eu/en/publication-detail/-/publication/ac9cd214-53c6-11ea-aece-01aa75ed71a1/language-en> [Accessed 13 October 2021].

Falco, G., 2018. The vacuum of space cyber security. In 2018 AIAA SPACE and Astronautics Forum and Exposition (p. 5275).

Georgescu, A. and Bucovețchi, O., 2017, May. A generic flow based model for understanding critical infrastructure dependency on space systems. In Proceedings of the 29th international business information management association conference (pp. 3-4).

Georgescu, A., Bucovetchi, O. and Tatar, U., 2018. Space systems as critical infrastructures. FAIMA Business & Management Journal, 6(1), pp.24-34.

Georgescu, A., Gheorghe, A.V., Piso, M.I. and Katina, P.F., 2019. Critical Space infrastructures: risk, resilience and complexity (Vol. 36). Springer.

Gheorghe, A.V. and Vamanu, D.V., 2007. Risk and vulnerability games. The anti-satellite weaponry (ASAT). International journal of critical infrastructures, 3(3-4), pp.457-470.

Gheorghe, A.V., Georgescu, A., Bucovețchi, O., Lazăr, M. and Scarlat, C., 2018. New Dimensions for a Challenging Security Environment: Growing Exposure to Critical Space Infrastructure Disruption Risk. International Journal of Disaster Risk Science, 9(4), pp.555-560.

Heinl, C.H., 2016. The potential military impact of emerging technologies in the Asia-Pacific region: A focus on cyber capabilities. In Emerging Critical Technologies and Security in the Asia-Pacific (pp. 123-137). Palgrave Macmillan, London.

Kaplan, S., 1991. The general theory of quantitative risk assessment. In Risk-Based Decision Making in Water Resources V (pp. 11-39). ASCE.

La Bella, J., 2020. Star Wars: Attack of the Anti-Satellite Weapons in Anticipatory Self-Defense. U. Pac. L. Rev., 52, p.733.

Logue, T.J. and Pelton, J., 2019. Overview of commercial small satellite systems in the “New Space” age. Handbook of Small Satellites: Technology, Design, Manufacture, Applications, Economics and Regulation, pp.1-18.

Luhnen, M., Waffenschmidt, S., Schwalm, A., Gerber-Grote, A. and Hanke, G., 2018. Quality Assessment of Systematic Reviews of Health Economic Evaluations: Pitfalls with the Application of the PRISMA Statement. Comment on Quang et al.(Sys Rev Pharm. 2017; 8 (1): 52-61). Systematic Reviews in Pharmacy, 9(1), pp.83-84.

Mark, C.P. and Kamath, S., 2019. Review of active space debris removal methods. Space Policy, 47, pp.194-206.

Moher, D., Liberati, A., Tetzlaff, J., Altman, D.G. and Prisma Group, 2009. Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. PLoS medicine, 6(7), p.e1000097.

Mures¸an L., A. Georgescu, I. Jiva˘nescu, S. Popa, and S. Arseni. 2016. Charting critical energy infrastructure dependencies on spaces Critical energy infrastructure protection and cyber security policies, ed. M.H. Cas¸ın, and G. Gluschke, 177–192. 2016. Istanbul, Turkey: Hazar Strateji Enstitu¨su¨.

Murthi, K.S. and Gopalakrishnan, V., 2017. Trends in Outer Space Activities—Legal and Policy Challenges. In Recent Developments in Space Law (pp. 27-42). Springer, Singapore.

Norris, M.J., 2013. The Law of Attack in Cyberspace: Considering the Tallinn Manual’s Definition of ’Attack’ in the Digital Battlespace. Inquiries Journal, 5(10).

Oltrogge, D.L. and Christensen, I.A., 2020. Space governance in the new space era. Journal of Space Safety Engineering, 7(3), pp.432-438.

Oralova, Y., 2015. Jus cogens norms in international space law. Mediterranean Journal of Social Sciences, 6(6), p.421.

Rao, R.V., Gopalakrishnan, V. and Abhijeet, K. eds., 2017. Recent Developments in Space Law: Opportunities & Challenges.

Sachdeva, G.S., 2017. Select Tenets of Space Law as Jus Cogen. In Recent Developments in Space Law (pp. 7-26). Springer, Singapore.

Schmitt, M.N. ed., 2017. Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press.

Space ISAC. 2021. Space ISAC - Space Information Sharing and Analysis Center. [online] Available at: <https://s-isac.org/> [Accessed 13 October 2021].

Swfound.org. 2021. The Global Nature of Space Activities | Secure World. [online] Available at: <https://swfound.org/space-sustainability-101/the-global-nature-of-space-activities/> [Accessed 13 October 2021].

Tatar, U., 2020. Critical Space Infrastructures: Perspectives and a Critical Review. Space Infrastructures: From Risk to Resilience Governance, 57, p.3.

UNOOS 2., 2021. ST/SPACE/61/Rev.2: International Space Law: United Nations Instruments. [online] Unoosa.org. Available at: <https://www.unoosa.org/oosa/oosadoc/data/documents/2017/stspace/stspace61rev.2_0.html> [Accessed 13 October 2021].

UNOOSA. 2021. Legal Principles. [online] Available at: <https://www.unoosa.org/oosa/en/ourwork/spacelaw/principles/legal-principles.html> [Accessed 13 October 2021].

Usman, M., Qaraqe, M., Asghar, M.R. and Shafique Ansari, I., 2020. Mitigating distributed denial of service attacks in satellite networks. Transactions on Emerging Telecommunications Technologies, 31(6), p.e3936.

Visner, S.S. and Kordella, S., 2020. Cyber Best Practices for Small Satellites. In ASCEND 2020 (p. 4013).

Wallace, DA and Jacobs, C.W., 2018. Conflict Classification and Cyber Operations: Gaps, Ambiguities and Fault Lines. U. Pa. J. Int'l L., 40, p.643.

Way, T., 2021. Counterspace Weapons 101 - Aerospace Security. [online] Aerospace Security. Available at: <https://aerospace.csis.org/aerospace101/counterspace-weapons-101> [Accessed 13 October 2021].