Coming Back Down to Earth: A Grounded Look at Space Cybersecurity in Southeast Asia

Shantanu Sharma
Center of Excellence for National Security, S. Rajaratnam School of International Studies, Singapore

shantanu.sharma@ntu.edu.sg

Abstract: This paper aims to open discussion regarding the absence of cybersecurity efforts for space systems in Southeast Asia and its implications. Although there is a consensus on the need for action, Southeast Asian states have not taken any concrete steps to address the challenge of space cybersecurity. Lacking sovereign capabilities, regulatory structures, and initiatives to tackle complex accidents that are waiting to happen, Southeast Asia is not adequately equipped to deal with the growing risk of attack on its space ecosystem. With increasing militarization of space programs, exponentially growing dominance of private sector, and reduced barriers of entry for malicious non-state actors, delaying any action for strengthening space cybersecurity can produce detrimental impact given the necessity of space sector for civil, commercial, and national sustenance in the region. Southeast Asia is in a unique position where the nascency of space sector and lack of rigid structures allows flexibility to learn, translate, and adapt existing initiatives and frameworks. To be on a path to bridge the gap between reality and the ideal, the region should focus on articulating principles and guidelines. The author proposes realistic policy recommendations and directions Southeast Asian states and the region at-large should pursue for promoting medium and long-term sustainability and usability, and for maintaining cybersecurity of space assets.

Keywords: Space, Cybersecurity, Southeast Asia, Cyber threat, Satellite

1. Introduction: "New Space" and New Opportunities

A renaissance in the space industry over the past few decades, driven by technology innovation, private sector investment, entrepreneurial activities, and diminished launch cost, has resulted in affordability and "democratization of space" (Wesler IV 2016). Outer space has become accessible not just to large enterprises and states but also to small state and non-state operators including start-ups and universities.

Technological miniaturization brought about by advancement in communication technologies and microelectronics have led to development of complex, smaller, and power efficient satellites. Furthermore, commercialization and global supply chains have produced an "assembly line" model for space system development. This has resulted in better access to foreign technologies (Upadhyay 2023), modern project management, agile production of modular commercial-off-the-shelf (COTS) components, payload specialization, shorter development process, and introduction of "as-a-Service" models.

Given its complex geography, space sector is a necessity for Southeast Asian states for civil, commercial, and national sustenance. States in the region use space systems to provide:

- earth observation for minerals, fisheries (The Economist 2023) and seasonal agricultural monitoring, disaster mitigation and management (Cowing 2023), and weather forecasting
- remote sensing and navigation for aviation and maritime sector
- telecommunications, internet (Raj 2023), and broadcasting for inaccessible islands in the archipelago.

Confronted with novel challenges like climate change, rising tensions in Taiwan Strait, increasing disputes in South China Sea, sudden shifts in supply chains (Tan 2023) due to friend-shoring and nearshoring, and growing digital population; interest in space sector have intensified in the region (Sarma 2019).

The current state of space ecosystem in Southeast Asia is fraught with fragmented capabilities and national objectives, and unequal legal and regulatory commitments (See Figure 1). Some states in Southeast Asia have established institutions and programmes, others are in the earliest stages of structuring their own. While no Southeast Asian state has an independent launch capability, five have national space programs – Indonesia, Malaysia, the Philippines, Thailand, and Vietnam. However, Brunei, Cambodia, Laos, and Myanmar have limited or no activities in space (Verspieren 2023). Whereas Singapore, geared towards a socio-economic angle, is active in developing its space sector despite not having a national agency.

Around the globe space systems have become deeply integrated with terrestrial digital infrastructure for global economic, militaristic, societal, and governmental activities. For many industries, space systems represent single point of failure (Falco 2018) with increasing relevance in countries' critical infrastructure (Carlo 2021).

Although Southeast Asia's space sector is still relatively nascent, threats to its space assets are no longer speculative. In June 2018, a campaign launched from China targeted companies in Southeast Asia and Unites States, infected satellite operators, defense contractors, and telecommunications companies with the aim to disrupt data traffic and change position of orbiting satellites (Menn 2018). The attack mounted did not cease until a year later. Indonesia, Malaysia, the Philippines, and Vietnam are just the latest victims of increasing attacks on space infrastructure in Southeast Asia (Symantec 2019).

Current literature focusing on space cybersecurity at-large do not consider nascency of space sector, fragmented capabilities, and disjointed objectives of states in Southeast Asia. Although, Verspieren (2022, 2023), Sarma (2019), Takahashi and Funabiki (2022), and Jones (2014) examine regional capabilities and structures and provide recommendations for encouraging growth of space ecosystem, the papers do not tackle security of space assets in the region. This paper therefore tries to fill the gap in current literature and aims to provide grounded policy recommendations that states in Southeast Asian should pursue to confront the growing cyber threat to space systems by leveraging their unique position and existing regional structures. The paper is structured as follows - after providing a brief overview of space ecosystem in Southeast Asia (Section 1), the paper details the importance of space system especially for military and national security (Section 2), the paper then focuses on challenges for implementing cybersecurity measures for space systems (Section 3 and 4); and lastly, a realistic plan for developing space cybersecurity measures in Southeast Asia is explored (Section 5).

Table 1: Comparison between major space powers in Southeast Asia[1]

	Singapore	Indonesia	Malaysia	The Philippines	Thailand	Vietnam
National Space Agency (Year of establishment)	None	BRIN (since 2022) Previously: LAPAN (1963)	MYSA (2019) Previously: ANGKASA (2002)	PhilSA (2019)	None. Consortium of 3 space related institutions including GISTDA (2000)	None. 2 Space-related institutes – STI (2006) and VNSC (2011) – under Vietnam Academy of Science and Technology
National Space Council (Years active)	None	None. Previously: DEPANRI (1963-2014)	None	Philippines Space Council (2019- Present)	None	None
National Space Law	None	Law no. 21 of 2013 on Space Activities	None	Philippines Space Act (2019)	None	None
National Space Policy or Strategy (Latest)	None	Presidential Regulation no. 45 of 2017 concerning the Master Plan for Space Activities (2016-2040)	National Space Policy 2030 (2017)	Philippines Space Development and Utilization Policy (2019)	National Space Master Plan 2017-2036	Strategy of Space Science and Technology Development and Application to 2030 (2021)
UN Space Treaties Ratified and Signed	Ratified: OST, ARRA, LIAB Signed: REG	Ratified: OST, ARRA, LIAB, REG	Signed: OST, ARRA	Ratified: MOON Signed: OST, ARRA, LIAB	Ratified: OST, ARRA	Ratified: OST Signed: ARRA
Government Space Budget (2020, in million USD)	35	303	22	57	94	21
Independent Space Launch Capabilities	No	No	No	No	No	No
Launch Year of 1st Satellite At Least Partially Made by Nationals	2011 (X-SAT)	2007 (LAPAN-TUBSAT)	2000 (TiungSAT-1)	2016 (DIWATA-1)	1998 (THAI-PAHT)	2013 (PicoDragon)
Launch Year of 1st Domestically Produced Satellite	2011 (X-SAT)	2015 (LAPAN-A2)	2023 (A-SEANSAT-PG 1)	None	None	2013 (PicoDragon)

2. Militarization of Space: Space for Defense and Defense for Space

Lower barrier of access to space has led to increasing number of satellites with multiplication and diversification of actors and their objectives have resulted in unprecedented proliferation of outer space, leading to congestion of LEO and near saturation of the frequency spectrum (De Neve 2022).

Space geopolitics mirrors Earth – there is a multipolar international order, intensifying tensions between competing powers, and the presence of commercial actors disrupting and increasingly dominating the space sector. Given the importance of space systems for sustenance, threat of degradation, disruption, and destruction by malign actors has become a national security issue and outerspace has become congested, contested, and competitive. To secure themselves, major powers are shoring up arsenal of counterspace weapons as a form of deterrence, leading to greater contestation and militarization of outer space.

A shift to multi-domain warfare strategies has increased the requirement for support from space-based platform for C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) (Verma 2023) capabilities and to obtain operational superiority against A2/AD (Anti-access/area denial) capabilities. This reliance on space systems has materialized as "space for defense" – with NATO declaring space

[1] Derived from (Verspieren 2022), (UNOOSA 2023), and (Ignatius 2023). Abbreviations: *BRIN* - National Research and Innovation Agency, *LAPAN* – National Institute of Aeronautics and Space, *MYSA* – Malaysia Space Agency, *ANGKASA* – National Space Agency, *PhilSA* – Philippines Space Agency, *GISTDA* – Geo-Informatics and Space Technology Development Agency, *STI* – Space Technology Institute, *VNSC* – Vietnam National Space Centre, *OST* - Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (Outer Space Treaty 1967), *ARRA* - Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space (Rescue Agreement 1968), *LIAB* - Convention on International Liability for Damage Caused by Space Objects (Liability Convention 1972), *REG* - Convention on Registration of Objects Launched into Outer Space (Registration Convention 1975), and *MOON* - Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (Moon Agreement 1979).

as the fifth operational domain (NATO 2023), and EU identifying space as a strategic domain (European Commission 2023).

Increasing operational dependence on space systems, both commercially and military owned, marks them as a target for an adversary trying to gain asymmetrical advantage. The issue was brought to the forefront during the Russian invasion of Ukraine. On 24 February 2022, a cyberattack on Viasat's KA-SAT satellite communication service was conducted by Russia, an hour before the ground invasion to cripple Ukrainian Army communications which relied on the satellite infrastructure. This also resulted in unanticipated consequences, affecting broadband services to tens of thousands of users in France, Hungary, Greece, Italy, Poland, and Germany, and affecting Enercon's remote monitoring and control access of 5,800 wind turbines (Poirier 2022).

Reliance on space systems also requires "defense for space". Following the United States, European states have reacted to threats in outerspace through militarization. Germany, Italy, and UK have established space commands (Rome 2021), and Spain and France (Machi 2022) have established air and space force, with more states to follow suit. US also introduced bipartisan Space Infrastructure Act to designate space sector to be the seventeenth critical infrastructure (Fortinsky 2023). A similar reaction, initiation of militarization of space program, is playing out in space-faring nations surrounding Southeast Asia – India (Kanwar et al. 2023), China (Stokes et al 2020), South Korea (Byun et al 2023), Japan (Kyodo News 2023), and Australia (Davis 2023).

3. Cyber and Space Infrastructure

Cyber counterspace activities is not foreign to Southeast Asia, despite states having minimal space assets and no active mega-constellations. Notably, in 1986, Indonesia was the first state accused of satellite eavesdropping violation (Pavur and Martinovic 2022); and in 1996, Indonesia was the first state to deliberately use a satellite for signal jamming another satellite (Fergusson and Wong 2010).

Due to extreme and unexpected environmental conditions in space and interference arising from ground-to-satellite communication (Pultarova 2023), it is challenging to distinguish unintentional failure or hardware malfunction from electronic and cyber-attacks (Wheeler et al. 2018). This results in lack of direct attribution to an attacker, providing political maneuverability for the attacker which can help evade any direct retaliation, escalation, or legal and political implications.

Challenges in attribution, possibility for deniability, controlled escalation, low operational cost and ease of access, ability to create reversible effects, and assurance of non-destructive attack below the threshold of armed conflict (Bingen, Johnson and Young 2023) make cyber-attacks on space systems stand out as the ideal option to create significant disruptions and instill damaging effect on military, commercial, and civilian operations.

Ambiguities in international cyber policies, regulations, and standards, exacerbated by shortcomings and creation of harmful technical knowledge gaps in adaptation of guidelines from terrestrial cyber assets to space cyber assets; creates an ideal space for adversaries to operate in and exploit (Pavur and Martinovic 2022). To date, almost 30 countries, including many non-spacefaring nations, have demonstrated some degree of cyber-offensive counterspace capabilities (Pavur and Martinovic 2022).

4. The Challenge of Space Cybersecurity

Increased digitalization through advanced on-board processing, software defined radios (SDRs), packet-based protocol, and cloud enabled high-performance computing has led to rapidly expanding attack surface available for cyberattacks on space systems. This has resulted in a significant spike in attacks like eavesdropping (DEFCON Conference 2020), malware injection (Francis 2022), and jamming (Laursen 2023), and also increased significant risk of backdoor, denial of service, and hijacking attacks (Hadley 2023). Even cyberattacks instigated by non-state actors and even independent hackers have risen in frequency, complexity, and magnitude (Rajagopalan 2019, Pavur and Martinovic 2022).

As satellites operate in challenging environments with different mission objectives, they require bespoke hardware to operate. Combined with proliferation of COTS components, a unique situation is created where vulnerabilities likely apply to many platforms but applying patches requires tailored modifications (Pavur 2021).

The loss of physical access to space assets after launch also limits the ability to perform upgrades, repairs, or audits. This translates to more acute security/performance trade-offs to be considered for space systems as compared to terrestrial systems. Satellites are highly constrained devices with limited power, fuel, and compute capabilities. Adopting stronger cybersecurity principles such as stronger encryption would incur bandwidth, storage, and compute cost, which would directly compete with core functionalities (Pavur and Martinovic 2022).

Since the value chain has evolved into a shared ownership model, security of space data and systems is a shared responsibility between satellite operators, carriers, and satellite manufacturers (Grady et al. 2022). With the blurring of boundaries due to inter-dependent multi-stakeholder collaboration, it is becoming increasingly difficult to clearly assign security ownership and impose regulations.

Taking note of the stacking complexities and vulnerabilities in space systems, militaries have also started building up cyber counterspace capabilities. For example, a CIA document leaked on Discord revealed Chinese build-up of sophisticated cyber weapons to target satellites which would allow China "to seize control of a satellite, rendering it ineffective to support communications, weapons, or intelligence, surveillance, and reconnaissance systems" (Srivastava, Schwartz and Sevastopulo 2023).

5. Next Steps for Southeast Asia: Leveraging Existing Structures

Southeast Asia currently finds itself in a unique position where the nascency of space sector and lack of rigid structures allows flexibility to learn, translate and adapt existing initiatives and frameworks put forth by more advanced space powers like USA, UK, Germany, China, India, Japan, and France. Exploiting this limited window of opportunity in a meaningful way would require collaboration, extending partnerships, strengthening existing initiatives, and aiming for regulations.

Walking the road towards concrete and clearly defined regulations require the first steps taken to be guidelines, norms, and principles, which are currently absent in Southeast Asia. It is vital to enshrine multistakeholder process at the heart of the norm development process. This requires engaging with the industry, international partners, and regional governments.

With international bodies like the UN OEWG paralyzed due to geopolitics, countries are leaning towards minilateral arrangements. Regional-level forums to discuss space-related issue like Japan-led APRSAF (Asia-Pacific Regional Space Agency Forum), China-led APSCO (Asia-Pacific Space Cooperation Organisation), Spatial Information Corridor under China's Belt and Road Initiative, and norm-based US-led Artemis Accords do exist, but they are subject to the competitive geopolitical dynamics at play globally. Despite a handful of countries that are members, all Southeast Asian states are not fully represented in any forum. There is no mechanism for these different forums focused on Southeast Asia to consult, cooperate, or communicate with each other.

As existing Southeast Asian structures are not concrete enough to collaborate, states are relying on cooperation of international partners like China, Japan, India, and the US to help build space capabilities. For example, in March 2023, United States, Japan, Malaysia, and Thailand conducted multilateral military exercise responding to simulated space attack (Inoue and Shiga 2023). As the space sector is still nascent in Southeast Asia, it would be important to focus on low hanging fruits for capacity and knowledge building and raising awareness, like constructing win-win collaborations through peaceful uses of outerspace like humanitarian assistance and disaster relief (HADR) objectives (U.S. Department of State 2023) and creating data centres in the region to process and analyse earth observational data.

To promote medium and long-term sustainability, usability, and security of space, existing Southeast Asian structures need to be strengthened and collective action is required. ACICE (ASEAN Cybersecurity and Information Centre of Excellence) and SCOSA (ASEAN Sub-Committee on Space Technology and Applications) should be utilized to discuss and put-forth guidelines for space cybersecurity and translate existing international frameworks for the region. For confidence-building measures, communication, cooperation, and collaboration between APSCO and APRSAF should be encouraged. More regional coordination and centres for collaboration are needed. The collective, coordinated, and unified voice can be more impactful, especially in international processes like UN OEWG and Space-ISAC.

Provided below are some concrete recommendations for Southeast Asian states. These should serve as the foundation for creating guidelines, norms, and principles to strengthen the cybersecurity of space assets -

5.1 Fostering Talent

Space is an inherently cross-disciplinary field. Even established space powers, like Japan, with advanced capabilities and significant resource allocation, are facing talent shortage to meet the growing demand (Verspieren 2021). The unmet demand will result in Southeast Asian states cannibalizing talent off of each other which would dampen the space ecosystem. Cross-disciplinary training and objective-based exchanges are needed to sustainably foster talent, which can be achieved in the region through replicating examples of existing memorandum of understanding (Space Foundation 2022), cross-university efforts, international research

initiatives, and collaboration for peaceful operations (JICA 2021) like climate monitoring and HADR (Garekar 2023).

5.2 Enforcing Basic Cybersecurity Principles and Practicing Cyber Hygiene

Willbold et al. (2023) highlighted the abysmal state of space cybersecurity. They noted that basic cybersecurity principles are missing, and in practice operators were instead still relying on outdated 'security through obscurity'. They also highlighted lack of authentication protocols, broadcasting of signal without encryption, lack of penetration testing, and missing separation of code and data.

To cultivate cyber hygiene, organizational security culture, and to raise awareness, Southeast Asia states can follow the examples of NIST IR 8270, 8401, 8441 (Scholl and Suloway 2021, Lightman, Suloway, and Brule 2022, McCarthy et al. 2023), and especially of UK Space Cybersecurity Toolkit which provides information on potential cyber threats, cybersecurity standards to adopt, list of relevant authorities, reporting obligations and process, and outlines impact assessment methodologies (UK Space Agency 2020). States should also promote broad set of frameworks and basic security principles like Zero Trust Architecture framework (Easley 2023), DevSecOps (Leonard 2021), and end-to-end encryption (E2E) to reduce the attack surface.

5.3 Fixing Supply Chain Vulnerabilities

The supply chain has shifted towards open-source software and COTS hardware for faster, cheaper, scalable, and standardized space system manufacturing and deployment. This can lead space systems vulnerable to attacks like backdoors and code injection. Attack on supplier side is not uncommon. Maximum Industries, a SpaceX supplier, was hit with a ransomware attack on March 2023 (Greig 2023).

Since supply chain have become global, ideally countries should consider extending cybersecurity certification and labelling scheme to space hardware and software. Nevertheless, space ecosystem in Southeast Asia is still in early stages of development, imposing compliance on local small business and start-ups could create additional cost, and in-turn create an unfair advantage for established international players (Strohmier et al. 2022). However, it is important for states to list and impose vendor check and certification requirement for space systems being used in military or dual-use capacity. US CMMC 2.0 certification (U.S. Department of Defense 2021) requirement is an example that Southeast Asian states can replicate, especially for satellites required to operate in D3SOE (Denied, Degraded, and Disrupted Space Operational Environment) capacity. Thailand, which is considering using space technology for defense purposes, is already contemplating legislation to curb foreign influence in COTS production (Inoue and Shiga 2023).

5.4 Modernizing Legacy Hardware

Lack of physical access to space-borne assets creates a unique situation where it is impossible to maintain aging hardware. These legacy assets can prove as an easy entry point for attackers (Kallberg 2018). States in Southeast Asia should list and modernise their aging space systems, including ground systems, when possible (Erwin 2021).

5.5 National Security and the Private Sector

The role of commercially-owned satellites in critical government operations should prompt countries to start thinking about guidelines and regulations that prioritize security. After Russia's cyberattack on Ukrainian space infrastructure, Ukraine replaced many communication links using SpaceX's Starlink constellation for communication (Weeden and Samson 2023), intelligence gathering, and coordinating drone strikes (Satariano et al. 2023). In 2022, Elon Musk after conversation with Russian officials (Davis 2023), deactivated Starlink satellites near Crimea to prevent a Ukrainian offensive operation (Kim 2023), leading to loss of lives (Farrow 2023). The private sector has become increasingly important and disruptive, prompting national security concerns, and provoking a wide range of reactions. It is noted that 80% of US military communications rely on commercial satellites (Becht and Trompille 2019). Concerns about Starlink dominance has influenced the EU to launch its own 2.4 Billion Euros satellite constellation for civilian and military use (Kim 2023). Whereas countries like Japan (Umeda 2023) and United States (Schogol 2023) are exploring options to use SpaceX products for militaristic purposes.

The states in Southeast Asia can look towards 8 (EUR-Lex 2023) and Critical Entities Resilience Directive (European Parliament and The Council of the European Union 2022) as foundation for coming up with broader principles.

5.6 Creating Cybersecurity Testbeds

As there are limited number of satellite development centres in Southeast Asia, the region needs to develop replicable research testbeds for satellite platform exploitation. Testbeds allows for controlled and repeatable experiment, improves access to technology for researchers who do not own and operate satellites (Pavur and Martinovic 2022), and combined hands-on experience with educational courses allow for better training for engineers. Similar bug bounty and penetration testing program should be explored like those initiated by SpaceX (Duffy 2022); European Space Agency's CYSAT 2023, where researchers took control of ESA nanosatellite (Thales Group 2023); and DEF CON 2023 Hack-a-Sat (Antoniuk 2023), where a satellite was launched for first ever capture-the-flag competition on a space-borne asset (Vasquez 2023).

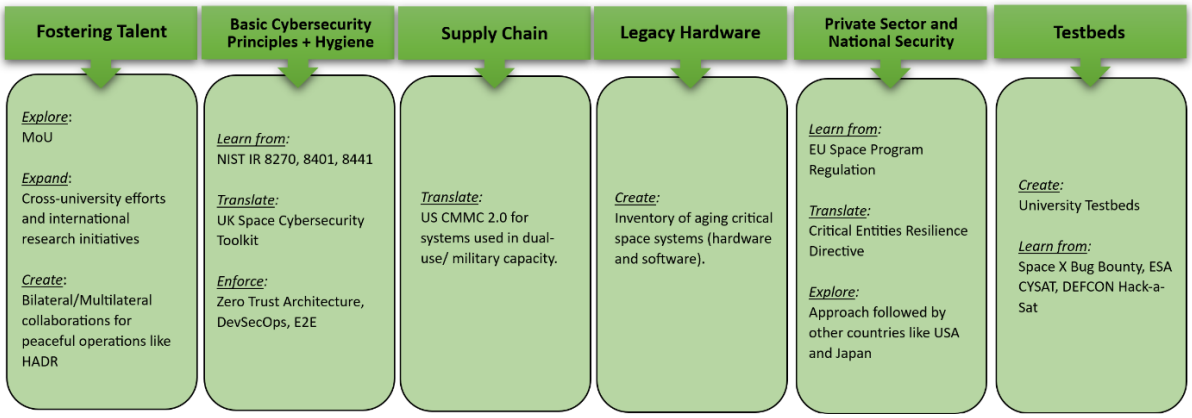

Figure 1: Summary of recommendations and directions Southeast Asian states should pursue

6. Conclusion

Around the globe space systems have become deeply integrated with terrestrial digital infrastructure for global economic, militaristic, societal, and governmental activities. The cyberattack on Viasat satellite brough the issue of cybersecurity of space assets to the forefront. States in Southeast Asia are not adequately equipped to deal with the growing risk of attack on their space ecosystem. However, Southeast Asia currently finds itself in a unique position where the nascency of space sector and lack of rigid structures allows flexibility to learn, translate and adapt existing initiatives and frameworks. Exploiting this limited window of opportunity in a meaningful way would require collaboration, extending partnerships, strengthening existing initiatives, and aiming for regulations. The paper provides some recommendations Southeast Asian states should pursue (See Figure 1) for increasing stability, strategic autonomy, building sovereign capabilities, and securing its space assets from cyberattacks. The recommendations provided should serve as foundation for creating guidelines, norms, and principles. Further research and dialogue are needed to create regulations and standards for cybersecurity of space assets.

Acknowledgement

The author would like to express his gratitude to Manoj Harjani (Research Fellow, IDSS, RSIS) for providing invaluable feedback and comments.

References

Antoniuk, D. (2023) "This new satellite enters orbit with one mission: To get abused by hackers", *Recorded Future*, 7 June. Available at: https://therecord.media/new-satellite-enters-orbit-to-get-hacked (Accessed at: 17 November 2023).

Becht, O. and Trompille, S. (2019) "Information report n°1574", *French Commission de la Défense Nationale et des Forces Armées*, pp. 70-71. Available at: https://www.assemblee-nationale.fr/dyn/opendata/RINFANR5L15B1574.html (Accessed at: 17 November 2023).

Bingen, K., Johnson, K. and Young, M. (2023). "Space Threat Assessment 2023", *CSIS*, pp. 5-7. Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-04/230414_Bingen_Space_Assessment.pdf (Accessed at: 17 November 2023).

Byun, C., Ahn, T., Choi, S. and Handberg, R. (2023) "Developing the Direction of Military Space Capabilities in South Korea." *Journal of Indo-Pacific Affairs*, *6*(4), pp. 106-112.

Carlo, A. (2021) 'Cyber threats to space communications: space and cyberspace policies', *Outer Space and Cyber Space: Similarities, Interrelations and Legal Perspectives*, pp.55-66.

Cowing, K. (2023) 'Satellite-based Disaster Early Warning Systems Can Improve Evacuation Measures In Remote Asian Communities', *SpaceRef*, 5 July. Available at: https://spaceref.com/newspace-and-tech/satellite-based-disaster-early-warning-systems-can-improve-evacuation-measures-in-remote-asian-communities/ (Accessed at: 15 November 2023).

Davis, C. R. (2023) "Elon Musk blocked Ukraine's access to Starlink near Crimea after speaking with Russian officials, biographer says", *Business Insider*, 8 September. Available at: https://www.businessinsider.com/elon-musk-blocked-ukraine-starlink-access-crimea-russia-war-putin-2023-9 (Accessed at: 17 November 2023).

Davis, M. (2023) "A higher place for space in the defence strategic review", *Australian Strategic Policy Institute The Strategist*, 8 May. Available at: https://www.aspistrategist.org.au/a-higher-place-for-space-and-the-defence-strategic-review/ (Accessed at: 16 November 2023).

De Neve, A. (2022) "Crowded and Dangerous Orbits: European Space Governance at a Time of Potentially Saturating Programs", *Notes de l'Ifri*, pp. 19-20. Available at: https://www.ifri.org/sites/default/files/atoms/files/a._de_neve_crowded_dangerous_orbits_feb_2022.pdf (Accessed at: 15 November 2023).

DEFCON Conference (2020) *DEF CON Safe Mode - James Pavur - Whispers Among the Stars.* Available at: https://www.youtube.com/watch?v=ku0Q_Wey4K0 (Accessed at: 16 November 2023).

Duffy, K. (2022) "SpaceX says researchers are welcome to hack Starlink and can be paid up to $25,000 for finding bugs in the network", *Business Insider*, 15 August. Available at: https://www.businessinsider.com/spacex-starlink-pay-researchers-hack-bugs-satellite-elon-musk-2022-8 (Accessed at: 17 November 2023).

Easley, M. (2023) "Space Force awards contract to protect space systems, data with zero-trust approach", *Defense Scoop*, 3 October. Available at: https://defensescoop.com/2023/10/03/space-force-xage-security-zero-trust/ (Accessed at: 17 November 2023).

Erwin, S. (2021) "Space Force grappling with aging infrastructure used to operate satellites", *Space News*, 19 September. Available at: https://spacenews.com/119100-2/ (Accessed at: 17 November 2023).

EUR-Lex (2023) *EU space programme (2021–2027) – European Union Agency for the Space Programme.* Available at: https://eur-lex.europa.eu/EN/legal-content/summary/eu-space-programme-2021-2027-european-union-agency-for-the-space-programme.html (Accessed at: 17 November 2023).

European Commission (2023) "EU Space Strategy for Security and Defence" Available at: https://defence-industry-space.ec.europa.eu/eu-space-policy/eu-space-strategy-security-and-defence_en (Accessed at: 15 November 2023).

European Parliament and The Council of the European Union (2022) DIRECTIVE (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC. *Off. J. Eur. Union*, *333*, p.164. ELI: http://data.europa.eu/eli/dir/2022/2557/oj

Falco, G. (2018) 'The vacuum of space cyber security', *AIAA SPACE and Astronautics Forum and Exposition*, p. 5278.

Farrow, R. (2023) "Elon Musk's Shadow Rule", *The New Yorker*, 21 August. Available at: https://www.newyorker.com/magazine/2023/08/28/elon-musks-shadow-rule (Accessed at: 17 November 2023).

Fergusson, J. and Wong, W.W. eds. (2010). *Military space power: a guide to the issues*. Bloomsbury Publishing USA.

Fortinsky, S. (2023) "Bipartisan bill designates space as critical infrastructure sector", *The Hill*, 27 July. Available at: https://thehill.com/homenews/space/4123413-bipartisan-bill-designates-space-as-critical-infrastructure-sector/ (Accessed at: 16 November 2023).

Francis, J. (2022) "Briefing 3: Wiper Malware: An Increasing Threat to Satellite and IoT Enabled Capabilities", *Kratos Defense Threat Briefing*, 12 December. Available at: https://www.kratosdefense.com/constellations/articles/threat-briefing-3-wiper-malware-an-increasing-threat-to-satellite-and-iot-enabled-capabilities (Accessed at: 16 November 2023).

Garekar, B. (2023) "Haze detection, aviation and maritime safety discussed in first S'pore-US space dialogue", *The Straits Times*, 13 October. Available at: https://www.straitstimes.com/world/ways-to-detect-haze-enhance-aviation-maritime-safety-discussed-in-first-s-pore-us-space-dialogue (Accessed at: 17 November 2023).

Grady, B., Camp, C. V., Muruganandham, S., and Placido, C. (2022) "Space Cybersecurity - Current State and Future Needs", *Northern Sky Research,* April, pp. 4-11. Available at: https://www.nsr.com/wp-content/uploads/2022/04/NSR-Space-Cybersecurity-White-Paper-FINAL.pdf (Accessed at: 17 November 2023).

Greig, J. (2023) "FBI, Air Force warn of cyberattacks on space industry by 'foreign intelligence operations'", *Recorded Future*, 19 August. Available at: https://therecord.media/fbi-warns-of-space-cyberattacks (Accessed at: 17 November 2023).

Hadley, G, (2023) "'Backdoor' to Attack Satellites: CSO Sees Cyber Risks in Space Force Ground Systems", *Air & Space Forces Magazine*, 31 January. Available at: https://www.airandspaceforces.com/backdoor-to-attack-satellites-cso-highlights-ground-networks/ (Accessed at: 17 November 2023).

Ignatius, C. (2023) "ANGKASA-X Launches First Homegrown Satellite", *BusinessToday Malaysia*, 28 June. Available at: (Accessed at: 20 January 2024)

Inoue, K., Shiga, Y. (2023) "Southeast Asia's space race chases wins in tourism, communications", *Nikkei Asia*, 11 May. Available at: https://asia.nikkei.com/Business/Aerospace-Defense-Industries/Southeast-Asia-s-space-race-chases-wins-in-tourism-communications (Accessed at: 17 November 2023).

JICA (2021) "Collaboration with JAXA to develop human resources in "Space Technology Utilization for SDGs" in Southeast Asia", 8 October. Available at: https://www.jica.go.jp/Resource/english/news/field/2021/20211008_01.html (Accessed at: 17 November 2023).

Jones, Z.P. (2014) *Southeast Asian space programs: motives, cooperation, and competition* (Doctoral dissertation, Monterey, California: Naval Postgraduate School). Available at: https://apps.dtic.mil/sti/tr/pdf/ADA619544.pdf (Accessed at: 20 January 2024).

Kallberg, J. (2018) "Why older satellites present a cyber risk", *C4ISRNET*, 29 December. Available at: https://www.c4isrnet.com/opinion/2018/12/28/why-older-satellites-present-a-cyber-risk/ (Accessed at: 17 November 2023).

Kanwar, V., Kapil, S., Suryavanshi, H., Reddy, K., and Chatterjee, C. (2022) "Space for defence in India", *PricewaterhouseCoopers and SatCom Industry Association India*, October, pp. 19-26. Available at: https://www.pwc.in/assets/pdfs/aero_defence/space-for-defence-in-india.pdf (Accessed at: 16 November 2023).

Kim, V. (2023) "Elon Musk Acknowledges Withholding Satellite Service to Thwart Ukrainian Attack", *The New York Times*, 8 September. Available at: https://www.nytimes.com/2023/09/08/world/europe/elon-musk-starlink-ukraine.html (Accessed at: 17 November 2023).

Kyodo News (2023) "Japan adopts space security policy, vows to expand defense use", 13 June. Available at: https://english.kyodonews.net/news/2023/06/caac42b9ada8-japan-adopts-space-security-policy-vows-to-expand-defense-use.html (Accessed at: 16 November 2023).

Laursen, L. (2023) "Satellite Signal Jamming Reaches New Lows", *IEEE Spectrum*, 18 May. Available at: https://spectrum.ieee.org/satellite-jamming (Accessed at: 16 November 2023).

Leonard, J. (2021) "DevSecOps in space: the challenges of updating satellites on-orbit", *Computing*, 10 June. Available at: https://www.computing.co.uk/analysis/4032657/devsecops-space-challenges-updating-satellites-orbit (Accessed at: 17 November 2023).

Lightman, S., Suloway, T., and Brule, J. (2022) "Satellite Ground Segment", *National Institute of Standards and Technology Interagency Report*, NIST IR 8401. Available at: https://doi.org/10.6028/NIST.IR.8401 (Accessed at: 17 November 2023).

Machi, V. (2022) "France puts space at top of national — and European — security priorities", *Defense News*, 14 March. Available at: https://www.defensenews.com/space/2022/03/14/france-puts-space-at-top-of-national-and-european-security-priorities/ (Accessed at: 14 November 2023).

McCarthy, J., Mamula, D., Brule, J., Meldorf, K., Jennings, R., Wiltberger, J., Thorpe, C., Dombrowski, J., Lattin, O.R. and Sepassi, S. (2023) "Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN)", *National Institute of Standards and Technology, NIST Interagency or Internal Report (IR) NIST IR*, *8441*(2023), p.28. DOI: 10.6028/NIST.IR.8441.

Meirizal, A. and Putri, D. J. (2022) "The Challenge of ASEAN Institutionalism in Outer Space", *ASEAN Studies Center Universitas Gadjah Mada*, 5 October. Available at: https://asc.fisipol.ugm.ac.id/2022/10/05/the-challenge-of-asean-institutionalism-in-outer-space/ (Accessed at: 20 January 2024).

Menn, J. (2018) 'China-based campaign breached satellite, defence companies – Symantec', *Reuters*, 20 June. Available at: https://www.reuters.com/article/us-china-usa-cyber/china-based-campaign-breached-satellite-defense-companies-symantec-idUSKBN1JF2X0 (Accessed at: 14 November 2023).

NATO (2023) "NATO's approach to space", 23 May. Available at: https://www.nato.int/cps/en/natohq/topics_175419.htm (Accessed at: 15 November 2023).

Pavur, J. (2021) *Securing new space: on satellite cyber-security* (Doctoral dissertation, University of Oxford), p. 26. Available at: https://ora.ox.ac.uk/objects/uuid:11e1b32a-8117-46b1-a0ce-9c485221d112 (Accessed at: 17 November 2023).

Pavur, J. and Martinovic, I., 2022. Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight. *Journal of Cybersecurity*, *8*(1), p.tyac008, https://doi.org/10.1093/cybsec/tyac008.

Poirier, C. (2022) "The war in Ukraine from a space cybersecurity perspective", *European Space Policy Institute Report*, 84, pp. 5-10. Available at: https://www.espi.or.at/wp-content/uploads/2022/10/ESPI-Report-84.pdf (Accessed at: 15 November 2023).

Pultarova, T. (2023) "GPS satellites threatened more by mild solar storms than monster sun flares", *Space.com*, 10 August. Available at: https://www.space.com/mild-solar-storms-threat-gps-satellites (Accessed at: 17 November 2023).

Rafikasari, A., Sumarlan, S. and Swastanto, Y. (2020) "Challenges and opportunities in strengthening ASEAN space technology cooperation", *The Indonesian Journal of Southeast Asian Studies*, *3*(2), pp.173-187.

Raj, A. (2023), 'Why internet from satellites in space work best in Southeast Asia', *TechWire Asia*, 23 June. Available at: https://techwireasia.com/2023/06/why-internet-from-satellites-in-space-work-best-in-southeast-asia/ (Accessed at: 15 November 2023).

Rajagopalan, R. P. (2019) *Electronic and cyber warfare in outer space*. Geneva: UNIDR. Available at: https://unidir.org/wp-content/uploads/2023/05/electronic-and-cyber-warfare-in-outer-space-en-784.pdf (Accessed at: 16 November 2023).

Rome, N. (2021) "European Militaries Join the U.S. in Space", *Georgetown Security Studies Review*, 7 April. Available at: https://georgetownsecuritystudiesreview.org/2021/04/07/european-militaries-join-the-u-s-in-space/ (Accessed at: 15 November 2023).

Sarma, N. (2019). 'Southeast Asian space programmes: Capabilities, Challenges and Collaborations', *ORF Special Report*, 82, pp. 13-15. Available at: https://www.orfonline.org/wp-content/uploads/2019/03/ORF_SpecialReport_82_SEA-Space.pdf (Accessed at: 15 November 2023).

Satariano, A., Reinhard, S., Metz, C., Frenkel, S. and Khurana, M. (2023) "Elon Musk's Unmatched Power in the Stars", *The New York Times*, 28 July. Available at: https://www.nytimes.com/interactive/2023/07/28/business/starlink.html (Accessed at: 17 November 2023).

Schogol, J. (2023) "Army combat advisors testing military version of Elon Musk's Starlink", *Task & Purpose*, 9 October. Available at: https://taskandpurpose.com/news/army-sfab-starshield-spacex-elon-musk/ (Accessed at: 17 November 2023).

Scholl, M. and Suloway, T. (2021) "Introduction to cybersecurity for commercial satellite operations", *National Institute of Standards and Technology, Tech. Rep*. DOI: 10.6028/NIST.IR.8270

Space Foundation (2022) "Space Foundation and Singapore Space & Technology Limited Sign Partnership Agreement", 21 September. Available at: https://www.spacefoundation.org/2022/09/21/space-foundation-singapore-space-technology-limited-partnership-agreement/ (Accessed at: 17 November 2023).

Srivastava, M., Schwartz, F. and Sevastopulo, D. (2023) "China building cyber weapons to hijack enemy satellites, says US leak", *Financial Times*, 21 April. Available at: https://www.ft.com/content/881c941a-c46f-4a40-b8d8-9e5c8a6775ba (Accessed at: 17 November 2023).

Stokes, M.A., Alvarado, G., Weinstein, E. and Easton, I. (2020). "China's Space and Counterspace Capabilities and Activities", *Project 2049 Institute and The U.S.-China Economic and Security Review Commission*, 30 March, pp.21-93. Available at: https://www.uscc.gov/sites/default/files/2020-05/China_Space_and_Counterspace_Activities.pdf (Accessed at: 16 November 2023).

Strohmier, H., Stoker, G., Vanajakumari, M., Clark, U., Cummings, J. and Modaresnezhad, M. (2022) Cybersecurity Maturity Model Certification Initial Impact on the Defense Industrial Base. *Journal of Information Systems Applied Research*, *15*(2), pp. 22-25.

Symantec (2019) *Thrip: Ambitious Attacks Against High Level Targets Continue*. Available at: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/thrip-apt-south-east-asia (Accessed at: 14 November 2023).

Takahashi, R. and Funabiki, N. (2022). Concrete Recommendations for Space Development in Non-spacefaring Countries. *ASEAN Space Programs: History and Way Forward*, pp.165-176.

Tan, H. (2023), 'Even Chinese companies are moving supply chains out China to avoid geopolitical risks. Here are the 6 places they're heading for instead.', *Business Insider*, 22 April. Available at: https://www.businessinsider.com/chinese-supply-chains-moving-companies-outside-mainland-2023-4 (Accessed at: 15 November 2023).

Thales Group (2023) *Thales seizes control of ESA demonstration satellite in first cybersecurity exercise of its kind*, 25 April. [Press release]. Available at: https://www.thalesgroup.com/en/worldwide/security/press_release/thales-seizes-control-esa-demonstration-satellite-first (Accessed at: 17 November 2023).

The Economist (2023) 'Keeping tabs on China's murky maritime manoeuvres', 15 August. Available at: https://www.economist.com/china/2023/08/15/keeping-tabs-on-chinas-murky-maritime-manoeuvres (Accessed at: 15 November 2023).

U.S. Department of Defense (2021) *Strategic Direction for Cybersecurity Maturity Model Certification (CMMC) Program,* 4 November. [Press release]. Available at: https://www.defense.gov/News/Releases/Release/Article/2833006/strategic-direction-for-cybersecurity-maturity-model-certification-cmmc-program/ (Accessed at: 17 November 2023).

U.S. Department of State (2023) *Joint Statement on U.S.-Singapore Space Dialogue,* 12 October. [Press release]. Available at: https://www.state.gov/joint-statement-on-u-s-singapore-space-dialogue/ (Accessed at: 17 November 2023).

UK Space Agency (2020) "Cyber Security Toolkit: Guidance on cyber security for space assets.", 19 May. Available at: https://assets.publishing.service.gov.uk/media/5ec298a3e90e071e2f955ebc/Space_cyber_toolkit_final_v4.pdf (Accessed at: 17 November 2023).

Umeda, K. (2023) "Satellite constellations taking on greater role in Japan's security", *The Japan Times*, 21 September. Available at: https://www.japantimes.co.jp/commentary/2023/09/21/japan/satellite-constellations-security/ (Accessed at: 17 November 2023).

UNOOSA (2023) "United Nations Office for Outer Space Affairs: Status of International Agreements Relating to Activities in Outer Space as at 1 January 2023". Available at: https://www.unoosa.org/res/oosadoc/data/documents/2023/aac_105c_22023crp/aac_105c_22023crp_3_0_html/AC105_C2_2023_CRP03E.pdf (Accessed at: 20 January 2024).

Upadhyay, S. N. (2023) 'Meet the Amazon for Space', *Analytics India Magazine*, 26 September. Available at: https://analyticsindiamag.com/meet-the-amazon-for-space/ (Accessed at: 15 November 2023).

Vasquez, C. (2023) "How a hacking crew overtook a satellite from inside a Las Vegas convention center and won $50,000" *CyberScoop*, 16 August. Available at: https://cyberscoop.com/mhackeroni-hackasat-space-def-con/ (Accessed at: 17 November 2023).

Verma, B. S. (2023) 'Rifle to Rafale: Space for defence', *ORF*, 22 September. Available at: http://20.244.136.131/expert-speak/rifle-to-rafale-space-for-defence (Accessed at: 15 November 2023).

Verspieren, Q. (2021) "Establishment of Space Operations Squadron at the Japan Air Self-Defence Force in 2020: current status and future prospects", *The Advanced Maui Optical and Space Surveillance Technologies* (*AMOS*) *Conference*, 22(3), pp. 1886-9. Available at: https://amostech.com/TechnicalPapers/2021/Poster/Verspieren.pdf (Accessed at: 17 November 2023).

Verspieren, Q. (2022) "Comparison of Established ASEAN Space Programs and Lessons Learned", *ASEAN Space Programs: History and Way Forward*, pp.125-127.

Verspieren, Q. (2023) 'ASEAN Space Programmes: Navigating Regional Rivalries', *RSIS Commentaries*, 008-23, pp. 1-2. Available at: https://www.rsis.edu.sg/rsis-publication/rsis/asean-space-programmes-navigating-regional-rivalries/ (Accessed at: 15 November 2023).

Weeden, B. and Samson, V. (2023) *Global counterspace capabilities: An Open Source Assessment*, Washington, DC: Secure World Foundation, pp. 13.06-13.12. Available at: https://swfound.org/media/207567/swf_global_counterspace_capabilities_2023_v2.pdf (Accessed at: 17 November 2023).

Wesler IV, W. (2016) 'The Democratization of Space', *RAND*, 28 March. Available at: https://www.rand.org/pubs/commentary/2016/03/the-democratization-of-space.html (Accessed at: 15 November 2023).

Wheeler, W.A., Cohen, N., Betser, J., Meyers, C., Snavely, W., Chaki, S., Riley, M. and Runyon, B. (2017) "Cyber resilient flight software for spacecraft", In *AIAA SPACE and Astronautics Forum and Exposition* (p. 5305). https://doi.org/10.2514/6.2018-5220.

Willbold, J., Schloegel, M., Vögele, M., Gerhardt, M., Holz, T. and Abbasi, A. (2023) May. "Space Odyssey: An Experimental Software Security Analysis of Satellites", *2023 IEEE Symposium on Security and Privacy (SP),* pp. 14-17. DOI: 10.1109/SP46215.2023.00131.