Cybersecurity Horizons: Navigating Challenges in the Space Tourism Industry

Mohamed Hussain Ibrahim
College of Law/ University of Sharjah
U18104410@sharjah.ac.ae

Sheer Abbas
College of Law/ University of Sharjah
sheer.abbas@sharjah.ac.ae

Accepted Date: 4/11/2024. **Publication Date: 25/2/2026.**

Abstract

The last decade witnessed a dynamic revival in human space exploration, propelled by burgeoning private sector involvement headed by companies like Virgin Galactic, Blue Origin, and SpaceX, catalyzing a global drive toward interstellar colonization aspirations and fostering collaborative efforts between nations and individuals evident in initiatives such as NASA's Artemis program, China's Tiangong program, and Russia and India's aspirations for independent space stations, which extends humanity's reach into the vast expanse of space beyond Earth's immediate celestial neighbors. This paper explores the under-addressed but critical domain of cybersecurity challenges in the rapidly advancing space tourism industry. It explains the potential threats posed by cyber-attacks to human spaceflights, specifically in the private sector, including the human factor, social engineering, and technical vulnerabilities. Furthermore, it draws attention to historical incidents in space exploration alongside its sensitive infrastructure. It emphasizes the pressing need for robust cybersecurity strategies to safeguard space tourism missions' security, safety, and integrity. It underscores the importance of collaborative efforts, including international cooperation, continuous monitoring, and enhanced crew training, and

developing a comprehensive legal framework. The paper argues that by addressing these challenges proactively and collaboratively, the space tourism industry can demonstrate resilience against evolving cyber threats and improve passenger safety, trust, and accessibility of this nascent but promising sector.
Keywords: Space Tourism, Space Tourism Industry, Space Flights, Cyber Threats, Cyber Security

آفاق الأمن السيبراني: مواجهة التحديات في صناعة السياحة الفضائية

محمد حسين ابراهيم علي الياسي*
كلية القانون/ جامعة الشارقة
U18104410@sharjah.ac.ae

شير عباس **
كلية القانون/ جامعة الشارقة
sheer.abbas@sharjah.ac.ae

تاريخ القبول: 2024/11/4. تاريخ النشر: 2026/2/25.

المستخلص

شهد العقد الماضي انتعاشًا ديناميكيًا في استكشاف الإنسان للفضاء، مدفوعًا بمشاركة القطاع الخاص المزدهرة برئاسة شركات مثل **Virgin Galactic** و**Blue Origin** و**SpaceX**، مما حفز التوجه العالمي نحو تطلعات الاستعمار بين النجوم وتعزيز الجهود التعاونية بين الدول والأفراد الواضحة في المبادرات. مثل برنامج أرتميس التابع لوكالة ناسا، وبرنامج تيانجونج الصيني، وتطلعات روسيا والهند لإنشاء محطات فضائية مستقلة، وهو ما يعمل على توسيع نطاق وصول البشرية إلى مساحة شاسعة من الفضاء تتجاوز جيران الأرض السماويين المباشرين. تستكشف هذه الورقة المجال الذي لم تتم معالجته ولكنه بالغ الأهمية لتحديات الأمن السيبراني في صناعة السياحة الفضائية سريعة التقدم. ويشرح التهديدات المحتملة التي تشكلها الهجمات السيبرانية على رحلات الفضاء البشرية، وتحديداً في القطاع الخاص، بما في ذلك العامل البشري، والهندسة الاجتماعية، ونقاط الضعف التقنية. علاوة على ذلك، فإنه يلفت الانتباه إلى الحوادث التاريخية في استكشاف الفضاء إلى جانب بنيته التحتية الحساسة. ويؤكد على الحاجة الملحة لاستراتيجيات قوية للأمن السيبراني لحماية أمن بعثات السياحة الفضائية وسلامتها ونزاهتها. ويؤكد على أهمية الجهود التعاونية، بما في ذلك التعاون الدولي، والمراقبة المستمرة، وتعزيز تدريب الطاقم، وتطوير إطار قانوني شامل. وترى الورقة أنه من خلال معالجة هذه التحديات بشكل استباقي وتعاوني، يمكن لصناعة السياحة الفضائية إظهار المرونة في مواجهة التهديدات السيبرانية المتطورة وتحسين سلامة الركاب والثقة وإمكانية الوصول إلى هذا القطاع الناشئ ولكن الواعد.

الكلمات المفتاحية: السياحة الفضائية، صناعة السياحة الفضائية، الرحلات الفضائية، التهديدات السيبرانية، الأمن السيبراني

*طالب ماجستير
**أستاذ مساعد دكتور

Introduction

In the last decade, a vibrant resurgent has ignited in the domain of human spaceflight missions. The increasing private sector interest in the cosmic arena fueled the transformative wave. This move comes with an ambition to colonize interstellar territory, reshaping the narrative of humanity's engagement with the cosmos [1]. Virgin Galactic, Blue Origin, and SpaceX are leading groundbreaking initiatives, turning the cosmos into a stage for innovation and urging nations and individuals to participate in the extraterrestrial narrative. A paradigm shift can be envisioned at the national level, going beyond the private domain [2]. The International Space Station (ISS) is not the only facility used for habitation during space travel, and the new move serves as the beginning of a new time where countries are eager to work together to compete in the area. China's Tiangong program inspired space-faring nations like Russia and India to articulate their intent to develop independent space stations. At the same time, NASA's Artemis program demonstrates a broader commitment to space habitation, increasing human curiosity and the quest for extraterrestrial frontiers [3] extending far beyond the boundaries of our immediate celestial neighborhood. The Artemis program is designed to explore the Moon and many more distant planets and claims that humans can reach out into massive, vast space beyond just imagining staying near Earth's planets.

Recreational Human Space Travel

Space tourism, comprising recreational human space travel, encompasses orbital, suborbital, and lunar ventures. Seven space tourists boarded eight trips to the International Space Station through the Russian Soyuz spacecraft facilitated between 2001 to 2009, facilitated by Space Adventures. In 2010, Russia suspended orbital space tourism and resumed in 2021 [4]. NASA announced

plans in 2019 to permit private astronauts on the ISS with SpaceX and Boeing spacecraft. The Soviet Interkosmos program increased the number of cosmonauts by including individuals from Warsaw Pact nations, allies of the USSR, and non-aligned countries by offering them shorter missions than Soviet cosmonauts[5]. On the contrary, the US Space Shuttle program introduced payload specialists, including Charles D. Walker. Furthermore, NASA's Space Flight Participant program aimed to include civilians without scientific roles, mainly as they selected Christa McAuliffe as the first Teacher in Space in cooperation with subsequent civilian programs, which were cancelled due to the failure of the Challenger disaster[6].

Concerns of Space Travel

Nevertheless, with the evolvement of space tourism, activities for orbital and suborbital ventures become increasingly feasible, but a critical concern arises concerning cybersecurity in this emerging industry due to its high reliance on sophisticated technological systems. These systems are used in operating spacecraft, such as navigation systems, communication protocols, and life support systems, urging to increase cyber security to ensure the security of these systems. Since space tourism opened the final frontier to a broader range of participants, including private citizens, the potential consequences of cyber-attacks on spacecraft systems pose severe threats ranging from compromised missions to endangering human lives. Therefore, understanding and addressing the cybersecurity challenges specific to space tourism is essential to safeguard these ventures' integrity, safety, and success.

In my own opinion, space tourism is a high-profile industry that is under immense development and needs a multi-faceted approach to cybersecurity well beyond technical fixes. The industry needs

to take immediate care in terms of cyber resilience as far as spacecraft and, of course, personal data of tourists are concerned, which may lead to further consequences in case of breaches. Additionally, I support the establishment of a sound regulatory mechanism that addresses the peculiar challenges of space tourism, just like aviation. The framework shall also focus on public awareness, making sure that would-be tourists understand the risks they will undertake in space travel and thus create confidence in the industry.

Challenges of Space Tourism

The novice space tourism industry presents numerous challenges demanding urgent attention to address them before its widespread commercialization [7]. The existing domain of knowledge underlines several concerns, such as the safety of passengers, medical risks, issues of environmental sustainability, and the need for a dedicated legal and regulatory framework. Passenger safety and medical risks associated with space tourism are always discussed in the limelight as space tourism holds inherent dangers of spaceflight due to exposure to radiance, potential accidents, and the effect of microgravity [8]. These risks are augmented amid the limited availability of medical facilities and expertise during onboard space flights. Another growing concern about space tourism is its environmental impact, as different studies underscore the potential adverse effects on the Earth's atmosphere, mainly due to the generation of space debris and rocket launches [9]. Moreover, the resource-intensive nature of space travel gives birth to numerous questions concerning sustainability over the long run. On the contrary, the legal and regulatory framework domain is evolving rapidly [10]. Different studies stress the need to develop international regulations to determine clear safety standards [1112], liability issues, and environmental protection in space tourism [13]. However,

addressing these issues for responsible operations in this promising industry is critical. Beyond these challenges, cyber security emerges as a specifically critical concern in space tourism, rarely discussed in existing scholarly contributions.

Cyber Threats in Space Tourism Flights

In the thrilling world of space tourism, people are excited to go on a space journey for fun and exploration [14]. However, there is a downside to threats engulfing it, specifically cyberattacks. Cyber-attacks in space tourism fall into technical and social engineering [15]. Technical attacks result from weaknesses in the physical and digital systems [16] that aim to support space missions. On the contrary, social engineering attacks result from tricking people to help the attackers[17]. Though space tourism seems exciting, it holds a hidden gander of cyber threats. These dangers are accompanied by the thrill of space travel and the shadowy risks of online attacks.

Threat actors deploy these vectors as tools in the cosmic domain, directing them toward the core of mission, business, and safety-critical systems, forming the fundamental framework of space missions [18]. Regarding human spaceflight, it is necessary to focus on securing these vital systems by highlighting their susceptibility to cyber intrusions. Threat actors are drawn to human spaceflight missions for numerous reasons. For example, countries perceive them as a chance to showcase their power [19]. At the same time, cybercriminals understand their significant value by attaching themselves to the lives of crew members, hacktivists, and thrill seekers to witness recognition through association with these broader missions. Despite motive, these missions are high-value targets that must be embedded with robust cyber security measures [20].

Cyber threats have become complex and ambiguous despite

threat actors choosing the easiest route [2122]. Therefore, an insider's help is usually advantageous, but launching social engineering attacks is another way to compromise digital systems indirectly [23]. The ground infrastructure is the weakest point in the extensive realm of space because it is easily accessible, making it a more vulnerable target to interfere directly with spacecraft operations. It happened in the past when an astronaut unintentionally brought a compromised USB to the International Space Station, and the virus spread as soon as it connected with the space station's computers [24]. In short, there is a need to stay vigilant with computer security to avoid such problems.

NASA Struggles

NASA struggles to resist dozens of cyber-attacks yearly, with most aiming to steal its intellectual property instead of targeting the critical safety aspects related to human operations aboard the ISS and transport vehicles [25]. Still, if something goes wrong, even controlling fire, leak detection issues, air quality maintenance, or management of tiny organisms, it could lead to enormous consequences[26]. Engineers must consider these perspectives to make spacecraft more reliable.

Other than the technical realm, interpersonal conflicts crews made up of astronauts from different nations add a layer of complexity to the cybersecurity landscape of human spaceflight missions [27]. The commercial nature of space tourism and the diversity of tasks open new horizons for potential crew-instigated cyber-attacks, extending beyond traditional insider threats and social engineering vectors.

In per my personal view, space tourism also demands the recognition of a dire need in cybersecurity. I believe it is important that space tourism, while taking shape and form, would not only build technical defenses but also nurture a culture of

cybersecurity awareness across its various participants. The development of an overarching regulatory framework will be important, taking into consideration the peculiar challenges presented in each case to make sure safety and privacy are concerned for all who engage in space missions. Upcoming sections further highlight cyber security challenges in space tourism by exploring the risks to critical mission and safety systems.

Human Factor in Cyber Security of Space Flights

Human factors play multifaceted roles in space tourism cyber security; crew members are potential attackers, unwitting vectors, collateral damage, and direct targets. For instance, crew members can initiate insider threats if they engage in certain motives to launch cyber-attacks while offering corporate espionage services or working as nation-state agents. They can also be involved in IP theft and data exfiltration [28]. These kinds of threats can be exacerbated with extensive training provided to crew members to understand the spacecraft system.

Ways to Lower Threats

The risk of crew members' cyber-attack involvement can be lowered by evaluating the options for performing manual operations [29] on space flight missions. At the same time, automation can eliminate such risks by limiting human interaction. Access controls and authentication protocols can also restrict access to minimize the impact of malicious actions [30]. Moreover, founding crew members approaching devices unnecessarily may require thorough background checks and temporary block of access devices until their association with malicious actors is proved wrong.

Challenges to Crewmembers

Crewmembers could also face harm as collateral damage in the

aftermath of a cyberattack on a spacecraft [31]. Such flights are highly mission-critical systems and heavily rely on safety as a second alternative, as the result of such attacks could disrupt life-sustaining systems onboard. Therefore, it is necessary to disconnect the safety system from the mission system completely. Such scenarios can occur where crew members could become direct targets of cyberattacks, leading to bodily harm Spacesuits, considered crucial to regulate life-critical functions, can be vulnerable to cyber threats, enabling attackers to exploit communication vulnerabilities and compromise sensor functions, which can pose substantial risks to the safety of crew members [32]. In believe, addressing the human factor in space tourism cybersecurity is vital, and it requires a comprehensive understanding of crew members' roles as potential threat actors.

Emerging Trends in Space Cyber Security

Advancements in the space tourism industry introduce new cybersecurity challenges by threatening the safety and security of passengers and infrastructure. Amid a growing number of spaceflight operations, the attack surface is expanding[33]. According to the Secure World Foundation 2023 report, the number of satellite operations, currently 5,700, will surpass 100,000 by 2030 [34]. Each satellite serves as a potential entry point for cyberattacks. The exponentially growing number of spaceflights is making interconnected networks more complicated and securing the entire ecosystem more complex and intricate.

Satellites and spacecraft use radio frequency communication, which is vulnerable to various attacks[35]. In 2022, such an incident happened when malicious minds jammed operations of Starlink terminals in Ukraine by underlining that they could disrupt communication channels during spaceflight missions and halt space tourism operations. Moreover, spoofing attacks on radio

frequency have the potential to navigate data by potentially endangering passengers and the spacecraft itself[36].

Vast Amounts of Data in Space Tourism

Space tourism operations create vast amounts of sensitive data, such as passenger information, flight plans and schedules, and spacecraft telemetry. It also holds detailed passenger-specific personal details, medical records, and financial information. Confidential information about orbital maneuvers, spacecraft trajectories, and landing procedures makes space flight information more sensitive. In addition, real-time data encompass vital details on the spacecraft's health, environmental conditions, and operational parameters[37]. This wealth of data makes space tourism an attractive target for malicious actors, urging them to disrupt operations and steal sensitive information to get lucrative benefits through selling on the dark web or ransomware attacks.

Ransomware Attack

In 2020, a ransomware attack was launched on Maxar Technologies, which collects geospatial data and satellite imagery [38]. The incident points out the legitimacy of the impact on space tourism logistics. As such incidents can disable critical systems for navigation, communication could be disrupted, leaving space tourists stranded and endangering their safety.

Social Engineering

Social engineering programs can be launched to target space travelers through their social media platforms and phishing [39]. Cybercriminals can easily personate legitimate entities to trick passengers into revealing sensitive information or hack their digital devices by enabling them to click on illegitimate links. For instance, criminal minds can send an official email requesting

login credentials to confirm flight schedules or inform change schedules, which could be a social engineering attempt to gain access to personal accounts. Moreover, disgruntled employees and personnel with privileged access to systems can serve as legitimate threats [40]. Since they have access to sensitive information, they could sabotage operations by leaking sensitive data or installing malware[52] within the spacecraft's network, aiming to cause significant damage.

From my perspective, these are a few essential illustrations of the ever-evolving threats landscape in cyberspace tourism. New threats can emerge with the advancement of technology and the maturing of the industry. Therefore, ongoing vigilance to deploy proactive security measures is unavoidable, alongside a comprehensive understanding of the attack surface to mitigate these evolving threats.

Ethical and Legal Dilemmas in Space Cyber Security

The growth of the space tourism industry opens new avenues to explore exciting possibilities; however, it also presents new challenges to humanity [41]. One is cybersecurity, alongside ethical and legal dilemmas surrounding cybersecurity in space tourism.

Ethical Dilemmas

Ethical dilemmas concern privacy, safety, access, and equity [42]. For instance, space tourism is experiencing a medical emergency, and a need to collect sensitive medical data of patients, physiologists, and diagnostic details emerges. The required information may need to travel or be stored, but cybercriminals can manage data breaches, compromising the privacy of passengers, doctors, and other collaborators [43]. Such incidents will further create emotional distress, financial harm, lack of trust in potential passengers, and dissatisfaction.[57]

Consent Issues

Potential surveillance of passenger activities during their space travel experience without their consent is needed. Such incidents can further erode public trust, raising questions about the safety and reliability of space tourism services [44]. The landscape of cyber threats is so strengthened that a cyber-attack can invade a spacecraft's navigation system by potentially altering its course. Criminal minds or state hackers may try to hack life support systems to disrupt critical functions such as oxygen supply or temperature control, causing life-threatening situations. Robust cyber security measures are costly but unavoidable [45]. Therefore, space tourism companies would likely pass these costs to passengers, making an industry only accessible to the wealthy. Such situations further cause ethical concerns about inclusivity and potentially hinder the democratization of space exploration [46]. Therefore, robust cybersecurity measures must be ensured in space tourism alongside proper legislation to prevent discrimination against inequitable access to space travel opportunities.

Consequences of Cyber Threats

Cyber breaches can result in financial losses for space tourism companies, including potential revenue loss, legal expenses, and reputation damage. These incidents require investigation and mitigation costs, further threatening the viability of the space tourism business. In addition, a severe cyber breach in space tourism activities can have severe implications for future space exploration [47]. Such incidents will undermine the public's interest and deter commercial space flight feasibility and safety, leading to decreased investment in space tourism ventures and related industries [48].

Legal Challenges

Alongside ethical dilemmas in space tourism, legal difficulties are causing great concern, specifically about jurisdiction, regulations, and data protection. Since there is no clear jurisdiction in outer space [49], it might become difficult to trace the origin of cyber-attacks or to conclude which jurisdiction rules would be applied. The situation will become further complicated regarding which authorities can investigate and prosecute the perpetrators, making the post-attack situation more difficult [50]. Consequently, it will become challenging to hold organizations responsible for such mishaps.

As of 2024, no clear and comprehensive international regulations address cyber security in space tourism. The lack of clear guidelines creates further uncertainties for space tourism companies in developing passengers' trust by raising concerns about potential vulnerabilities in spacecraft systems [51]. While existing agreements, such as the Outer Space Treaty, outline state jurisdiction in space, they may be insufficient to address cyber incidents. Therefore, there is a need to establish international standards to implement best practices of cybersecurity to promote consistency and enhance the industry's overall safety.

Historical View

The space tourism industry is in its beginner stages; therefore, incidents related to cybersecurity issues affecting commercial flights have not been explicitly reported. However, some cybersecurity and space exploration incidents can help us understand the nature of the severity.

In 2010, the incident of Stuxnet Worm served as an example of a cyberattack on critical infrastructure as it targeted supervisory control and data acquisition (SCADA) systems [52]. These attacks specifically target systems associated with Iran’s nuclear program.

The incident shows that cyberattack can potentially manipulate physical systems with high security. Numerous researchers point out potential vulnerabilities of satellites and their components, including communication, navigation, and Earth observation capabilities. For instance, 2018, the Galileo Navigation System of the European Union faced technical incidents [53]. Though they reported the issue of disruption in ground infrastructure, the incident raised questions about the resilience and security of the satellite navigation system.

NASA is a government-backed agency responsible for administering space programs, space research, and aeronautics research. It has faced numerous cybersecurity breaches, including unauthorized access and incidents targeting its servers [54]. In 1999, a 15-year-old Jonathan James attacked NASA's servers to gain fame and popularity in the hacker's hall of fame. It also faces security breach issues in 2011 and 2016, raising questions about its ability to secure such sensitive servers from hackers and the possible power of other space exploration companies [55]. Such incidents underscore the challenge of ensuring the digital infrastructure supporting space agencies and their missions.

In 2023, a denounced ransomware group, LockBit, claimed to have stolen valuable files from SpaceX by breaching Texas-based Maximum Industries [56]. The organization holds more than 3000 drawings of certified SpaceX engineers for auction. Russia-based Lockbit claims its expertise in exploiting vulnerabilities, accessing victim systems, and getting insider information.

Space infrastructure is critical for space tourism and maintaining global communication [57]. At the same time, threats on spacecraft and satellites point toward significant threats, allowing hackers to take control of systems by manipulating control and stealing confidential Data [58]. Numerous incidents of jamming and

spoofing disrupt satellite communication, such as cyberattacks on the Starlink SpaceX terminals during the Ukraine conflict. Moreover, a research paper by the University of Oxford underscores the increasing threats of cyberattacks on space systems [59]. It mentions that many space stations and infrastructure lack sufficient cybersecurity measures, making them more vulnerable targets. FBI, NCSC, and Air Force issued a bulletin to warn foreign intelligence agencies that were expecting to target American space capabilities. The advisory urged the US commercial space industry to take preventive measures against satellite communications, imaging capabilities, remote sensing, and commercial space infrastructure threats [60].

Impact of Cyber Security Incidents on the Space Tourism Industry

The industry of space tourism faces significant cybersecurity challenges, including potential disruption of satellite communication systems, sabotage of ground control operations, unauthorized access to critical systems, manipulation of spacecraft navigation, ransomware attacks causing operational downtime, intellectual property theft, breaches of privacy concerns, vulnerabilities in the supply chain, and disruption of reservation systems[61]. Together, these risks pose severe risks to the safety of passengers, the integrity of the mission, and the industry's reputation [62].There is a need to have a comprehensive cybersecurity strategy to safeguard against potential disruptions, unauthorized access, and the compromise of sensitive information to ensure the continued growth and success of the space tourism sector.

While the industry promises a 44.8% annual growth rate by 2030, a single cyberattack can crash those dreams as per the report of space tourism market size 2030. For instance, in 2021, hackers

penetrated the International Space Station (ISS) network by showcasing the vulnerabilities of even the most advanced space system in the world [63]. Moreover, a significant cyber incident could shatter public trust in the space tourism industry. An incident about a near-miss space disaster can be expected, with a massive data breach leading to a public outcry and a potential freeze on future space tourism ventures [64]. These vulnerabilities can scare away potential investors, and insurance companies may refuse coverage or demand high premiums, making space tourism a risky proposition only accessible to the wealthiest.

The increased hype about cyber incidents triggers the need for stricter regulations and urges government agencies to implement protocols by launching procedures to make space tourism potentially more accessible industry [65]. It seems to me that Cyberattack could result in significant financial losses for space tourism companies due to operational disruptions and reputational damage. According to experts in cyber security, cyber-attacks targeting space tourism will become more frequent and sophisticated as the industry grows.

Future of Space Tourism and Cyber Threats

Despite the dangers of cyber threats, the future of space tourism is bright, further expanding the threat landscape and urging relevant international and national institutes to develop sound regulations and policies to combat such harms. The Counter Space report of 2023 by the Secure World Foundation evaluates 11 countries with capacity in five major categories: direct ascent, co-orbital, electronic warfare, directed energy, and cyber [66]. The domain of counter-space efforts is led by the US, Russia, and China, while India seems to be emerging with its ASAP capability. Australia, Japan, France, South Korea, and the UK are focusing more on strengthening their military-related capabilities in space. North

Korea and Iran demonstrate their skills to disrupt satellite signals, yet no country has used destructive counterspace capabilities in military operations.

Operational satellites in Earth's orbit rose from 958 to 3,371 between 2010 and 2020 which is a 252% increase. As per industry predictions, by 2030 the operational satellite reached to 100,000. Consequently, global space economy expected to grow reach $1 trillion by 2040 while currently it is $400 billion [67]. The key players in private sector are Telesat, SpaceX, Amazon, and OneWeb.

Observing the industry dynamics and future growth, Gregory Falco, an assistant professor John Hopkins shared his concerns about cybersecurity in space missions, sparked by the lack of cybersecurity features in Artemis crew spacesuits. He mentions that currently the security of space industry is outdated and insignificant approaches making it more vulnerable for spacecraft activities specifically in terms of cyber threats. The major threats include ransomware attacks, malware installation, threats to crewed spacecraft, and deliberate targeting to safety critical systems.

Though, there is no deadly cyber threats on the surface related to space but there are incidents about ethical breach in cyber space. For instance, in 2019, NASA astronaut Anne McClain accessed the bank account of her estranged spouse Summer Worden while on the International Space Station, raising questions about data privacy and cybersecurity in space. McClain had been authorized to access the account, but this incident highlighted the challenges of implementing Earth-based privacy and legal systems in outer space. It also pointed to potential cybersecurity risks associated with sensitive information being accessed from remote locations, such as the ISS. This case gives further impetus to the urgent

updates of regulations on privacy, jurisdiction, and cybersecurity since human activity in space will be expanding. Other cyber incidents besides this 2019 incident involving McClain have shown how these space-related systems are vulnerable. In 2008, a virus infected the computer systems of the International Space Station because of the unintentional act of taking a compromised USB drive on board; it proved that malware can cause problems in space environments. Also in 2020, it was reported that Russian hackers tried to compromise the US satellite systems-exposing the vulnerability of space assets to international cyber threats. These incidents bring us to the fore that cybersecurity for protecting space missions and assets both from within and outside becomes paramount.

From the University of Washington, Saadia Pekkanen underline the need for national polices to refute cybersecurity risks in space. Her suggestions include adopting terrestrial cybersecurity standards, for instance, zero-trust protocols, and developing an environment which support ethical hackers. In essence, there is an urgent call to reinvest cybersecurity paradigms for space missions rather than transferring imperfect terrestrial solutions.

The $546 billion worth economy of global space demands strict cybersecurity initiatives on urgent basis as unlike other industries it heavily relies on space infrastructure for telecommunications, internet connectivity, weather tracking, and GPS making cyber-attacks potentially devastating. The recent incidents of cyberattacks invading telescopes and consequent warnings from US Air Force and FBI about espionage targeting the US space threatening the whole world by questioning capabilities of sensitive institutes. However, certain challenges impeding this progress including vulnerabilities in satellite systems, limited resources, and potential impacts ranging from disruptions to endangering astronauts to national security.

Conclusion

The growing space tourism industry, with its promises to explore extraterrestrial frontiers and reshape humanity's engagement with the cosmos, faces critical yet often overlooked challenges, specifically cybersecurity. Advancements in industry developed technical vulnerabilities, social engineering, and the human factor to pose substantial threats to space tourism missions' safety, security, and integrity. The landscape of cyber threats is complicated, including potential disruption of satellite communication to the compromise of sensitive passenger information, which requires immediate attention and proactive measures. The historical context underscores the incident in space exploration and critical infrastructure, emphasizing the need for a robust cyber security strategy to safeguard against evolving threats in this emerging but typically growing industry.

Recommendations

A comprehensive but collaborative approach is essential to addressing the cybersecurity challenges in space tourism.

- First, space tourism companies must prioritize cybersecurity measures, investing in developing and implementing advanced technologies to secure sensitive systems. International cooperation is inevitable to create clear regulations and standards for cybersecurity in space tourism, as it ensures consistency and accountability.
- Improved training programs for crew members should incorporate cybersecurity awareness to mitigate the risk of insider threats.
- Moreover, regular monitoring and threat intelligence sharing among industry stakeholders can help anticipate and respond to emerging cyber threats.
- In this regard, government agencies, space companies,

and private organizations must work collectively to establish a robust legal framework that defines jurisdiction and

develop regulations and data protection standards to address the ethical and legal dilemmas surrounding cybersecurity in space tourism. The industry can build resilience only through proactive efforts and global collaboration against cyber threats to maintain trust, safety, and accessibility of space tourism for future generations.

Endnotes

[1] Mihir Neal, 'Soyuz MS-20 Space Tourism Flight Docks with ISS', *NASASpaceFlight.Com* (blog), 8 December 2021, https://www.nasaspaceflight.com/2021/12/soyuz-ms-20-tourist-launch/.

[2] Steve Creech, John Guidi, and Darcy Elburn, 'Artemis: An Overview of NASA's Activities to Return Humans to the Moon', in *2022 IEEE Aerospace Conference (AERO)* (2022 IEEE Aerospace Conference (AERO), Big Sky, MT, USA: IEEE, 2022), 1–7, https://doi.org/10.1109/AERO53065.2022.9843277.

[3] Marshall Smith et al., 'The Artemis Program: An Overview of NASA's Activities to Return Humans to the Moon', in *2020 IEEE Aerospace Conference* (2020 IEEE Aerospace Conference, Big Sky, MT, USA: IEEE, 2020), 1–10, https://doi.org/10.1109/AERO47225.2020.9172323.

[4] Neal, 'Soyuz MS-20 Space Tourism Flight Docks with ISS'.

[5] Neal.

[6] Creech, Guidi, and Elburn, 'Artemis'.

[7] Michael Bouchey and Jason Delborne, 'Redefining Safety in Commercial Space: Understanding Debates over the Safety of Private Human Spaceflight Initiatives in the United States', *Space Policy* 30, no. 2 (May 2014): 53–61, https://doi.org/10.1016/j.spacepol.2014.03.002.

[8] Carol Norberg, ed., *Human Spaceflight and Exploration* (Berlin, Heidelberg: Springer Berlin Heidelberg, 2013), https://doi.org/10.1007/978-3-642-23725-6.

[9] Abbas Sheer and Shouping Li, 'Space Debris: A New Broadway to Address Organizational and Operational Aspects for Removal', *Journal of East Asia and International Law* 12, no. 2 (30 November 2019): 269–82, https://doi.org/10.14330/jeail.2019.12.2.02.

[10] Ali Al Zaabi, 'Legal Reasoning and Investigation in the Crimes Related to the Outer Space: An Analytical Study in UAE Legislation', *مجلة جامعة الشارقة للعلوم القانونية* 18, no. 1 (18 January 2022): 676–703, https://doi.org/10.36394/jls.v18.i1.22.

[11] Abdalla Al-Hosni and Wael Allam, 'نِطَاق التزامات الإمارات في القانون الدولي للفضاء', *مجلة جامعة الشارقة للعلوم القانونية* 19, no. 3 (3 October 2022): 56–86, https://doi.org/10.36394/jls.v19.i3.3.

[12]

[13] Sheer and Li, 'Space Debris'.

[14] J. Benson, 'The Role of the Private Sector/Entrepreneur in Future Human Space Exploration', in *Beyond the International Space Station: The Future of Human Spaceflight*, ed. M. Rycroft, vol. 7, Space Studies (Dordrecht: Springer Netherlands, 2002), 217–22, https://doi.org/10.1007/978-94-015-9880-4_29.

[15] Myriam Dunn Cavelty and Andreas Wenger, *Cyber Security Politics Socio-Technological Transformations and Political Fragmentation* (Milton: Taylor & Francis Group, 2022).

[16] رزق Samoudi, 'The Right to Self-Defense in Response to Cyber-Attacks in Light of International Law', 15 *مجلة جامعة الشارقة للعلوم القانونية*, no. 2 (31 December 2018): 336–62, https://doi.org/10.36394/jls.v15.i2.12.

[17] Fatima Salahdine and Naima Kaabouch, 'Social Engineering Attacks: A Survey', *Future Internet* 11, no. 4 (2 April 2019): 89, https://doi.org/10.3390/fi11040089.

[18] Charlotte Van Camp and Walter Peeters, 'A World without Satellite Data as a Result of a Global Cyber-Attack', *Space Policy* 59 (February 2022): 101458, https://doi.org/10.1016/j.spacepol.2021.101458.

[19] Dunn Cavelty and Wenger, *Cyber Security Politics Socio-Technological Transformations and Political Fragmentation*.

[20] Samoudi, 'The Right to Self-Defense in Response to Cyber-Attacks in Light of International Law'.

[21] Shaikha Alzahrani, 'International Cooperation in Combating Cyber Attacks', 17 *مجلة جامعة الشارقة للعلوم القانونية*, no. 1 (24 November 2021): 740–72, https://doi.org/10.36394/jls.v17.i1.23.

[22]

[23] Ahmed Hayajneh and Hamda Alsuwaidi, ' التحقيق الجنائي بتقنية الاتصال عن بعد وفقًا للتشريع الإماراتي', *مجلة جامعة الشارقة للعلوم القانونية* 19, no. 4 (12 January 2023), https://doi.org/10.36394/jls.v19.i4.13.

[24] Ellie Zolfagharifard, 'Russian Cosmonaut "accidentally Infected International Space Station" with USB Stick | Daily Mail Online', 2013, https://www.dailymail.co.uk/sciencetech/article-2503352/Russian-cosmonaut-accidentally-infected-International-Space-Station-USB-stick.html.

[25] Paul Kallender, 'Waking Up to a New Threat: Cyber Threats and Space', *TRANSACTIONS OF THE JAPAN SOCIETY FOR AERONAUTICAL AND SPACE SCIENCES, AEROSPACE TECHNOLOGY JAPAN* 12, no. ists29 (2014): Tv_1-Tv_10, https://doi.org/10.2322/tastj.12.Tv_1.

[26] Al-Hosni and Allam, 'نِطَاق التزامات الإمارات في القانون الدولي للفضاء'.

[27] Otman Driouch, Slimane Bah, and Zouhair Guennoun, 'A Holistic Approach to Build a Defensible Cybersecurity Architecture for New Space Missions', *New Space* 11, no. 4 (1 December 2023): 203–18, https://doi.org/10.1089/space.2022.0029.

[28] Alzahrani, 'International Cooperation in Combating Cyber Attacks'.

[29] Jacob G. Oakley, *Cybersecurity for Space: Protecting the Final Frontier*, For Professionals by Professionals (New York, NY: Apress, 2020).

[30] Ioannis Agrafiotis et al., 'A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate', *Journal of Cybersecurity* 4, no. 1 (1 January 2018), https://doi.org/10.1093/cybsec/tyy006.
[31] James Pavur and Ivan Martinovic, 'The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space', in *2019 11th International Conference on Cyber Conflict (CyCon)*, vol. 900, 2019, 1–18, https://doi.org/10.23919/CYCON.2019.8756904.
[32] Driouch, Bah, and Guennoun, 'A Holistic Approach to Build a Defensible Cybersecurity Architecture for New Space Missions'.
[33] Kallender, 'Waking Up to a New Threat'.
[34] Jessica Lis, 'Secure World Foundation Releases 2023 Update to Counterspace Report', Payload, 14 April 2023, https://payloadspace.com/secure-world-foundation-releases-2023-update-to-counterspace-report/.
[35] Pavur and Martinovic, 'The Cyber-ASAT'.
[36] Hari Sourabh Konkimalla, 'An Analysis of the Security of the Global Positioning System (GPS) and Proposed Solutions', 2023, https://doi.org/10.7939/R3-3KY4-A853.
[37] Keith Epstein and Ben Elgin, 'Network Security Breaches Plague NAS', 2005, https://www.cs.clemson.edu/course/cpsc420/material/Papers/NASA.pdf.
[38] Susan White and Protiti Dastidar, 'Lockheed Martin Acquisitions: Stay the Course or Change Strategy?', *The CASE Journal* 17, no. 4 (12 October 2021): 494–541, https://doi.org/10.1108/TCJ-08-2020-0112.
[39] Zolfagharifard, 'Russian Cosmonaut "accidentally Infected International Space Station" with USB Stick | Daily Mail Online'.
[40] Agrafiotis et al., 'A Taxonomy of Cyber-Harms'.
[41] Oakley, *Cybersecurity for Space*.
[42] Driouch, Bah, and Guennoun, 'A Holistic Approach to Build a Defensible Cybersecurity Architecture for New Space Missions'.
[43] Kallender, 'Waking Up to a New Threat'.
[44] Van Camp and Peeters, 'A World without Satellite Data as a Result of a Global Cyber-Attack'.
[45] M. Manulis et al., 'Cyber Security in New Space: Analysis of Threats, Key Enabling Technologies and Challenges', *International Journal of Information Security* 20, no. 3 (June 2021): 287–311, https://doi.org/10.1007/s10207-020-00503-w.
[46] Alyssa Goessler, 'The Private Sector's Assessment of U.S. Space Policy and Law', 2022, https://aerospace.csis.org/wp-

content/uploads/2022/07/AGoessler_The-Private-Sectors-Assessment-of-U.S.-Space-Policy-and-Law.pdf.

[47] Dunn Cavelty and Wenger, *Cyber Security Politics Socio-Technological Transformations and Political Fragmentation*.

[48] Kallender, 'Waking Up to a New Threat'.

[49] Ms Amna Al Dhahouri and Professor Wael Allam, ' المسؤولية الدولية عن انتهاك الالتزام بمنع تَلَوُّث بيئة الفضاء الخارجي (دراسة في إطار القانون الدولي للبيئة)', *مجلة جامعة الشارقة للعلوم القانونية*, 21 no. 1 (4 April 2024), https://doi.org/10.36394/jls.v21.i1.18.

[50] P. J. Blount, 'Jurisdiction in Outer Space: Challenges of Private Individuals in Space', *Journal of Space Law* 33 (2007): 299.

[51] Ankit Kumar Padhy and Amit Kumar Padhy, 'Legal Conundrums of Space Tourism', *Acta Astronautica* 184 (July 2021): 269–73, https://doi.org/10.1016/j.actaastro.2021.04.024.

[52] Nicholas R. Rodofile, Kenneth Radke, and Ernest Foo, 'Extending the Cyber-Attack Landscape for SCADA-Based Critical Infrastructure', *International Journal of Critical Infrastructure Protection* 25 (June 2019): 14–35, https://doi.org/10.1016/j.ijcip.2019.01.002.

[53] Vidal Ashkenazi, 'The Challenges Facing Galileo', *Space Policy* 16, no. 3 (July 2000): 185–88, https://doi.org/10.1016/S0265-9646(00)00030-8.

[54] Epstein and Elgin, 'Network Security Breaches Plague NAS'.

[55] Dylan Rafferty and Kevin Curran, 'The Role of Blockchain in Cyber Security', *Semiconductor Science and Information Devices* 3, no. 1 (21 May 2021), https://doi.org/10.30564/ssid.v3i1.3153.

[56] Eduard Kovacs, 'Ransomware Group Claims Theft of Valuable SpaceX Data From Contractor', SecurityWeek, 14 March 2023, https://www.securityweek.com/ransomware-group-claims-theft-of-valuable-spacex-data-from-contractor/.

[57] Zolfagharifard, 'Russian Cosmonaut "accidentally Infected International Space Station" with USB Stick | Daily Mail Online'.

[58] Jan Schmitz et al., 'Sixty Years of Manned Spaceflight—Incidents and Accidents Involving Astronauts between Launch and Landing', *Aerospace* 9, no. 11 (2 November 2022): 675, https://doi.org/10.3390/aerospace9110675.

[59] James Pavur and Ivan Martinovic, 'Building a Launchpad for Satellite Cyber-Security Research: Lessons from 60 Years of Spaceflight', *Journal of Cybersecurity* 8, no. 1 (28 January 2022): tyac008, https://doi.org/10.1093/cybsec/tyac008.

[60] Michael Martina, 'US Warns Space Companies about Foreign Spying | Reuters', accessed 14 March 2024, https://www.reuters.com/world/us/us-warns-space-companies-about-foreign-spying-2023-08-18/.

[61] Epstein and Elgin, 'Network Security Breaches Plague NAS'.

[62] Kallender, 'Waking Up to a New Threat'.
[63] Driouch, Bah, and Guennoun, 'A Holistic Approach to Build a Defensible Cybersecurity Architecture for New Space Missions'.
[64] Zolfagharifard, 'Russian Cosmonaut "accidentally Infected International Space Station" with USB Stick | Daily Mail Online'.
[65] White and Dastidar, 'Lockheed Martin Acquisitions'.
[66] Lis, 'Secure World Foundation Releases 2023 Update to Counterspace Report'.
[67] Irene Klotz, 'Burgeoning Satellite Industry Paving Way To $1 Trillion Space Economy | Aviation Week Network', 2021, https://aviationweek.com/aerospace/program-management/burgeoning-satellite-industry-paving-way-1-trillion-space-economy.

References

i. Agrafiotis, Ioannis, Jason R C Nurse, Michael Goldsmith, Sadie Creese, and David Upton. 'A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate'. *Journal of Cybersecurity* 4, no. 1 (1 January 2018). https://doi.org/10.1093/cybsec/tyy006.

ii. Al Zaabi, Ali. 'Legal Reasoning and Investigation in the Crimes Related to the Outer Space: An Analytical Study in UAE Legislation'. 18 *مجلة جامعة الشارقة للعلوم القانونية*, no. 1 (18 January 2022): 676–703. https://doi.org/10.36394/jls.v18.i1.22.

iii. Al-Hosni, Abdalla, and Wael Allam. ' نِطَاق التزامات الإمارات في القانون الدولي للفضاء'. *مجلة جامعة الشارقة للعلوم القانونية* 19, no. 3 (3 October 2022): 56–86. https://doi.org/10.36394/jls.v19.i3.3.

iv. Alzahrani, Shaikha. 'International Cooperation in Combating Cyber Attacks'. 17 *مجلة جامعة الشارقة للعلوم القانونية*, no. 1 (24 November 2021): 740–72. https://doi.org/10.36394/jls.v17.i1.23.

v. Ashkenazi, Vidal. 'The Challenges Facing Galileo'. *Space Policy* 16, no. 3 (July 2000): 185–88. https://doi.org/10.1016/S0265-9646(00)00030-8.

vi. Benson, J. 'The Role of the Private Sector/Entrepreneur in Future Human Space Exploration'. In *Beyond the International Space Station: The Future of Human Spaceflight*, edited by M. Rycroft, 7:217–22. Space Studies. Dordrecht: Springer Netherlands, 2002. https://doi.org/10.1007/978-94-015-9880-4_29.

vii. Blount, P. J. 'Jurisdiction in Outer Space: Challenges of Private Individuals in Space'. *Journal of Space Law* 33 (2007): 299.

viii. Bouchey, Michael, and Jason Delborne. 'Redefining Safety in Commercial Space: Understanding Debates over the Safety of Private Human Spaceflight Initiatives in the

United States'. *Space Policy* 30, no. 2 (May 2014): 53–61. https://doi.org/10.1016/j.spacepol.2014.03.002.

ix. Creech, Steve, John Guidi, and Darcy Elburn. 'Artemis: An Overview of NASA's Activities to Return Humans to the Moon'. In *2022 IEEE Aerospace Conference (AERO)*, 1–7. Big Sky, MT, USA: IEEE, 2022. https://doi.org/10.1109/AERO53065.2022.9843277.

x. Dhahouri, Ms Amna Al, and Professor Wael Allam. المسؤولية الدولية عن انتهاك الالتزام بمنع تَلَوُّث بيئة الفضاء الخارجي ' (دراسة في إطار القانون الدولي للبيئة)'. *مجلة جامعة الشارقة للعلوم القانونية* 21, no. 1 (4 April 2024). https://doi.org/10.36394/jls.v21.i1.18.

xi. Driouch, Otman, Slimane Bah, and Zouhair Guennoun. 'A Holistic Approach to Build a Defensible Cybersecurity Architecture for New Space Missions'. *New Space* 11, no. 4 (1 December 2023): 203–18. https://doi.org/10.1089/space.2022.0029.

xii. Dunn Cavelty, Myriam, and Andreas Wenger. *Cyber Security Politics Socio-Technological Transformations and Political Fragmentation*. Milton: Taylor & Francis Group, 2022.

xiii. Epstein, Keith, and Ben Elgin. 'Network Security Breaches Plague NAS', 2005. https://www.cs.clemson.edu/course/cpsc420/material/Papers/NASA.pdf.

xiv. Goessler, Alyssa. 'The Private Sector's Assessment of U.S. Space Policy and Law', 2022. https://aerospace.csis.org/wp-content/uploads/2022/07/AGoessler_The-Private-Sectors-Assessment-of-U.S.-Space-Policy-and-Law.pdf.

xv. Hayajneh, Ahmed, and Hamda Alsuwaidi. ' التحقيق الجنائي بتقنية الاتصال عن بعد وفقًا للتشريع الإماراتي'. *مجلة جامعة الشارقة للعلوم القانونية*, 19 no. 4 (12 January 2023). https://doi.org/10.36394/jls.v19.i4.13.

xvi. Kallender, Paul. 'Waking Up to a New Threat: Cyber

Threats and Space'. *TRANSACTIONS OF THE JAPAN SOCIETY FOR AERONAUTICAL AND SPACE SCIENCES, AEROSPACE TECHNOLOGY JAPAN* 12, no. ists29 (2014): Tv_1-Tv_10. https://doi.org/10.2322/tastj.12.Tv_1.

xvii. Klotz, Irene. 'Burgeoning Satellite Industry Paving Way To $1 Trillion Space Economy | Aviation Week Network', 2021. https://aviationweek.com/aerospace/program-management/burgeoning-satellite-industry-paving-way-1-trillion-space-economy.

xviii. Konkimalla, Hari Sourabh. 'An Analysis of the Security of the Global Positioning System (GPS) and Proposed Solutions', 2023. https://doi.org/10.7939/R3-3KY4-A853.

xix. Kovacs, Eduard. 'Ransomware Group Claims Theft of Valuable SpaceX Data From Contractor'. SecurityWeek, 14 March 2023. https://www.securityweek.com/ransomware-group-claims-theft-of-valuable-spacex-data-from-contractor/.

xx. Lis, Jessica. 'Secure World Foundation Releases 2023 Update to Counterspace Report'. Payload, 14 April 2023. https://payloadspace.com/secure-world-foundation-releases-2023-update-to-counterspace-report/.

xxi. Manulis, M., C. P. Bridges, R. Harrison, V. Sekar, and A. Davis. 'Cyber Security in New Space: Analysis of Threats, Key Enabling Technologies and Challenges'. *International Journal of Information Security* 20, no. 3 (June 2021): 287–311. https://doi.org/10.1007/s10207-020-00503-w.

xxii. Martina, Michael. 'US Warns Space Companies about Foreign Spying | Reuters'. Accessed 14 March 2024. https://www.reuters.com/world/us/us-warns-space-companies-about-foreign-spying-2023-08-18/.

xxiii. Neal, Mihir. 'Soyuz MS-20 Space Tourism Flight Docks with ISS'. *NASASpaceFlight.Com* (blog), 8 December 2021. https://www.nasaspaceflight.com/2021/12/soyuz-ms-20-tourist-launch/.

xxiv. Norberg, Carol, ed. *Human Spaceflight and Exploration*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013. https://doi.org/10.1007/978-3-642-23725-6.

xxv. Oakley, Jacob G. *Cybersecurity for Space: Protecting the Final Frontier*. For Professionals by Professionals. New York, NY: Apress, 2020.

xxvi. Padhy, Ankit Kumar, and Amit Kumar Padhy. 'Legal Conundrums of Space Tourism'. *Acta Astronautica* 184 (July 2021): 269–73. https://doi.org/10.1016/j.actaastro.2021.04.024.

xxvii. Pavur, James, and Ivan Martinovic. 'Building a Launchpad for Satellite Cyber-Security Research: Lessons from 60 Years of Spaceflight'. *Journal of Cybersecurity* 8, no. 1 (28 January 2022): tyac008. https://doi.org/10.1093/cybsec/tyac008.

xxviii. ———. 'The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space'. In *2019 11th International Conference on Cyber Conflict (CyCon)*, 900:1–18, 2019. https://doi.org/10.23919/CYCON.2019.8756904.

xxix. Rafferty, Dylan, and Kevin Curran. 'The Role of Blockchain in Cyber Security'. *Semiconductor Science and Information Devices* 3, no. 1 (21 May 2021). https://doi.org/10.30564/ssid.v3i1.3153.

xxx. Rodofile, Nicholas R., Kenneth Radke, and Ernest Foo. 'Extending the Cyber-Attack Landscape for SCADA-Based Critical Infrastructure'. *International Journal of Critical Infrastructure Protection* 25 (June 2019): 14–35. https://doi.org/10.1016/j.ijcip.2019.01.002.

xxxi. Salahdine, Fatima, and Naima Kaabouch. 'Social Engineering Attacks: A Survey'. *Future Internet* 11, no. 4 (2 April 2019): 89. https://doi.org/10.3390/fi11040089.

xxxii. Samoudi, رزق. 'The Right to Self-Defense in Response to Cyber-Attacks in Light of International Law'. *مجلة جامعة الشارقة للعلوم القانونية*, 15 no. 2 (31 December 2018): 336–62. https://doi.org/10.36394/jls.v15.i2.12.

xxxiii. Schmitz, Jan, Matthieu Komorowski, Thais Russomano, Oliver Ullrich, and Jochen Hinkelbein. 'Sixty Years of Manned Spaceflight—Incidents and Accidents Involving Astronauts between Launch and Landing'. *Aerospace* 9, no. 11 (2 November 2022): 675. https://doi.org/10.3390/aerospace9110675.

xxxiv. Sheer, Abbas, and Shouping Li. 'Space Debris: A New Broadway to Address Organizational and Operational Aspects for Removal'. *Journal of East Asia and International Law* 12, no. 2 (30 November 2019): 269–82. https://doi.org/10.14330/jeail.2019.12.2.02.

xxxv. Smith, Marshall, Douglas Craig, Nicole Herrmann, Erin Mahoney, Jonathan Krezel, Nate McIntyre, and Kandyce Goodliff. 'The Artemis Program: An Overview of NASA's Activities to Return Humans to the Moon'. In *2020 IEEE Aerospace Conference*, 1–10. Big Sky, MT, USA: IEEE, 2020. https://doi.org/10.1109/AERO47225.2020.9172323.

xxxvi. Van Camp, Charlotte, and Walter Peeters. 'A World without Satellite Data as a Result of a Global Cyber-Attack'. *Space Policy* 59 (February 2022): 101458. https://doi.org/10.1016/j.spacepol.2021.101458.

xxxvii. White, Susan, and Protiti Dastidar. 'Lockheed Martin Acquisitions: Stay the Course or Change Strategy?' *The CASE Journal* 17, no. 4 (12 October 2021): 494–541. https://doi.org/10.1108/TCJ-08-2020-0112.

xxxviii. Zolfagharifard, Ellie. 'Russian Cosmonaut "accidentally Infected International Space Station" with USB Stick | Daily Mail Online', 2013. https://www.dailymail.co.uk/sciencetech/article-2503352/Russian-cosmonaut-accidentally-infected-International-Space-Station-USB-stick.html.

xxxix. Jackson, A. (2024, June 29). *Cyberattacks in Space? The "Next Frontier" for Cybersecurity*. Cybermagazine.com; Bizclik Media Ltd. https://cybermagazine.com/hacking-malware/cyberattacks-in-space-the-next-frontier-for-

cybersecurity

xl. Varadharajan, V., & Suri, N. (2023). Security challenges when space merges with cyberspace. *Space Policy*, 101600. https://doi.org/10.1016/j.spacepol.2023.101600

xli. Williams, K. (2021). *Space Crime Continuum: Discussing Implications of the First Crime in Space*.