J. East Asia & Int'l L. Vol. 17/No.2 (2024); 405-422
Publication type : Research Article
Section : Notes & Comments
DOI : http://dx.doi.org/10.14330/jeail.2024.17.2.08

Cybersecurity Challenges in Outer Space: Innovation, Collaboration and Legal Reforms

Alya Hassan* & Abbas Sheer**

The increase in space activity has contributed to a convergence of cybersecurity and outer space at a critical moment in the digital era requiring a thorough examination of the threats to space-based assets and the protective measures required. As satellites and space technology become integral to global operations, their cyber security is paramount given their vulnerability to cyber espionage, interference and attacks. This paer highlights the significance of technological advancements and their dual role in improving space systems while also introducing new vulnerabilities. It explores varied national cybersecurity practices focusing on space stakeholders such as the US, the EU, China, Russia and UAE, revealing the global strategies employed against cyber threats. Moreover, the importance of laws and regulations such as the Outer Space Treaty in countering cyber attacks and emphasising the need for agile legal frameworks to address cybersecurity challenges in outer space is also examined. Moreover, the paper addresses complex issues of cybersecurity in outer space, particularly innovation, collaboration and legal reforms.

Keywords
Cybersecurity, Outer Space, Satellites, Space Technology Advancements, Legal Frameworks, Technological, International Law

* Legal Counsel of Emirates Integrated Telecom. Co. (attorney-at-law); LL.M. candidate in Air and Space Law at University of Sharjah College of Law. The author may be contacted at: U20104410@sharjah.ac.ae / Address: College of Law, University of Sharjah 27272, UAE.

** Assistant Professor at College of Law, University of Sharjah, UAE. LL.M. (FUUST, Pak.), Ph.D. (BIT, China). ORCID: https://orcid.org/0000-0002-3770-1164. The author may be contacted at: sheer.abbas@sharjah.ac.ae / Address: College of Law, University of Sharjah 27272, UAE.

All the websites cited in this article were last visited on November 17, 2024.

1. Background

The ditigal revolution in the twenty-first century has not only changed the cybersecurity concerns of the terrestrial world, but also stretched into the vastness of space. This juncture between cybersecurity and outer space operations represents a significant era in international security and space exploration. Therefore, a thorough investigation of the problems and solutions in securing space-based resources is a timely endeavour. Cybersecurity in outer space is important as satellites and space technology play a crucial role in global communications, navigation and defence systems, which are regarded as the prime targets for cyber threats.[1] With increasing commercialisation and militarisation of space, the cybersecurity of outer space has become a major concern requiring countermeasures to protect these assets from cyber espionage, interference and attacks.[2]

Empirical evidence has shown that the effect of new technologies on the future of cybersecurity in space is profound and fundamental. For instance, advancements in computing, miniaturisation and artificial intelligence (AI) have facilitated the development of more sophisticated and resilient space systems, which has resulted in developments in satellite technology. Moreover, the increasing number of satellites poses a new challenge for cybersecurity in space and requires the development of strong security protocols.[3] However, these innovations introduce new vulnerabilities as they expand the target for potential cyber threats. Thus, the rapid technological evolution in space systems demands an agile and forward-thinking approach to cybersecurity, emphasising the importance of continuous innovation in security measures to anticipate and mitigate emerging threats.[4]

Previously, the outer space and Earth-based networks were seen as two separate entities. However, they have now changed drastically into a complex web of dependencies. These space-based services are essential to such fields as the military, utilities, aviation and emergency response, rapidly becoming a critical point of contention for geopolitical disputes around the world.[5] This trend underscores the

1 James Pavur & Ivan Martinovic, *The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space*, *in* 11th Int'l Conf. on Cyber Conflict (CyCon) 1-18 (2019).

2 David Fidler, Cybersecurity and the New Era of Space Activities, Council on Foreign Relations (Apr. 2014), https://www.cfr.org/report/cybersecurity-and-new-era-space-activities.

3 Matthias Manulis et al., *Cyber Security in New Space*, 20(3) Int'l J. Info. Sec. 305 (2021).

4 Meg King & Sophie Goguichvili, Cybersecurity Threats in Space: A Roadmap for Future Policy, Wilson Center (Oct. 8, 2020), https://www.wilsoncenter.org/blog-post/cybersecurity-threats-space-roadmap-future-policy.

5 Algirde Pipikaite et al., *DAVOS AGENDA: Will the Battle for Space Happen on the Ground?*, World Econ. F. (May 25,

interconnected nature of modern infrastructure where the strategic importance of space extends far beyond its physical boundaries and directly influences key terrestrial operations. However, the effort to put cybersecurity practices in place in different countries is insufficient to obtain a full picture of the global scope of cybersecurity in outer space.[6] In this regard, the cybersecurity frameworks of Singapore and the contrasting approaches of the US and the UAE reveal various strategies and challenges in protecting space assets. Singapore's strategic initiatives in cybersecurity exemplify a proactive stance in bolstering defences against cyber threats, while the comparative analysis of the US and the UAE cybersecurity practices in space underscores the diverse methodologies that the nations adopted to overcome the complex domain of space cyber security.

Indeed, laws and regulations are critical in safeguarding space activity against cyber attacks. In this regard, international legal frameworks such as the Outer Space Treaty (OST) are required to lay foundational principles for the peaceful use of outer space.[7] However, the specificity and efficacy of these laws in addressing cyber threats to space assets remain topics of active debate and development. It is important to point out that international, regional and national cybersecurity regulations are crucial for protecting space activities, especially considering the interdependence of cyber and space domains. Therefore, a structured regulatory framework responsive to cyber threats is necessary.[8] Besides, the OST and subsequent international agreements provide the legal framework that partially addresses cybersecurity in space by imposing state responsibility for countries' exploration in outer space including liability for the damage caused by space objects. These provisions could include cyber operations against space assets.[9]

However, cybersecurity in outer space demonstrates a new developing area in which technology, law and international security intersect. As dependence on space-based technologies increases, the development of comprehensive cybersecurity measures that can handle the ever-changing threats to it also becomes apparent. Moreover, collaboration between nations, the adoption of novel technologies, and

2022), https://www.weforum.org/agenda/2022/05/increased-cybersecurity-for-space-based-services.

6 João Serra, *Cybersecurity and Outer Space: Learning from Connected Challenges*, *in* Outer Space and Cyber Space 1-24 (Annette Froehlich ed., 2021).

7 Jana Robinson, *Governance Challenges at the Intersection of Space and Cyber Security*, Space Rev. (Feb. 15, 2016), https://www.thespacereview.com/article/2923/1.

8 Anne-Sophie Martin, *Outer Space, the Final Frontier of Cyberspace: Regulating Cybersecurity Issues in Two Interwoven Domains*, 21(1) Astropolitics 1-22 (2023).

9 Stephen Dilworth & David Osborne, *Cyber Threats Against and in the Space Domain: Legal Remedies*, *in* 14th Int'l Conf. on Cyber Conflict (CyCon) 235-47 (2022).

strong legal frameworks are critical for not only addressing cybersecurity in outer space, but also securing and sustaining the key space operations that are the basis of modern civilisation.

The primary goal of this research is to identify the cybersecurity challenges amidst AI revolution to secure sustainability of space activities through the advancement of peaceful uses of outer space.This paper is composed of four parts including a short Introduction and Conclusion. Part two will discuss exploration of cybersecurity in outer space. Part three will examine jurisdictional challenges and the role of international organisations.

2. Exploration of Cybersecurity in Outer Space and Future Prospects

A. Definition and Analysis of Cybersecurity and Outer Space

Cybersecurity in outer space merges the vast cyberspace with the final frontier of space itself. As the underlying components of cybersecurity and space operations are substantially interconnected through technology, a comprehensive approach is crucial for understanding and protecting against cyberthreats within and towards outer space operations. Such an analysis defines and clarifies key terms of cybersecurity and explains the scope of cybersecurity in the space framework. In general, cybersecurity is regarded as the set of technologies and processes that are applied to protect equipment, networks, programmes and data from attacks, damage or unauthorised access. As for the space domain, this entails safeguarding satellite communication, data transmission and space-based services from cyberthreats.[10]

Furthermore, cybersecurity involves safeguarding networks, devices and data against unauthorised entry or illicit usage and maintaining information confidentiality, integrity and availability.[11] Likewise, it includes detecting, preventing, handling and reducing threats in, or originating from, cyberspace.[12] It refers to the condition of being safeguarded against illicit or unauthorised exploitation of electronic data and strategies implemented to secure this state.[13] It is also defined as the consolidation of

10 Dan Craigen et al., *Defining Cybersecurity*, 4(10) Tech. Innovation Mgmt. Rev. 13-21 (2014).

11 Cybersecurity & Infrastructure Security Agency, What is Cybersecurity? (2021), https://www.cisa.gov/news-events/news/what-cybersecurity.

12 The Oxford Handbook of Cyber Security 761 (Paul Cornish ed., 2021).

13 Oxford Learners Dictionaries, Cybersecurity, https://www.oxfordlearnersdictionaries.com/definition/english/cybersecurity.

methods, policies, principles of security, protective measures, guidelines, strategies for managing risk, actions, education, recommended practices, assurance and technologies deployed to defend a digital world, organisations and users' assets.[14] These definitions encompass securing all aspects of life depending on computers and the Internet, including communication.

Meanwhile, the virtual environment created through information and communication technologies is considered as the cyberspace. It incorporates all digital activities and infrastructure, including those that enable outer space operations.[15] Furthermore, cyberspace is referred to as systems and services connected either directly or indirectly to the Internet, telecommunications and computer networks.[16] Also, it is described as a global sphere within the information system characterised as an infrastructure of closely linked networks including the Internet, telecommunication networks, computer systems and built-in processors and controllers.[17] The term "outer space cybersecurity" specifically addresses security concerns related to space activities such as satellite communication, data transmission and the operation of space-based technology. It also involves protecting space assets from cyber attacks that could interfere with the functionality or compromise the data collected or transmitted by these assets.[18] Additionally, space operations are inherently intertwined with cyberspace and space systems face distinct challenges that make them attractive targets for hackers.[19]

However, integrating cyberspace and outer space activities has increased vulnerabilities and potential for cyber attacks. Satellites and other space assets integrated to national security, communication, navigation and scientific research face threats like interference, jamming and hacking. These risks underscore the importance of robust cybersecurity measures tailored to the unique challenges of space operations.[20] As digital dependence increases among societies, governments, businesses and individuals, their vulnerability to the digital environment's misuse escalates correspondingly. It has given rise to a substantial industry focused on

14 International Telecommunication Union, Overview of Cybersecurity, ITU Rec. ITU-T X.1205 (Apr. 2008), at 64, https://www.itu.int/rec/T-REC-X.1205-200804-I/en.

15 Al-Sakib Pathan, *On the Scale of Cyberspace and Cybersecurity*, 44(6) Int'l J. Computers & Applications 805-6 (2022).

16 Serra, *supra* note 6.

17 National Institute of Standards and Technology, Guide for Conducting Risk Assessments (Sept. 2012), at 800-30, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

18 Martin, *supra* note 8.

19 Jacob Oakley, Cybersecurity for Space: Protecting the Final Frontier 127 (2020).

20 Max Mutschler, *Security Cooperation in Space and International Relations Theory*, *in* Handbook of Space Security 50 (Kai-Uwe Schrogl et al. eds., 2015).

fortifying cyberspace, aiming to make it more secure, stable and reliable.[21] This development implies that the efforts to protect outer space and cyberspace are becoming intertwined. Increasingly, the Internet leans on services for communication and information that are enabled by space technology.

Meanwhile, space commercialisation mission increases cybersecurity risks due to the need to reduce costs and innovations that sometimes neglect software and hardware security. Moreover, the emergence of new space sectors, including tourism, asteroid mining, operations on the moon and exploration of Mars are expanding. At the same time, a revolution in small-scale satellites is taking place.[22] It indicates that these networks aim to deliver Internet access, communication and other relevant services which are vulnerable to cyber attacks.

Thus, regulating cybersecurity in the intertwined domains of cyberspace and outer space requires international cooperation under the comprehensive frameworks. The 'global' nature of space and concerning areas require collaboration among countries to develop and implement strategies that will ensure the safety, security and sustainability of space activities for the benefit of humanity. It means the end of the the end of an ineffective approach and a call for integrated action that focuses on detecting and counteracting the cyber threats aimed at space systems and infrastructure.[23]

From all indications, cybersecurity in outer space is a critical concern that spans the technical, legal and policy domains. As outer space becomes more accessible and integral to various aspects of contemporary life, it is paramount to protect space-based assets and the information they handle from cyber threats. Understanding the definitions and implications of cybersecurity in the outer space context is essential for fostering safe and secure space exploration and use.

B. What Will the Effects of New Technologies on Cybersecurity Be in the Future?

Cybersecurity in outer space is becoming increasingly important as nations and corporations expand their presence and operations beyond the Earth. Transformation technologies advance human capabilities in outer space and introduce complex challenges to securing these extraterrestrial operations. In particular, recent academic

21 The Oxford Handbook of Cyber Security, *supra* note 12, at 771.

22 Fidler, *supra* note 2.

23 Jessica West, Where Outer Space Meets Cyberspace: A Human-Centric Look at Space Security, Centre for International Governance Innovation (Jan. 29, 2023), https://www.cigionline.org/articles/where-outer-space-meets-cyberspace-a-human-centric-look-at-space-security.

research shows the insight that new technologies, notably cyber weapons, threaten the stability of outer space due to their accessibility, low attributability and reduced risk of collateral damage.[24] For example, simulated cyber anti-satellite weapon (cyber-ASAT) capabilities can alter debris collision forecasts to harm critical space systems without physical intervention.[25] New government officials, companies and technologies are expanding and transforming space activities. However, stakeholders in cyberspace acknowledge that neither space policy nor cybersecurity policy is fully prepared for the challenges arising from this meshing of space and cyberspace, which is increasing national security risks.[26] As cybersecurity in outer space has become automated and digitized, cyberspace risks should be considered to ensure the safety, security and sustainability of space activities. The global common use of cyberspace and outer space exhibits numerous interactions, especially in terms of cybersecurity, with increasing risks of attacks against satellites, such as interference, jamming and hacking.[27]

Moreover, the future of cybersecurity is connected to the fast-paced progress of technology, whose effects will be determined by the emerging devices shaping cybersecurity, such as the Internet of Things (IoT), AI and quantum computing. For instance, the proliferation of IoT devices significantly expands the scope for cyber threats; despite several devices possessing helpful capabilities, collecting data is a significant reason for developing smart devices. Nonetheless, the vulnerability of a home network to hacking escalates with the increasing number of connected devices, a concern amplified by the prolonged lifespan of IoT devices.[28] As IoT continues to be integrated into critical infrastructure, the potential for catastrophic cyber attack outcomes escalates. Thus, the need for robust cybersecurity measures tailored to the unique vulnerabilities of IoT devices is critical to safeguard these interconnected systems from exploitation.[29]

Meanwhile, experts have identified AI and machine learning (ML) as emerging technologies that will pose challenges to cybersecurity in the future. Although AI and ML technologies offer promising advances in automating cybersecurity defences, they also present new vulnerabilities. Attackers can exploit AI systems to conduct

24 Pavur & Martinovic, *supra* note 1, at 5.

25 *Id.*

26 Oakley, *supra* note 19, at 20.

27 Martin, *supra* note 8.

28 Zoltan Balazs, *As Threats to IoT Devices Evolve, Can Security Keep Up?*, World Econ. F. (Aug. 10, 2021), https://www.weforum.org/agenda/2021/08/threats-to-iot-devices-are-constantly-evolving-but-is-security-keeping-up.

29 Syarulnaziah Anawar et al., *IoT Technological Development: Prospect and Implication for Cyberstability*, 10(2) Int'l J. Advanced Computer Sci. & Applications 8 (2019).

more sophisticated and targeted attacks. The dual nature of AI technologies stresses the need for innovative approaches to secure AI systems and harness their potential responsibly.[30] The critical roles of AI and ML in cybersecurity in tackling current obstacles cannot be underestimated. However, as legal and ethical considerations are tied to their deployment, incorporating AI and ML into cybersecurity frameworks holds substantial promise for future exploration and innovation. Besides the IoT, AI and ML, quantum computing is another medium that promises to solve complex problems beyond the reach of classical computers, but its potential to break current cryptographic standards poses a significant threat to cybersecurity. The development of quantum computing requires the growth of quantum-resistant cryptographic algorithms to protect sensitive data from future quantum attacks. Transitioning to quantum-safe cryptography is critical in preparing for the post-quantum cybersecurity.[31]

Nowadays, global connectivity and space technology are important in the international communication, navigation and security systems. Earth-orbiting satellites are necessary in diverse tasks such as guiding GPS systems and processing cross-border financial transactions. At the same time, they are the foundations of our daily life and global infrastructure. As time goes by, however, satellites in orbit are more likely to become the targets of cyber warfare tactics aimed at disabling them.[32] The future of cybersecurity lies in the ability of businesses and governments to discover, learn about and prevent threats continuously evolving.[33] The OST and subsequent discussions in the UN General Assembly, the Conference on Disarmament and the UN Open-Ended Working Group aimed at reducing space threats which have been the most important tools for establishing rules, norms and principles of responsible conduct.[34]

The impacts of new technologies on cybersecurity are a two-edged weapon: they not only provide new opportunities for strengthened protection, but also

30 Harshada Salvi & Supriya Surve, *Emerging Trends and Future Prospects of Cybersecurity Technologies: Addressing Challenges and Opportunities*, 10(4) Int'l J. Sci. Res. Sci. & Tech. 399-406 (2023).

31 Simon Torkington, *Quantum computing could threaten cybersecurity measures. Here's why – and how tech firms are responding*, World Econ. F. (Apr. 23, 2024), https://www.weforum.org/stories/2024/04/quantum-computing-cybersecurity-risks.

32 Sylvester Kaczmarek, *Cybersecurity for Satellites is a Growing Challenge, as Threats to Space-Based Infrastructure Grow*, Conversation (Feb. 20, 2024), https://theconversation.com/cybersecurity-for-satellites-is-a-growing-challenge-as-threats-to-space-based-infrastructure-grow-223877.

33 Ramesh Ramakrishnan, *The Future of Cybersecurity and Its Potential Threats*, 11(7) Int'l J. Res. Applied Sci. & Eng'g Tech. 269-74 (2023).

34 Cécile Aptel & Susan Erickson, *Outer Space Security: Past and Ongoing Multilateral Efforts and Challenges*, 35(2) J. E. Asian Aff. 5-38 (2022).

create weaknesses for attackers, such as in social media or video games. The future cybersecurity will be marked by the continuous fight between the speed of technological developments and the adaption of cybersecurity measures to combat new threats.

C. Threats to Cybersecurity in Outer Space

Although there are not many open-source cases of cybersecurity breaches in outer space due to their secretive nature, some public cases highlight the fundamental role of cybersecurity in space operations whose consequences expose the weaknesses for national security and breaches of privacy. The event involving the NASA astronaut Anne McClain accessing her estranged spouse's bank account from the International Space Station (ISS) in 2019 draws our attention to two alarming issues regarding data privacy and cybersecurity in outer space environments. McClain's behaviour, although not illegal because she was authorised to do so, exemplifies the complexity of applying Earth-based privacy norms and legal frameworks in space - a territory where common jurisdictions are vague and the environment is fundamentally different.[35]

Multi-factor authentication could be encouraged to mitigate risks as it will provide an extra layer of security, which could be a biometric verification. This measure is vital in the environment where a traditional security breach could have a disproportionately large impact. The McClain case is a good example of how complicated it can be for outer space law enforcement officers to apply the laws governing the Earth. A special international legal system for space is thus necessary to define the legality of personal actions and data security. Moreover, in 2015, Terra Bella (formerly Skybox Imaging, later acquired by Google), suffered a security breach that was allegedly carried out by Chinese hackers. This case is an example of a more general trend of cyber attacks that are being carried out against the US aerospace companies to collect intelligence for espionage and the strategic interests of states in gaining an understanding of the US capabilities and technologies in space.[36] The implication of cyber attacks from space is not limited to the disruption of communications. These could be catastrophic for countries, for instance, causing economic turbulence by disrupting global navigation and financial systems and posing security concerns. The significance of satellites and other space assets makes them a good target for cyber attacks which can reduce

35 Jackie Wattles, *NASA Astronaut Anne McClain Accused by Spouse of Crime in Space*, N.Y. Times (Aug. 23, 2019), https://www.nytimes.com/2019/08/23/science/nasa-astronaut-anne-mcclain.html.

36 Myriam Wall & Peter Martinez, *Securing Space Systems: International and Commercial Implications*, 33(1) Space Pol'y 9-20 (2015).

countries' capabilities in defence and regular functioning.[37]

As both spacecraft and other space systems are becoming an integral part of national infrastructure, communications and defence, they are a more appealing target for cyber adversaries. Such systems are even more vulnerable to cyber threats, which are also compounded by the inherent vulnerabilities of these systems. Lei and colleagues note that the software and communication links that control satellites and other spacecraft may be obsolete or have inadequate encryption, which could be exploited by cybercriminals to hijack or manipulate their operations.[38]

Meanwhile, orbital debris could be a source of indirect cybersecurity threats that may damage space assets. It will affect the entire communication system, whereby data could be lost or exposed. Adushkin and Nechayev state that the dangers of space debris are caused by collisions with satellites, so that or a reliable monitoring system and mitigation strategies are needed to protect spacecraft from physical threats that may have a cyber component.[39] Furthermore, deliberate signal interference is a fundamental cybersecurity threat as it directly impacts the integrity and availability of data sent between satellites and Earth stations. Lisi's works shows how GPS signal spoofing and jamming will sabotage global navigation satellite systems which are of paramount importance for both military and civilian purposes, thereby making it necessary to use secure communication protocols and anti-jamming technologies.[40] Because of the dual nature of most space technologies, they are the point of contention in international relations and geopolitics. Dolman and Cooper underline the issue of strategic consequences of space assets and the need for international agreements that not only prevent space armament but also stimulate cybersecurity cooperation between nations to avoid conflicts of a terrestrial nature.[41]

The solution would be to integrate the proposals, strategies and international cooperation which will be reflected in the technological outcomes, policy initiatives and international partnerships. The security and sustainability of space actions necessitate a global effort, which all space actors should take part in, as a contribution to building the peaceful and secure use of outer space.[42]

37 Walter Peeters, *Cyberattacks on Satellites: An Underestimated Political Threat*, Space Pol'y (2024), https://www.lse.ac.uk/ideas/projects/space-policy/publications/Cyberattacks-on-Satellites.

38 Fidler, *supra* note 2.

39 Abid Murtaza et al., *Orbital Debris Threat for Space Sustainability and Way Forward*, 8 IEEE Access 61000-19 (2020).

40 David Miralles et al., *Android Raw GNSS Measurements as the New Anti-Spoofing and Anti-Jamming Solution*, *in* Proc. of the 31st International Technical Meeting of the Satellite Division of the Institute of Navigation (Ion Gnss+ 2018) 1-6 (2018).

41 Alan Steinberg, *Weapons in Space: The Need to Protect Space Assets*, 10(3) Astropolitics 248-67 (2012).

42 Biswanath Gupta & Rajrupa Roy, *Sustainability of Outer Space: Facing the Challenge of Space Debris*, 48(1) Glob.

3. Jurisdictional Challenges and the Role of International Organisations

A. Who Has the Jurisdiction to Control Cybersecurity in Outer Space?

In space exploration, a major international legal problem is sovereignty. According to the classical definition of sovereignty, states have supreme authority over the territory under their control. However, for the OST, space is not subject to appropriation by any nation. Article II of the OST states: "Outer space, including the moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means." This statement rejects the traditional framework of sovereignty and thus it is necessary to give a detailed interpretation of the legal meaning and implications of the statement. It points out that the Treaty sets up a distinct legal regime that leaves the old sovereignty paradigm behind and chooses instead common trusteeship. The principle that outer space is the "province of all mankind"[43] has both theoretical and practical complexities. For example, it creates an atmosphere of international cooperation for the management of space resources and their distribution beyond national sovereignty. In his paper, Bin Cheng notes that it is a mixture of freedom of exploration and the principle of non-appropriation and, therefore, it is a communal resource area theoretically accessible to all states without sovereign claims.[44] Consequently, the OST was historical in creating a structure that was conducive to peace and cooperation in outer space. However, the OST needs to be shaped to match the new challenges of today and tomorrow. The principle of space as the "province of all mankind" remains both a legal basis and a controversial doctrine as space activities remain in the process of development.[45]

In addition, it is necessary to examine the roles of the United Nations Office for Outer Space Affairs (UNOOSA), the International Telecommunication Union (ITU) and other relevant bodies in cybersecurity control in outer space. The UNOOSA fosters collaboration in the peaceful use of outer space and intermediarily implements the UN treaties that govern space activities.[46] However, the UNOOSA can only work for cybersecurity to a certain extent. International legal control of outer space has

L. & Pol'y Dev. 5 (2008).

43 OST art. 1.

44 Bin Cheng, Studies in International Space Law 510 (1997).

45 Secure World Foundation, Handbook for New Actors in Space 5 (Peter Martinez et al. eds., 2024), https://swfound.org/media/207931/handbook-for-new-space-actors_2024-revision.pdf.

46 UNOOSA, About Us, https://www.unoosa.org/oosa/en/aboutus/index.html.

to be based on consensus and cooperation. The Office can develop legally binding cybersecurity protocols, but its compliance is based on the voluntary and different capacities of the member states to implement such measures.[47]

In contrast to the UNOOSA, the ITU has a more structured and compelling role in space cybersecurity, which is quite significant in the field of satellite communication.[48] It provides frequency allocations and satellite orbit positions, and integrates cybersecurity into these frameworks to prevent interference and to guarantee safe communication. The ITU standards and protocols developed in response to emerging cyber threats indicate its operational capacity to establish detailed technical regulations relevant to space objects. Although the UNOOSA and ITU are trying to make outer space secure and peaceful, their operational frameworks and techniques are substantially different. While the ITU is empowered to adopt specific technical standards, the UNOOSA lacks the mechanism to compel compliance in its broader mandate. Such a difference points out a serious deficiency in the outer space cybersecurity governance system of the international community. It finally suggests integrated approaches and new frameworks.[49]

The OST provides that outer space should be free for exploration and use by all states and no state can claim sovereignty over outer space or any celestial body. The principle of non-interference presents a major question for outer space law concerning the cybersecurity measures. It is hard to determine if a sovereign country might be held responsible for any cybersecurity protocols in outer space, even though there are no sovereign claims. The Treaty reflects a general reference on the challenges posed by the non-appropriation and peaceful purposes around the specificity needed in cybersecurity threats.[50]

The 1976 Convention on Registration of Objects Launched into Outer Space (hereinafter Registration Convention) brings some order to space by requiring states to register space objects.[51] The Registration Convention records the state which launched each object belongs and is thus responsible for it. Registering these objects implies that states are in charge of cybersecurity for their registered objects.[52] As the

47 UN, Understanding International Law (2011), at 1, https://treaties.un.org/doc/source/events/2011/press_kit/fact_sheet_1_english.pdf.

48 Sheetal Kumar, Cybersecurity: what's the ITU got to do with it?, Freedom Online Coalition, https://freedomonlinecoalition.com/blog/cybersecurity-whats-the-itu-got-to-do-with-it-by-sheetal-kumar.

49 Secure World Foundation, *supra* note 45, at 124.

50 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205.

51 Convention on Registration of Objects Launched into Outer Space, Nov. 12, 1974, 28 U.S.T. 695, 1023 U.N.T.S. 15.

52 *Id.* art. II.

registration is limited to the objects they have launched, however, no regulation is provided yet for international cooperation and joint development of outer space objects between states.

The ITU is in charge of assigning global radio spectrum and satellite orbits, and regulating the use of space communications which are of the utmost importance in maintaining space objects communications. The ITU is a defence against potential disruption but is not involved in cybersecurity actions.[53] Although the regulatory framework provides the technical platform for communication, it is not yet empowered to enforce specific cybersecurity processes that fall under the jurisdiction of individual states or collective international entities. As such, the ITU has only adopted non-binding frameworks in this regards, such as the global Global Cybersecurity Agenda.[54] Globally, some countries such as the US have framed particular policies, for instance, the US Space Policy Directive-5 (SPD-5), which provides a framework for coordinating cybersecurity efforts in outer space. The SPD-5 is a set of guidelines for space system operators to engage in the responsible use and management of space systems and to reflect a national approach to space cybersecurity.[55] However, these measures are not extraterritorial and the challenge is to unilateral national measures in a domain inherently international.[56]

International law and regulations on cybersecurity are distributed among different countries without any central entity having full control over the issue.[57] Although already-existing legal frameworks, such as the Cyber Laws of the UAE,[58] serve as a foundation for state responsibility, there is a lack of mechanisms for cooperation and comprehensive management that are necessary for cybersecurity governance in outer space. Such mismatch calls for a globally accepted treaty or framework on cybersecurity in outer space in line with the increasing use of and reliance on space technology. Even if such a treaty or framework is adopted, the jurisdiction in outer space will continue to be contested even in this process. There is a possibility for the existing domestic laws or treaty to be applied by then.[59]

53 Audrey Allison, The ITU and Managing Satellite Orbital and Spectrum Resources in the 21st Century 5 (2014).

54 ITU, Global Cybersecurity Agenda (GCA), https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx.

55 US Office of Space Commerce, Space Policy Directive 5 (2020), https://www.space.commerce.gov/president-signs-space-cybersecurity-policy-directive.

56 *Id*.

57 Duncan Hollis, A Brief Primer on International Law and Cyberspace, Carnegie Endowment for International Peace (June 14, 2021), https://carnegieendowment.org/posts/2021/06/a-brief-primer-on-international-law-and-cyberspace?lang=en.

58 Government of UAE, Cyber Laws, https://u.ae/en/resources/laws.

59 Vienna Convention on the Law of Treaties, May 23, 1969, 1155 U.N.T.S. 331.

B. National Space Practices and Global Legislation

The US has developed a comprehensive framework to address space-related cybersecurity. It was anchored by the National Cyber Strategy under the specific directives such as the SPD-5, which establishes cybersecurity principles for space systems. This directive is critical as it represents the first integrated approach to specifically address the cybersecurity of space systems.[60] SPD-5's guidelines emphasizes the collaboration between government and private sector entities to enhance the security and resilience of space operations.[61] In case of Russia, a more centralised approach is employed for space cybersecurity. Russia strictly controls both civilian and military space activities. Russia's military doctrine and national security strategy focus on protecting space assets from cyber and physical threats. Russia is defensive to national security concerns.[62] Such a centralised approach can respond to threats quickly, but is not as flexible as that in decentralised frameworks. China adopted the Cybersecurity Law in 2017 to protect critical information infrastructure including space assets.[63] China incorporates the cyberspace security of both the public and private sector into space activities. In China, the government controls all space-related entities.[64] Meanwhile, the EU is align with the cybersecurity policies of its member states. The EU's policy is illustrated by the Network and Information Systems Directive.[65] Although the Directive is not specifically aimed at space, it addresses the infrastructure for space systems.[66] The EU integrates the cybersecurity strategy across member states into a common level of preparedness in cybersecurity for all sectors, including outer space.[67]

The UAE has passed a series of laws regulating outer space operations including the Federal Decree by Law No. (46) of 2023 concerning the Regulation of the Space Sector. This law regulates all space activities including licensing requirement and

60 *Id.*

61 US Office of Space Commerce, President Signs Space Cybersecurity Policy Directive (Sept. 4, 2020), https://www.space.commerce.gov/president-signs-space-cybersecurity-policy-directive.

62 Julian Cooper, Russia's Updated National Security Strategy, NATO Defense College (Russian Studies Series 2/21, 2021), https://www.ndc.nato.int/research/research.php?icode=704.

63 PRC Cybersecurity Law, https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017.

64 The State Council Information Office of China, "China's Space Program: A 2021 Prespective (Jan. 28, 2022), https://www.cnsa.gov.cn/english/n6465645/n6465648/c6813088/content.html.

65 EU Agency for Cybersecurity, Supporting the implementation of Union policy and law regarding cybersecurity, https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new.

66 EU, Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, EU Directive 2016/1148, at 1, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L1148.

67 *Id.*

cybersecurity guidelines in space operations, thereby ensuring safety, security and compliance with international treaties. [68] The UAE recognizes the various challenges to outer space activities, including threats to cybersecurity urgently in accordance with increasing space activities and accessibility for different purposes.[69] Cybersecurity in outer space operations should be addressed through both national strategies and international regulatory frameworks. The UAE's National Cybersecurity Strategy, for example, emphasizes protecting such a critical information infrastructure as satellites. The integration of cybersecurity measures in outer space reflects a proactive approach to the dual-use nature of space technologies - both civilian and military.[70] The UAE's legal and strategic approach to cybersecurity in outer space showcases a forward-thinking model that integrates national security, technological innovation and international cooperation. However, as space becomes a more contested domain, continuous updates to cybersecurity practices and international collaboration will be critical to safeguard space assets and ensure the peaceful use of outer space.[71]

C. Establishing a New International Authority for Cybersecurity in Outer Space

The complexity of cybersecurity in space includes cooperation beyond national legal frameworks, through broader international platform. Steer proposes that international cooperation is indispensibe when tackling the cybersecurity threats.[72] Hence, a comprehensive framework is needed for cybersecurity in outer space to secure space assets and promote international cooperation. Such a framework should be started with devising a concise mission statement that encapsulates the key objectives such as promoting the security of space assets and setting norms for cybersecurity in space operations.[73] Bowen notes the imbalance between policy intentions and practical implementations, especially in adjusting cybersecurity policies to the quickly changing nature of space technologies.[74] This critique is important to analyze the level

68 Federal Decree Law No. 46 of 2023: The UAE Space Law, https://uaelegislation.gov.ae/en/legislations/2129/download.

69 Dubai Electronic Security Center, Dubai Cyber Security Strategy (2017), at 7, 11 & 16, https://www.desc.gov.ae/wp-content/uploads/2023/pdfs/CSS_Eng.pdf.

70 Government of UAE, National Cyber Security Strategy 2019, https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/strategies-plans-and-visions-untill-2021/national-cybersecurity-strategy-2019.

71 Permanent Mission of the UAE to the UN, UAE Renews Commitment to Strengthening Cyber Security (June 29, 2021), https://uaeun.org/press_release/uae-renews-commitment-to-strengthening-cyber-security.

72 Delbert Terrill Jr., The Air Force Role in Developing International Outer Space Law 87 (1999).

73 Cybersecurity and Infrastructure Security Agency, Recommendations to Space System Operators for Improving Cybersecurity (2024), at 13, https://www.cisa.gov/sites/default/files/2024-06/Recommendations%20to%20Space%20System%20Operators%20for%20Improving%20Cybersecurity%20%28508%29.pdf.

74 Bleddyn Bowen, War in Space: Strategy, Spacepower, Geopolitics 193-227 (2020).

of countries' legislative and strategic frameworks.

To obtain international support and sponsorship, major spacefaring countries and international bodies like the UN should be actively involved. In his regard, the UNOOSA should be strategically entrusted with this task as it has already coordinated many space activities and is capable of overseeing the creation of such an authority.[75] Rajeswari underlined the need to develop the capacity to deal with both the defensive and offensive cyber challenges in outer space.[76] He stressed that countries are adopting their own space regulations and cybersecurity frameworks. However, it is crucial to have an inclusive strategy that integrates cyber resilience from the bottom-up in space technologies.[77] The most important aspect in this regard is to ensure that the authority is entitled to legally implement the global rules and standards. In this course, the focus is on creating new international treaties and/or adapting existing rules to the complex cybersecurity in outer space. Listner underlines that outer space law must be in affiliation with new challenges and technologies.[78]

Innovation remains the major determining factor of the credibility and strength of the authority. Forging collaborations with academia and private companies will be the key to pushing technological developments further and strengthening the cybersecurity of the global community. Such measures can be achieved with the strong support and cooperation of all the stakeholders, who are a part of the space process. This overarching strategy will thus enable the proposed agency to successfully protect space assets and establish a safe and stable outer space environment.

4. Conclusion

This study has highlighted the vital connections of cybersecurity with the technological, policy and legal dimensions of space missions. Following the commercialisation and militarisation of outer space, space assets have been victimized by a cyber threat. Because of development of AI, recent space systems have become more capable but more vulnerable simultaneously. The increasing reliance on satellites requires robust cybersecurity protocols to address both present and future challenges. Furthermore,

75 UNOOSA, Cybersecurity Law, Its Regulation and Relevance for Outer Space (2017), at 35 & 47, https://www.unoosa.org/documents/pdf/hlf/HLF2017/presentations/Day2/Session_7b/Presentation5.pdf.

76 Rajeswari Rajagopalan, *Enhancing Cybersecurity in Outer Space*, Diplomat (Apr. 15, 2024), https://thediplomat.com/2024/04/enhancing-cybersecurity-in-outer-space.

77 *Id.*

78 Fabio Tronchetti, Fundamentals of Space Law and Policy 107 (2013).

cybersecurity in outer space is going together with cybersecurity on Earth since the networks of space and Earth are interlinked.

While analyzing the cybersecurity frameworks comparatively between the US, the EU, Russia, China and the UAE, different strategic approaches are crafted to suit various national contexts. Such diversity suggests the need for international cooperation and sharing of best practices to elevate global security in outer space activities. Furthermore, this article has stressed to updating legal systems following technological developments and emerging cybersecurity problems. Updating old treaties such as the OST and developing new regulations are necessary. Such legal means should give clear and transparent definitions, responsibilities and enforcement power to protect space activities. In the end, as space missions play a leading role in future civilisations, it is critical to integrate cybersecurity with effective international legal frameworks and cooperative efforts. With this approach, we can secure sustainability of space activities and help advance peaceful uses of outer space for the benefit of mankind.

Received: August 1, 2024
Modified: September 15, 2024
Accepted: November 1, 2024