A New Dawn for Space Security

Jordan J. Plotnek and Jill Slay
University of South Australia, Adelaide, Australia
Jordan.Plotnek@mymail.unisa.edu.au
Jill.Slay@unisa.edu.au

Abstract: Space infrastructure provides vital services for a number of critical industries, including; defence, transportation, energy, utilities, emergency services, banking, environment, academia, and others. These services range from global communications to remote sensing and geolocation, with many new applications undoubtedly on the horizon, including plans for further exploration and even human settlement. It is therefore essential that space technologies are protected from unwanted interferences – a task that is becoming more challenging by the day. Adding to the already complex space security environment, we are experiencing the beginnings of a second space race that is seeing the rapid deployment of space systems containing a vast array of new technologies, such as the Internet of Things (IoT) and advanced onboard processing. This is subsequently introducing new vulnerabilities to an already aged and vulnerable satellite ecosystem, hence increasing the risk of potentially catastrophic security events. Although well-articulated in political, legal, and international relations literature, the engineering, science, and technology aspects of space security are currently under-studied and disjointed, leading to fragmented research and inconsistent terminology. This paper examined space security from an engineering perspective by conceptually tying existing space and security literature together to detail the space threat landscape and identify research gaps and opportunities. Additionally, this paper identifies the need for wider recognition of space systems security as a specialist inter-disciplinary domain in order to break down disciplinary silos, enhance collaboration, and unify definitions, taxonomies, and research objectives.

Keywords: critical infrastructure, cyber threat, resilience, satellite, space security, space weapon

1. Introduction

In 1957 the Soviet Union launched Sputnik-1, the first manmade object to enter earth's orbit, triggering a two-decade long space race and forever changing the course of human history. Today we are on the cusp of a second space race, this time with almost 3000 artificial satellites already in operation (UCS, 2020), and countless more space debris littered in perpetual orbit. As the battle for space superiority ramps up for a second time, we are forced to acknowledge the wildly different technological landscape compared to that of our scientific colleagues back in 1957.

Industrial systems are increasingly both particularly vulnerable and specifically targeted by adversarial groups and state actors (Kaspersky Lab, 2019), and space systems are not immune. In fact, as detailed in the following sections, space systems face an even greater range of threats and have even further reaching consequences than those combatted by terrestrial critical infrastructures (Bradbury et al., 2020), and considering the level of military dependence on space infrastructure and the volatile state of global affairs today (Donnelly, 2021), there has never been a more urgent need for resilient space systems as there is now.

This paper aims to lay the academic foundations in response to the existing void in literature on security and resilience in a space systems context. The paper commences with a review of published literature in the field at Section 2, moving onto setting the scene by introducing space infrastructure, space threats, past events, and future trajectories in Section 3. With context in hand, the need for space systems security as a recognised interdisciplinary domain is then presented in Section 4, followed by a discussion of potential space systems security research opportunities in Section 5 and finally concluding in Section 6.

2. Foundational Literature

Of the various disciplines contributing to space security knowledge, the social sciences are the most mature, with several decades of published history. Traditionally, space security has been viewed primarily as a military domain due to Cold War motivations behind the first space race (Sheehan, 2015). More recently, however, this view has expanded to include three dimensions of space security (Mayence, 2010):

1. security in space (i.e., protecting space systems);
2. space for security (i.e., military space operations); and
3. security from space (i.e., protecting Earth from space-based threats).

This paper focuses exclusively on the first dimension of space security, herein referred to as `Space Systems Security'. Drawing from older literature we can find several space security definitions that can be reapplied directly to space systems security. Moltz's definition serves as a good baseline, defining it as "the ability to place and operate assets outside the Earth's atmosphere without external interference, damage, or destruction" (Moltz, 2011).

A whitepaper by the United States Office of the Assistant Secretary of Defense for Homeland Defense & Global Security entitled 'Space Domain Mission Assurance: A Resilience Taxonomy' (USDoD, 2015) gets particular attention amongst space resilience advocates, however it does little to set the scene before proposing a resilience taxonomy that is detached from tangential resilience and security literature.

A second key text in this domain is the book entitled 'Critical Space Infrastructures: Risk, Resilience and Complexity' (Georgescu et al., 2019), which successfully introduces space system fundamentals and examines space systems as critical infrastructure but is decidedly lacking in its discussion of cyber security issues. Though, the introduced taxonomy is helpful as it splits Critical Space Infrastructure (CSI) into five distinct categories, as well as discussing interdependencies with other systems like those for water and energy.

Harrison et al. conducted a 'Space Threat Assessment' in 2020 (Harrison et al., 2020) that focuses on the threat of counter-space weapons, breaking them down into four broad but useful categories: kinetic physical, non-kinetic physical, electronic, and cyber. The remainder of the report is less repurposable and goes on to analyse different nation state capabilities and their threat to the United States at the point in time of the assessment.

A paper entitled 'Cybersecurity Threats to Satellite Communications' (Housen-Couriel, 2016) establishes a typology of state actor responses. However, it does not adequately address space security from a technical perspective. In contrast to Harrison et al., Housen-Couriel identifies only three kinds of satellite 'disruptions': kinetic (direct impact of one satellite with another), virtual (interference with communications), and hybrid (electromagnetic pulse, or EMP, weapons). It then plots these three disruption categories against five stages of satellite operations:

1. pre-launch;
2. at launch;
3. telemetry, tracking, and command (TT&C);
4. transmissions; and
5. end-of-life.

Livingstone and Lewis (2016) take a high-level approach to space cybersecurity, discussing topics such as cyber threats and risks to satellite infrastructure, as well as challenges and trends in the industry. However, the paper is directed toward a general audience so is not guided by existing taxonomies, and hence does not serve the purpose of a foundational academic text. It also is limited to cyber threats alone, which forms only one threat type that a space security practitioner must be aware of.

Finally, a comprehensive paper by Pavur and Martinovic (2020) details the cybersecurity threats to satellites and examines over 100 significant satellite hacking incidents over the past 60 years. The paper identifies four sub-domains that satellite cybersecurity applies to: satellite radio-link security, space hardware security, ground station security, and operational/mission security. They comment on the cross-disciplinary nature of space security but, perhaps due to their narrow focus on cybersecurity, stop short of treating space security as a separate domain in its own right.

A few other papers touch on the subject (Hannan, 2018; Ikitemur et al., 2020; Kallberg, 2012; Kang et al., 2018; Santamarta, 2014) but are specific to niche technologies or formal methods and hence do not adequately lay the foundations for future research on space systems security as a holistic domain. It is important to note that this literature review was only conducted across open-source English resources, not only skewing the threat context to a Western bias, but also excluding any additional or conflicting research that may exist within classified archives.

3. The Space Context

Space is the next frontier for human civilisation. Humans have long relied on space infrastructure for the advancement of technologies here on earth, with such dependencies becoming more and more critical. We are now even on the path toward developments such as extra-terrestrial colonisation, space mining, and other feats that were unimaginable a mere three generations ago.

3.1 Space Infrastructure

CSI can be broken down into five key categories (Georgescu et al., 2019):

- Remote Sensing;
- Communications;
- Meteorological;
- Global Navigation Satellite Systems (GNSS); and
- Administrative and Legislative Frameworks.

The technologies covered by the above are predominantly artificial satellites, but may also include space stations, rovers and vehicles, rockets, space probes, ground stations, and terrestrial communications links. Naturally each of these systems have various unique processes, technologies, and vulnerabilities.

Remote sensing involves the passive or active collection of data about a subject of study without making physical contact. Space infrastructures that fall under this category include systems that conduct surveillance, scientific monitoring, or information gathering for things like terrain mapping and military reconnaissance. These kinds of systems are particularly vulnerable to laser attacks as they allow for electromagnetic penetration to achieve their primary function (Georgescu et al., 2019).

Communications Satellites (ComSat) provide global telecommunications coverage and are useful for aviation and long-distance connections where earth's curvature inhibits the line of sight; communications which, if interrupted, could result in significant loss of life here on earth. A study done by Steinberger at the US Joint Electronic Warfare Center found that the most vulnerable component of satellite communications infrastructure is the antenna, which exposes the satellite to attacks such as jamming or spoofing (Steinberger, 2008). The earth segment was also found to be particularly vulnerable to jamming, but also to threats stemming from internet connectivity.

Meteorological space infrastructures are generally used to monitor earth's climate and weather and are critical for tasks like extreme weather prediction and monitoring. These satellites are generally quite minimal in build, as their primary purpose is simply to transmit photos and meteorological data to earth. There is yet to be any published research specific to meteorological satellite vulnerabilities, however due to their simple anatomy it can be inferred that they likely share general commonalities with other satellite systems.

GNSS includes navigation, positioning, and timing applications, and is perhaps most recognisable in satellite technologies such as the Global Positioning System (GPS). GNSS are heavily relied on by terrestrial applications such as the electric grid and guided weapons systems, whereby a satellite failure could cause far-reaching and catastrophic consequences, including loss of life. Due to the relatively long history of such systems, satellites delivering GNSS capabilities have been privy to greater levels of security research compared to other space-based systems. Across the literature, jamming and spoofing surface as the primary vulnerabilities of GNSS (Ioannides et al., 2016; de Abreu Faria et al., 2016; Amin et al., 2016).

Administrative and Legislative Frameworks are undoubtedly a quintessential component of CSI and are also notably immature at this point in time (Planck, 2009). A growing number of countries around the world are recognising space systems as Critical National Infrastructure (CNI) and hence the administrative and legal frameworks to support them are gaining global attention and prioritisation. One notable example is The Woomera Manual project, which is an international research collaboration to articulate existing international laws applicable to military space operations (Stephens, 2021). Space as a legal domain is notoriously complex due to its international significance and lack of any divisible territory (del Monte, 2013). For space security purposes this category functions as more of a supporting component because, although frameworks are not targetable by a threat actor, they can aid in pre-emptive security efforts, data collection and retention standards, post-compromise forensics, and attribution, prosecution and retaliation.

3.2 Threat Landscape

Space systems operate in one of the most naturally hostile environments known to man, constantly facing threats such as electromagnetic radiation and space debris. In addition, systems deployed in space also face a variety of unique challenges that don't commonly apply to terrestrial infrastructure, such as lack of redundancy or maintenance options (Georgescu et al., 2019). Although non-malicious threats should definitely be considered when risk assessing space technologies, this is outside the scope of this paper.

When discussing targeted threats, it is helpful to break them down into three components (see Fig. 1): the actor, the vector, and the attack. The threat actor is the person or organisation behind the attack and can be assessed by considering their capability to conduct an attack versus their intent behind the attack. The threat vector refers to the vulnerable point of entry used by the threat actor to successfully carry out the attack; for example, if a ground system is air gapped (i.e., not connected to any network) then the threat vector may be a flash drive. Finally, the attack itself is the exploit used by the threat actor to achieve their objectives and cause the desired impact, for example malware or spoofing.

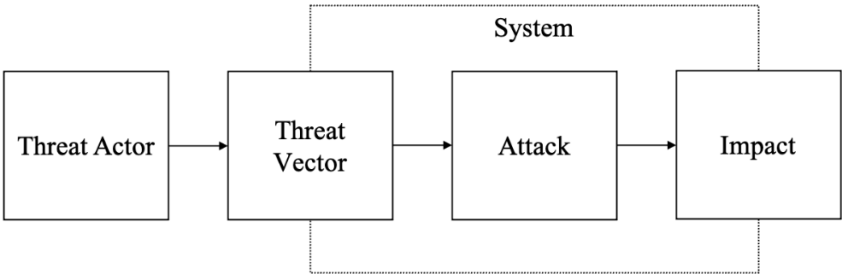

Figure 1: Anatomy of a targeted threat

Although a formal threat actor taxonomy is yet to emerge in the literature, a threat actor is generally categorised as one of the following: nation-state, terrorist, criminal group, or individual (e.g., insider threats, hacktivists, or bored teenagers) (Livingstone and Lewis, 2016). Sometimes hacktivism occurs on a larger scale (e.g., Anonymous) and can be treated as a separate category, conforming to neither terrorist nor criminal motivations. Bradbury et al. broke these high-level categories down further and provided space-specific examples, whereby each space-cyber actor has their own intent (e.g., goals and motivations) and capability (e.g., capabilities, environment, and resources) that drives their decision-making process when carrying out a targeted attack (Bradbury et al., 2020). Pavur and Martinovic produced a similar yet simpler version of this threat actor table, expanding beyond just cybersecurity considerations in Figure 2.

Attacker Type	Example Motivations	Technical Capabilities
National Military	• Space Control • Anti-Satellite Weapons	High
State Intelligence	• Counter-Intelligence • Technology Theft • Eavesdropping	High
Industry Insiders	• Sabotage • Technology Theft	High
Parts Suppliers	• Sabotage • Espionage	High
Organized Crime	• Eavesdropping • Ransom • Technology Theft	Moderate
Commercial Competitors	• Sabotage • Technology Theft	Moderate
Terrorists	• Societal Harm • Notoriety • Message Broadcasting	Low
Individuals	• Notoriety • Personal Challenge	Low
Political Activists	• Message Broadcasting	Low

Figure 2: Summary of Satellite Threat Actors by Pavur and Martinovic, 2020

Threat vectors need to be assessed on a case-by-case basis, however there are four common attack surfaces for deployed space systems (Wheeler et al., 2018):

- inputs (e.g., sensors and RF antennae);
- outputs (e.g., telemetry transmitters);
- internal communications (e.g., Spacewire buses); and
- computing (e.g., the internal system that integrates each component).

Each of these components can be accessed via a myriad of different threat vectors, such as through ground segments, supply chains, unsecured communications links, and countless other avenues. Bradbury et al. propose a handy reference architecture for assessing space system threat vectors and attack surfaces in their 2020 IEEE Aerospace Conference paper (Bradbury et al., 2020).

Targeted attacks to space infrastructure can be broken down into: kinetic physical, non-kinetic physical, electronic, and cyber; as per the threat assessment published by Harrison et al. (Harrison et al., 2020). In this context both kinetic and non-kinetic physical threats aim to impact the physical components of a space system. The difference between the two is inherent in the title, with kinetic referring to tangible threats such as anti-satellite (ASAT) missiles and non-kinetic referring to intangible threats such as lasers and EMP weapons. It is worth noting here that kinetic weapons are particularly risky as any ensuing space debris can cause cascading failures, where one collision leads to the next and suddenly a large number of satellites are transmorphed into space junk; including unintended targets (Wright et al., 2005).

Electronic threats do not aim to have a permanent physical impact, and so are not to be confused with non-kinetic physical threats that do. An electronic threat generally involves interfering with RF signalling, for example signal jamming or spoofing, to interfere with the availability or integrity of communications, with the consequences to the space infrastructure itself usually being temporary.

Finally, cyber threats seek to interfere with the confidentiality, integrity, or availability of space infrastructures through the manipulation of data and code. Cyber threats are the most flexible of the categories, with a wide range of malicious options and outcomes available to the adversary (Plotnek and Slay, 2021a). Cyber attacks are rapidly growing in occurrence and severity due to their accessibility, affordability, and the increased level of control an actor has over the impact compared to alternative forms of attack. As such, cyber attacks deserve special attention when researching threats to space systems. The Cyber Kill Chain is a conceptual model invented by Lockheed Martin to understand the various stages of a cyber attack (i.e., reconnaissance, weaponization, delivery, exploitation, installation, command & control, and actions on objectives), and helps to analyse attacks and attack vectors for prevention and incident response. In their 2021 conference paper Van der Watt and Slay adapted the Cyber Kill Chain model to Low Earth Orbit (LEO) satellites; a helpful reference when discussing cyber threats to space infrastructure (van der Watt and Slay, 2021).

3.3 Past Events

Unfortunately, secrecy clouds public access to information about incidents to critical infrastructure, leaving the idea of space systems security to the imagination of Hollywood. The lack of academic research in the field only exacerbates the fallacy that space security is a hypothetical need. Pavur and Martinovic (2020) conducted a study of historical satellite hacking incidents and identified 116 significant events since Sputnik, with the first occurring in 1986.

The first few years of space attacks saw a heavy focus on piracy and spoofing, with satellite imagery data being eavesdropped to avoid subscription fees and television streams being hijacked to broadcast unsolicited messages. A noteworthy example is the 1987 hack conducted by an employee of the American Christian Broadcasting Network who transmitted unauthorised biblical messages over the Playboy Channel's planned broadcast. The 1990s saw a move towards signal jamming, with commercially available satellite jammers being produced and state actors such as the US, Iran, Indonesia, and Russia carrying out various jamming operations.

The use of commercial and state-sponsored jamming, signal hijacking, laser attacks, malware, eavesdropping, and other increasingly sophisticated attacks have been becoming more and more common (Pavur and Martinovic, 2020). In 2007 China even compromised two NASA satellites via the ground station, taking complete control over their flight signalling (Bardin, 2013). That same year China also demonstrated a kinetic ASAT weapon

against one of their own satellites, producing hundreds of pieces of dangerous space debris along with it, and playing a role in the onset of the second space race that we are witnessing today (Zissis, 2010).

There are many more examples of malicious threats to space infrastructure that solidify the need for space security. Appendix A of Pavur and Martinovic's paper contains a comprehensive list of past cyber attacks on satellite infrastructure (Pavur and Martinovic, 2020).

3.4 Looking Towards the Future

Where the first space race cemented space systems as critical infrastructure, the second space race is shifting the focus from government to commercial interests. According to Livingstone and Lewis (2016), the next decade or so will see system-on-a-chip avionics, self-optimizing autonomous systems, complex on-board satellite processing, autonomous satellite-to-satellite (S2S) communications, plus a number of complex software additions. Each technological advancement introduces new vulnerabilities that could be exploited, producing unseen effects. For example, consider a futuristic piece of worm-like malware that corrupts a satellite connected via an autonomous S2S system – the entire fleet could be compromised and potentially rendered unserviceable after a single infection.

Alongside this resurgence in the rapid development of space systems, all kinds of new threats are emerging. Talk of cyber warfare, cyber terrorism, and cyber crime are increasing and so are the capabilities of motivated threat actors (Plotnek and Slay, 2021b). Both cyber and electronic weapons are becoming more effective and accessible by the day, with at least 120 different countries already invested in cyber warfare capabilities (McAfee, 2005).

Mass-scale environmental and political events may also impact humankind's reliance on CSI, which could cause unforeseeable impacts. For example, hazardous asteroids heading for earth (O'Neill and Handal, 2021) or the growing threat of climate change, both of which are tracked and assessed using space infrastructure – a reliance that may evolve and become more critical as time goes on. Another example might be a third eruption of world warfare. Military equipment has become increasingly reliant on satellite technology and such a situation may over-burden aging infrastructure and cause denials of service in critical moments. On a similar tangent, the United States has officially approved the establishment of a Space Force to directly counter these threats (Farley, 2020) and many other countries are likely to follow suit, events that will undoubtedly impact the space security domain in the coming decades.

4. The Case for Space Systems Security

With an understanding of the criticality of space infrastructure, its deepening vulnerability issues, and the unpredictable threat environment within which it is situated, it is easy to see the importance of space security. Unfortunately, up until now there has been little recognition or structure afforded to the complex domain of space systems security. In fact, there even exists some hostility towards security research within the space industry (CSRIC, 2015), a culture that could impede the advancement of space development altogether.

The second space race has sparked a period of rapid development and deployment, which presents significant complications without a unified understanding of the domain's research problems for efficient prioritisation and collaboration. The current lack of direction and common purpose has led to a double-up in the limited research available, with each contributing discipline evidently taking a siloed approach to space security terminology and taxonomy. Additionally, unlike a lot of other critical infrastructures space has direct military applications, meaning that efficient research and development is crucial for national security objectives such as effective threat deterrence and space superiority.

The kind of efficiency needed to compete in the volatile arena of this new space race is only made possible through wider recognition of space systems security as a specialist inter-disciplinary domain, where each contributing field has a valid voice for enhanced collaboration.

5. Research Opportunities

Pulling together the different research threads identified in Section 2 paints a picture of the current state of space security as a domain and highlights areas needing further development, as shown in Figure 3. As can be seen, we have a preliminary understanding of attack surfaces, threats, and actors, as well as past events and

future predictions, which are not shown in the diagram. Findings in these areas should be verified and formally defined and taxonomised to ensure cross-disciplinary consistency and to aid collaboration.

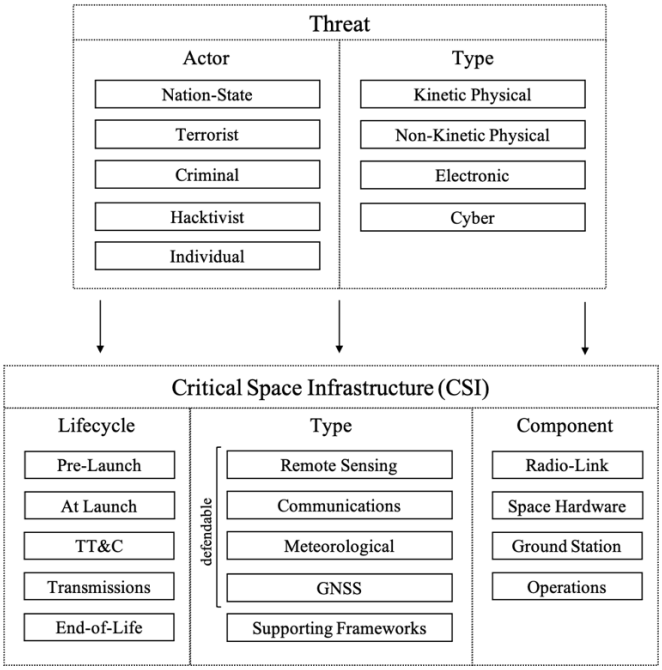

Figure 3: Threats to CSI broken down into taxonomical sub-categories as per available literature

Expanding on Harrison et al. we can class malicious (i.e., non-environmental) space threats under four categories: kinetic physical, non-kinetic physical, electronic, and cyber (Harrison et al., 2020). These four categories are more descriptive for general security use compared to the three law-driven categories (kinetic, virtual, and hybrid) proposed by Housen-Couriel in their earlier paper (Housen-Couriel, 2016), however more research may be required to determine a universally robust space threat taxonomy. In that same paper, Housen-Couriel identifies five stages of satellite operations, which should be confirmed by satellite engineering academia and analysed from a mission security perspective.

With a clear idea of the current state of literature it becomes easier to see where research should be focused in future. Firstly, space systems security should be formally defined and taxonomised according to the in-scope domains or high-level sub-topics. A research roadmap should then be developed that identifies the fundamental objectives of space systems security as a formal domain, the key stakeholders to the problem of space systems security (i.e., contributing specialisations), and how each stakeholder interacts across each taxonomical sub-domain and objective.

6. Conclusions

Far from a hypothetical consideration, vulnerable space infrastructures have already experienced a plethora of significant security events and this will only increase in frequency and impact looking towards the high-tech and interconnected future of space flight. Earth-based societies are already dependent on space infrastructure and face dire consequences without the proper consideration of space systems security.

This paper has established a contextualised foundation for space systems security drawn from existing cross-disciplinary literature on the subject. Additionally, it was found that wider recognition of space systems security as a specialist inter-disciplinary domain is needed to break down disciplinary silos, enhance collaboration, and unify definitions, taxonomies, and research objectives. Finally, the paper painted a picture of the current state of space systems security research and drew from this to propose a direction for future research.

References

Amin, M.G., Closas, P., Broumandan, A., Volakis, J.L., 2016. Vulnerabilities, threats, and authentication in satellite-based navigation systems [scanning the issue]. Proceedings of the IEEE 104, 1169–1173. https://doi.org/10.1109/JPROC.2016.2550638

Bardin, J., 2013. Satellite Cyber Attack Search and Destroy, in: Computer and Information Security Handbook. Elsevier Science & Technology, pp. 1093–1102.

Bradbury, M., Maple, C., Hu, Y., Ugur, I.A., Cannizzaro, S., 2020. Identifying Attack Surfaces in the Evolving Space Industry Using Reference Architectures, in: 2020 IEEE Aerospace Conference. Presented at the 2020 IEEE Aerospace Conference, IEEE, USA, pp. 1–20. https://doi.org/10.1109/AERO47225.2020.9172785

CSRIC, 2015. Cybersecurity Risk Management and Best Practices Working Group 4: Final Report (Working Group No. 4). The Communications Security, Reliability and Interoperability Council, U.S.A.

de Abreu Faria, L., de Melo Silvestre, C.A., Correia, M.A.F., 2016. GPS-Dependent Systems: Vulnerabilities to Electromagnetic Attacks. Journal of Aerospace Technology and Management 8, 423–430. https://doi.org/10.5028/jatm.v8i4.632

del Monte, L., 2013. Towards a cybersecurity policy for a sustainable, secure and safe space environment, in: Proceedings of the 64th International Astronautical Congress (IAC).

Donnelly, D., 2021. War fears as China vows punishment on Australia for Taiwan support - Long-range strikes. Express.

Farley, R., 2020. Space Force: Ahead of Its Time, or Dreadfully Premature? CATO Institute Policy Analysis 904.

Georgescu, A., 2020. Critical Space Infrastructures, in: Schrogl, K.-U., Hays, P.L., Robinson, J., Moura, D., Giannopapa, C. (Eds.), Handbook of Space Security. Springer, New York, United States of America, pp. 227–244.

Georgescu, A., Gheorghe, A.V., Piso, M., Katina, P.F., 2019. Critical Space Infrastructures: Risk, Resilience and Complexity, Topics in Safety, Risk, Reliability and Quality. Springer, Switzerland.

Hannan, N., 2018. An Assessment of Supply-Chain Cyber Resilience for the International Space Station. The RUSI Journal 163, 28–32. https://doi.org/10.1080/03071847.2018.1469249

Harrison, T., Johnson, K., Roberts, T.G., Way, T., Young, M., 2020. Space Threat Assessment 2020. Center for Strategic & International Studies, Washington, United States.

Housen-Couriel, D., 2016. Cybersecurity threats to satellite communications: Towards a typology of state actor responses. Acta Astronautica 128, 409–415. https://doi.org/10.1016/j.actaastro.2016.07.041

Ikitemur, G., Karabacak, B., Igonor, A., 2020. A Mixed Public-Private Partnership Approach for Cyber Resilience of Space Technologies, in: Space Infrastructures: From Risk to Resilience Governance, NATO Science for Peace and Security Series - D: Information and Communication Security. IOS Press, pp. 120–130.

Ioannides, R.T., Pany, T., Gibbons, G., 2016. Known Vulnerabilities of Global Navigation Satellite Systems, Status, and Potential Mitigation Techniques. Proceedings of the IEEE 104, 1174–1194. https://doi.org/10.1109/JPROC.2016.2535898

Kallberg, J., 2012. Designer Satellite Collisions from Covert Cyber War. Strategic Studies Quarterly 6, 124–136.

Kang, M., Hopkinson, K., Betances, A., Reith, M., 2018. Mitigation of Cyber Warfare in Space Through Reed Solomon Codes. Presented at the 13th International Conference on Cyber Warfare and Security, acpi, Washington DC, United States.

Kaspersky Lab, I.C., 2019. Threat Landscape for Industrial Automation Systems. Kaspersky Lab, ICS CERT.

Livingstone, D., Lewis, P., 2016. Space, the Final Frontier for Cybersecurity? Chatham House.

Mayence, J.-F., 2010. Space security: transatlantic approach to space governance, in: Robinson, J., Schaefer, M., Schrogl, K.-U., von der Dunk, F. (Eds.), Prospects for Transparency and Confidence-Building Measures in Space. ESPI, Vienna, Austria, p. 35.

McAfee, 2005. McAfee Virtual Criminology Report: North American Study into Organized Crime and the Internet. McAfee.

Moltz, J.C., 2011. The Politics of Space Security: Strategic Restraint and the Pursuit of National Interests, Second. ed. Stanford University Press, California, United States of America.

O'Neill, I.J., Handal, J., 2021. https://www.jpl.nasa.gov/news/nasa-analysis-earth-is-safe-from-asteroid-apophis-for-100-plus-years. NASA Jet Propulsion Laboratory.

Pavur, J., Martinovic, I., 2020. SOK: Building a Launchpad for Impactful Satellite Cyber-Security Research. eprint arXiv:2010.10872.

Planck, M., 2009. Air and Space Law, in: Max Planck Institute for Comparative Public Law and International Law, World Court Digest (Formerly Fontes Iuris Gentium). Springer, Berlin, Heidelberg.

Plotnek, J.J., Slay, J., 2021a. Cyber terrorism: A homogenized taxonomy and definition. Computers & Security 102, 102145. https://doi.org/10.1016/j.cose.2020.102145

Plotnek, J.J., Slay, J., 2021b. Satellite Cyber Resilience Whitepaper. SmartSat CRC, Adelaide, Australia.

Santamarta, R., 2014. SATCOM Terminals: Hacking by Air, Sea, and Land. IOActive, United States of America.

Schrogl, K.-U., Hays, P.L., Robinson, J., Moura, D., Giannopapa, C. (Eds.), 2020. Handbook of Space Security. Springer, New York, United States of America.

Sheehan, M., 2020. Defining Space Security, in: Schrogl, K.-U., Hays, P.L., Robinson, J., Moura, D., Giannopapa, C. (Eds.), Handbook of Space Security. Springer, New York, United States of America, pp. 7–21.

Steinberger, J.A., 2008. A Survey of Satellite Communications System Vulnerabilities. Joint Electronic Warfare Center, United States.

Stephens, D., 2021. The Woomera Manual [WWW Document]. URL https://law.adelaide.edu.au/woomera/ (accessed 3.29.21).

UCS, 2020. Union of Concerned Scientists Satellite Database [WWW Document]. Union of Concerned Scientists. URL https://ucsusa.org/resources/satellite-database (accessed 12.16.20).

USDoD, 2015. Space Domain Mission Assurance: A Resilience Taxonomy. Office of the Assistant Secretary of Defense for Homeland Defense & Global Security, United States.

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.

Wheeler, W.A., Cohen, N., Betser, J., Ewart, R.M., 2018. Cyber Resilient Flight Software for Spacecraft, in: AIAA SPACE and Astronautics Forum and Exposition. American Institute of Aeronautics.

Wright, D., Laura, G., Lisbeth, G., 2005. The Physics of Space Security: A Reference Manual. American Academy of Arts and Sciences, Cambridge, United States of America.

Zissis, C., 2010. China's Anti-Satellite Test. Council on Foreign Relations.