Canadian Journal of Law and Technology

Volume 21 | Number 1 Article 5

7-2023

The Need for Cyber Resilience of Space Assets: Law and Policy Considerations of Ensuring Cybersecurity in Outer Space

Daniella Febbraro
University of Ottawa, Faculty of Law

The Need for Cyber Resilience of Space Assets: Law and Policy Considerations of Ensuring Cybersecurity in Outer Space

Daniella Febbraro[*]

1. INTRODUCTION

In 2018, NASA's Jet Propulsion Laboratory was the subject of a data breach where over 500 megabytes of data from a major mission system was stolen by hackers.[1] This attack affected NASA's Deep Space Network, prompting the United States Johnson Space Center to disconnect the International Space Station from the affected gateway due to fears that mission systems could become compromised.[2] NASA has acknowledged that its vast online presence, which includes thousands of publicly accessible datasets, offers a large potential target for cybercriminals.[3] The 2018 incident was one of many, with NASA experiencing more than 6000 cyberattacks from 2017-2021 alone.[4]

But NASA is not the only target — cyberattacks on space assets continuously occur around the globe.[5] Outer space is experiencing unprecedented transformation, with more satellites being built and deployed than ever before.[6] Increasing reliance on satellite communication, satellite data, Earth observation services, and "cloud" ecosystems creates a new domain for cyberattacks that can affect any space mission.[7] This means that there is a growing need to minimize exposure to cyberthreats to protect the global population and economy.[8]

---

[*] JD, MSc. Thank you to Professor Vivek Krishnamurthy for his comments, support, and encouragement.

1 See Office of Inspector General, "Cybersecurity Management and Oversight at the Jet Propulsion Laboratory" (18 June 2019) at 3, online (pdf): *National Aeronautics and Space Administration* < oig.nasa.gov/docs/IG-19-022.pdf > .

2 *Ibid* at 19.

3 See Office of Inspector General, "NASA's Cybersecurity Readiness" (18 May 2021) at 3, online (pdf): *National Aeronautics and Space Administration* < oig.nasa.gov/docs/IG-21-019.pdf > [NASA's Readiness].

4 *Ibid* at 7.

5 See e.g., "ALMA Successfully Restarted Observations" (20 December 2022), online: *ALMA* < alma-telescope.jp/en/news/63a0f09493398 > (recently, the ALMA observatory in Chile suffered a cyberattack on its computer systems, forcing operations to be suspended for a total of 48 days). See also Debra Werner, "Russian invasion of Ukraine exposes cybersecurity threat to commercial satellites," *SpaceNews* (14 April 2022), online: < spacenews.com/russian-invasion-of-ukraine-exposes-cybersecurity-threat-to-commercial-satellites/ > .

6 See Brad Grady et al, "Space Cybersecurity: Current State and Future Needs" (2022) Northern Sky Research White Paper at 4.

Why is protecting space assets from cyberattacks so important? Because vulnerabilities associated with space assets like satellites pose serious risks to critical infrastructure on Earth.[9] Many existing satellites have been in service for over a decade, were not launched with modern technology, and were not designed with cybersecurity in mind.[10] Cyberattacks on space assets could therefore result in the targeting of governments, private corporations, or individuals; cybercrimes or espionage activities; the spread of misinformation or disinformation; and disruption to critical infrastructure systems like power grids, communication networks, transportation systems, water systems, or financial services.[11]

Considering the growth of the industry and the technology in use, cyberattacks on space assets should be expected.[12] Traditional methods and past practices lacking organized approaches to cybersecurity will not be sufficient to prevent cyberattacks from occurring.[13] In this article, it is argued that States must move towards "comprehensive and evolving"[14] cybersecurity strategies that can provide full life cycle protection to space assets. To accomplish this, I propose that an international, industry-specific cybersecurity standard be developed and imposed on all space actors.

2. POTENTIAL ATTACK SURFACES AND THREATS

Space missions are supported by three areas of infrastructure that can present potential attack surfaces: (1) the ground segment, (2) the space segment, and (3) the control segment. The ground segment is mission control — those based on Earth that provide support to the space asset. The space segment is the space asset itself, whether that be a satellite, a crewed vehicle, or another type of payload. The control segment is the set of commands that travel between the ground segment and the space segment.[15] Each segment presents its own

---

7 See Stefano Zatti, "Space and Cyber Threats" in Kai-Uwe Schrogl et al, eds, *Handbook of Space Security: Policies, Applications and Programs*, 2nd ed (Switzerland: Springer Nature, 2020) 245 at 248.

8 Grady, *supra* note 6 at 4.

9 See Salvador Llopis Sanchez et al, "Cybersecurity Space Operation Center: Countering Cyber Threats in the Space Domain" in Kai-Uwe Schrogl et al, eds, *Handbook of Space Security: Policies, Applications and Programs*, 2nd ed (Switzerland: Springer Nature, 2020) 921 at 923-924.

10 See Graham Wright, "Cybersecurity in the Space Age" (2020) 62:2 ITNOW 60 at 60. See also Vilius Petkauskas, "Space Security in 2022: expect a hacked satellite," *CyberNews* (10 January 2022), online: <cybernews.com/security/space-security-in-2022-expect-a-hacked-satellite/> [Space Security in 2022].

11 Sanchez et al, *supra* note 9 at 923-924.

12 Space Security in 2022, *supra* note 10.

13 Grady, *supra* note 6 at 6; NASA's Readiness, *supra* note 3 at 3.

14 Grady, *supra* note 6 at 6.

15 Zatti, *supra* note 7 at 251-252.

opportunity for cyberattacks, with an attack on any segment potentially affecting the entire space mission.[16] Additionally, the rapidly growing network of connected devices, commonly referred to as the Internet of Things (''IoT''), presents security challenges that provide additional attack surfaces on space missions.[17]

In general, cyberattacks affecting a space mission can be categorized into two main groups: (1) threats targeted towards information (like obtaining data or infiltrating command centres), and (2) threats targeted towards infrastructure (like affecting onboard components, launch capabilities, or payloads).[18] These threats can be intentional and malicious, or they can be the outcome of unintentional human error,[19] like when virus-infected devices were connected to networks on the International Space Station.[20]

Depending on the attack surface and the type of threat, a cyberattack on a space mission could lead to:

(a) Unauthorized operation of the spacecraft, potentially leading to the loss of data, the payload, or the entire mission;
(b) Unavailability of communications for commands and telemetry during a spacecraft's critical maneuvers during launch, trajectory correction, or collision avoidance, potentially leading to the loss of the spacecraft or the entire mission;
(c) Theft or destruction of equipment and information, including potential loss of critical mission information or confidential information; or
(d) Unavailability of critical services or destruction of critical infrastructure on Earth, including navigation and communication services.[21]

Any vulnerability associated with a space mission can be exploited, ''resulting in a compromise of the properties of information assurance of the system, namely, confidentiality, integrity, or availability.''[22] Given the commercialization of space and the interconnectivity of networks, the confidentiality, integrity, and availability triad ''is flipping.''[23] A shift in emphasis towards integrity of space systems is occurring.[24] Researchers and hackers alike are testing the integrity of space assets by conducting controlled experiments to demonstrate the ease with

[16] *Ibid.*

[17] See ''IoT Security Issues'' (last visited 27 December 2022), online: *Check Point* < www.checkpoint.com/cyber-hub/network-security/what-is-iot-security/iot-security-issues/# > .

[18] Sanchez et al, *supra* note 9 at 928.

[19] Zatti, *supra* note 7 at 247-248.

[20] See Samuel Gibbs, ''International Space Station attacked by 'virus epidemics,'" *The Guardian* (12 November 2013), online: < www.theguardian.com/technology/2013/nov/12/international-space-station-virus-epidemics-malware > .

[21] Zatti, *supra* note 7 at 251, 253-254, 259.

[22] *Ibid* at 247-248.

[23] Grady, *supra* note 6 at 11.

[24] *Ibid.*

which satellites can be hacked.[25] This recognition of the importance of "cyber resilience"[26] has led to countries placing cybersecurity at the forefront of their policy agendas.[27]

3. LEGAL AND POLICY CONSIDERATIONS ASSOCIATED WITH CYBERSECURITY IN OUTER SPACE

The interconnectivity of potentially billions of users relying on space assets vulnerable to cyberattacks presents challenges to legal procedures and the governance of both outer space and cyberspace.[28] Countries are becoming increasingly concerned about potential threats to critical infrastructure that could result from a cyberattack.[29] However, cybersecurity in outer space is an unknown warzone, with the law of cyberspace not fully developed and the law of outer space remaining vague and unmodernized. In this landscape, international consensus regarding operational principles in the digital age are consistently violated.[30] This leaves tough questions for law and policy makers to consider. Notably, how should cybersecurity in outer space be governed, and who should be responsible if something goes wrong?

The law of outer space is governed by five main international treaties, including the *Treaty on Principles Governing Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies* (the "Outer Space Treaty") and the *Convention on International Liability for Damage Caused by Space Objects* (the "Liability Convention").[31] The Outer

---

[25] See Vilius Petkauskas, "Satellite hackers can see every website you visit, every email you get," *CyberNews* (26 August 2022), online: < cybernews.com/security/satellite-hackers-guide-to-space/ > . See also Lily Hay Newman, "Researchers Used a Decommissioned Satellite to Broadcast Hacker TV," *Wired* (30 March 2022), online: < www.wired.com/story/satellite-hacking-anit-f1r-shadytel/ > .

[26] See Rich Isenberg et al, "Building cyber resilience in national critical infrastructure" (30 June 2021), online: *McKinsey & Company* < www.mckinsey.com/capabilities/risk-and-resilience/our-insights/building-cyber-resilience-in-national-critical-infrastructure > .

[27] See e.g., Bill C-26, *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*, 1st Sess, 44th Parl, 2022 (second reading 27 March 2023); Office of the Press Secretary, "Presidential Policy Directive (PPD-21) — Critical Infrastructure Security and Resilience" (12 February 2013), online: *The White House* < obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil > . See also Melissa Hathaway, "Getting Beyond Norms: When Violating the Agreement Becomes Customary Practice" in Paul Cornish, ed, *The Oxford Handbook of Cyber Security* (Oxford: Oxford University Press, 2021) 562 at 562.

[28] See International Institute of Space Law, *Six Decades of Space Law and its Development(s) (1960-2020)* (Paris: International Institute of Space Law, 2020) at 58.

[29] Hathaway, *supra* note 27 at 562.

[30] *Ibid.*

[31] *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies*, 27 Jan 1967, 610 UNTS 205 [*Outer*

Space Treaty emphasizes that space must be used for peaceful purposes and the benefit of all.[32] Activities in outer space must be carried on in accordance with international law, and States must have due regard for the interests of others.[33] According to the Outer Space Treaty, States are responsible for all national activities in outer space and are internationally liable for any damage to another State.[34] The principles governing liability for damage are further explained in the Liability Convention.[35]

The Outer Space Treaty and Liability Convention were written before cybersecurity and cyberattacks were on the minds of law and policy makers. Because of this, there is no mention of how to address cybersecurity in outer space or what processes to follow in the event of a cyberattack. Furthermore, the Outer Space Treaty and Liability Convention are relatively vague, lacking clear definitions for most principles. Therefore, the Outer Space Treaty and Liability Convention do not provide a conceivable basis for ensuring cybersecurity in outer space.[36]

Conversely, cyberspace is governed mostly by soft law.[37] Many of the principles of how cyberspace should be governed are outlined in the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (the "Tallinn Manual").[38] The Tallinn Manual has been complemented by the attempts of private actors to create simplified and clear guiding principles to follow throughout cyber operations. These include the Digital Geneva Convention, the Charter of Trust, and the Paris Call.[39]

Though far from hard law, the principles that could govern cybersecurity in outer space are best laid out in the Tallinn Manual. According to the Tallinn Manual, States "must not conduct cyber operations that violate the sovereignty of another State" and "must exercise due diligence."[40] These principles follow

---

Space Treaty]; *Convention on International Liability for Damage Caused by Space Objects*, 29 March 1972, 961 UNTS 187 [*Liability Convention*].

32 *Outer Space Treaty*, *ibid*, arts I, III.

33 *Ibid*, arts III, IX.

34 *Ibid*, arts VI, VIII.

35 *Liability Convention*, *supra* note 31, arts I-III.

36 See David Livingstone & Patricia Lewis, "Space, the Final Frontier for Cybersecurity" (2016) International Security Department Research Paper at 31.

37 International Institute of Space Law, *supra* note 28 at 58.

38 See Michael N Schmitt & Liis Vihul, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017).

39 See Brad Smith, "The need for a Digital Geneva Convention" (14 February 2017), online: *Microsoft* < blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/ > ; "Our 10 Principles: Cybersecurity Concerns Us All" (last visited 12 December 2022), online: *Charter of Trust* < www.charteroftrust.com/about/ > ; "The 9 Principles" (11 December 2018), online: *Paris Call* < https://pariscall.international/en/principles > .

40 Schmitt & Vihul, *supra* note 38 at 17-27, 30-50.

international law and align with the text of the Outer Space Treaty. Furthermore, the Tallinn Manual explicitly states that "cyber operations involving space objects are subject to the responsibility and liability regime of space law."[41] However, the Tallinn Manual notes that the reference to international law in the Outer Space Treaty could act as a hinderance against "imposing any obligation to refrain from cyber activities in outer space that is broader than those already expressly set forth in international law."[42] The lack of guidance in the Outer Space Treaty and other international law instruments, as well as the omission of any principles specific to cybersecurity in the Outer Space Treaty, could affect how issues relating to cyberattacks in outer space are both governed and resolved.

There are several other issues associated with governing cybersecurity in outer space. First, not all States are bound by the Outer Space Treaty and the Liability Convention, with only 135 parties to the Outer Space Treaty and 121 parties to the Liability Convention.[43] Second, under general international law, the due diligence obligation generally attaches only when there are "serious adverse consequences," so States may be exempt from this requirement when cyberattacks fall short of this threshold.[44] Third, when a cyberattack occurs, States are only required to terminate the harmful activity; they are not required to take preventative measures.[45] This reactive approach will likely not be sufficient to protect the global population and critical infrastructure from a serious cyberattack involving outer space.[46] Finally, according to the Outer Space Treaty and the Liability Convention, a State that is the subject of a cyberattack that causes harm is liable for any damage, as opposed to the State where the cyberattack originates.[47]

To circumvent these challenges, States must focus on consumer protection and citizen safety, which can be achieved by introducing responsibility and accountability through product liability.[48] Additionally, an international, industry-specific cybersecurity standard with clear definitions and guiding principles can be developed and imposed on all space actors to help govern cybersecurity in outer space.

---

41 *Ibid* at 280.

42 *Ibid* at 275.

43 See Committee on the Peaceful Uses of Outer Space, *Status of International Agreements relating to activities in outer space as at 1 January 2022*, UNCOPUOS, 61st Sess, UN Doc A/AC.105/C.2/2022/CRP.10 (2022).

44 See Michael N Schmitt, "Cybersecurity and International Law" in Robin Geiß & Nils Melzer, eds, *The Oxford Handbook of the International Law of Global Security* (Oxford: Oxford University Press, 2021) 661 at 671-672.

45 *Ibid.*

46 Sanchez et al, *supra* note 9 at 922.

47 *Outer Space Treaty*, *supra* note 31, arts VI, VIII; *Liability Convention*, *supra* note 31, arts I-III.

48 Hathaway, *supra* note 27 at 572-573.

4. RECOMMENDATIONS AND POTENTIAL SOLUTIONS

To build adequate defenses, space actors must assume that a cyberattack is imminent. They must then build a unified, integrated cyber-defense that protects assets.[49] While national standards for cybersecurity in outer space are being developed,[50] an international standard specific to the space domain would ensure stronger protection for both critical infrastructure and the global population. Furthermore, an international standard would help to circumvent uncertainties that exist in the current space law and cyberspace domain. Finally, in an era where complex supply chains make it challenging to attribute liability,[51] an international standard could also assist in ensuring no space actor leaves their space assets vulnerable to cyberattack.

Any international standard developed to address cybersecurity in outer space must recognize that both the cyber domain and the space domain are highly dynamic.[52] Furthermore, attempts to govern this area must acknowledge the importance of consumer protection, as well as the free flow of information and rights to privacy.[53] Civilian interests become especially important when remote communities are considered, as satellites are crucial in providing many essential services in remote and rural areas.[54] Satellite services can also ensure maintained connectivity and freedom of speech in times of war or domestic conflicts.[55]

---

[49] See "Secure design principles" (21 May 2019), online: *National Cyber Security Centre* <www.ncsc.gov.uk/collection/cyber-security-design-principles/cyber-security-design-principles> [National Cyber Security Centre]; "Cyber Security Principles" (June 2022), online: *Australian Cyber Security Center* <www.cyber.gov.au/acsc/view-all-content/advice/cyber-security-principles> [Australian Cyber Security Center]; Tony Hubbard et al, "Zero Trust in a Virtual Cybersecurity World" (2021) 70:2 J Government Financial Management 13; Scott Rose et al, "Zero Trust Architecture" (2020) National Institute of Standards and Technology Special Publication 800-207.

[50] See "The EU Faces Legal Changes Ahead for Cybersecurity in Space" (12 November 2021), online: *Satellite Today* <link.gale.com/apps/doc/A682549810/ITBC?u=otta77973&sid=bookmark-ITBC&xid=bad3ef0d>; Sandra Erwin, "Air Force to require cybersecurity audits of commercial satellite communications providers," *SpaceNews* (8 November 2019), online: <spacenews.com/air-force-to-require-cybersecurity-audits-of-commercial-satellite-communications-providers/>.

[51] See Gregory Falco, "Job One for Space Force: Space Asset Cybersecurity" (July 2018) at 13, online (pdf): *Harvard Kennedy School Belfer Center for Science and International Affairs* <www.belfercenter.org/sites/default/files/files/publication/CSP%20Falco%20Space%20Asset%20-%20FINAL.pdf>.

[52] Sanchez et al, *supra* note 9 at 924.

[53] *Ibid.*

[54] See National Research Council Canada, "Satellite communications bridge the digital divide between urban and remote areas" (10 February 2021), online: *Government of Canada* <nrc.canada.ca/en/stories/satellite-communications-bridge-digital-divide-between-urban-remote-areas>.

[55] See Vera Bergengruen, "'It's Our Home Turf.' The Man on Ukraine's Digital Frontline," *Time* (15 March 2022), online: <time.com/6157308/its-our-home-turf-the-man-on-ukraines-digital-frontline/>; Karl Vick, "Receivers for Elon Musk's

Therefore, States have a responsibility to require space actors to implement cybersecurity principles in all aspects of space missions and infrastructure.[56] To accomplish this, secure design principles, full life cycle protection, and a "zero-trust framework" should be implemented in the use of all space assets.[57]

Cybersecurity in all phases of space missions should be a top priority from initial design, to launch, to service, to end of life.[58] Ground segments, users, and devices connected to networks must also be considered.[59] Basic principles of cybersecurity should continue to be implemented. This includes end-to-end security, which encompasses internal and external access controls; personnel vetting, training, and oversight; security risk assessments; prevention, mitigation, detection, and reaction protocols; and information assurance, including firewalls, encryption, and authorization.[60] A zero-trust framework can assist in ensuring that these principles are maintained and can increase cyber resilience of the space domain.[61]

An increased focus on cybersecurity by implementing aspects of these principles can be seen globally. For example, the United States Space Force is implementing cyber training into missions, and the European Space Agency is implementing an International Organization for Standardization protocol focussed on information security, cybersecurity, and privacy protection.[62] Additionally, Canada has proposed new legislation to protect critical cyber systems and is testing new technology to ensure protection of space communications.[63]

Starlink Internet Are Being Smuggled Into Iran," *Time* (22 October 2022), online: < time.com/6223999/starlink-iran-elon-musk/ > .

[56] See e.g. *Developments in the field of information and telecommunications in the context of international security, and advancing responsible State behaviour in the use of information and communications technologies*, GA Res 76/19, UNGA, 76th Sess, UN Doc A/Res/76/19 (2021).

[57] National Cyber Security Centre, *supra* note 49; Australian Cyber Security Center, *supra* note 49; Hubbard et al, *supra* note 49; Rose et al, *supra* note 49.

[58] See "SpiderOak Space Cybersecurity Solutions" (last visited 27 December 2022), online: *SpiderOak* < spideroak.com/space/ > ; Sanchez et al, *supra* note 9 at 928.

[59] See Brandon Bailey, "Protecting Space Systems from Cyber Attack" (31 March 2022), online: *The Aerospace Corporation* < aerospacecorp.medium.com/protecting-space-systems-from-cyber-attack-3db773aff368 > .

[60] Zatti, *supra* note 7 at 254-255, 259.

[61] See "What is zero trust?" (last visited 27 December 2022), online: *IBM* < www.ibm.com/topics/zero-trust > .

[62] See Mike Slater, "Space Force embeds Cyber Squadrons into delta missions" (11 October 2022), online: *Joint Task Force-Space Defense* < www.jtf-spacedefense.mil/News/Article/3191613/space-force-embeds-cyber-squadrons-into-delta-missions/ > ; Zatti, *supra* note 7 at 257; "ISO/IEC 27005:2022" (last visited 15 December 2022), online: *ISO* < www.iso.org/standard/80585.html > .

[63] See Bill C-26, *supra* note 27; Canadian Space Agency, "Cybersecurity from space: the Government of Canada invests in quantum technology" (14 June 2019), online:

Perhaps the best example of a comprehensive commitment to cybersecurity can be seen in the European Union. The Network and Information Security ("NIS") Directive aimed "to achieve a high common level of cybersecurity" across the European Union, while the NIS2 Directive expands this scope to include more sectors, including outer space.[64] Furthermore, the Critical Entities Resilience Directive recognizes the increasing interconnectivity of services and aims to improve resilience of critical entities by establishing comprehensive obligations and international cooperation.[65] These directives are complemented by the standards established in both the *Cybersecurity Act*, which introduces a cybersecurity certification framework, and the *Cyber Resilience Act*.[66] Focussing on the security of both hardware and software components of connected devices, the *Cyber Resilience Act* introduces cybersecurity by design and imposes financial penalties on manufacturers for non-compliance.[67] Products that do not meet essential requirements will not be allowed entry to the market, increasing transparency, security, and trust for consumers.[68]

Though progress is being made, national cybersecurity developments lack the unified coordination required to ensure global protection. For this reason, existing principles, a zero-trust framework, and the European Union's

---

Government of Canada <www.canada.ca/en/space-agency/news/2019/06/cybersecurity-from-space-the-government-of-canada-invests-in-quantum-technology.html>.

64 See European Parliamentary Research Service, "The NIS2 Directive: A high common level of cybersecurity in the EU" (February 2023), online (pdf): *European Parliament* <www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf>; EC, *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*, [2022] OJ, L 333/80.

65 See EC, *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC*, [2022] OJ, L 333/164.

66 See EC, *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*, [2019] OJ, L 151/15; "Cyber Resilience Act" (15 September 2022), online: *European Commission* <digital-strategy.ec.europa.eu/en/library/cyber-resilience-act> [Cyber Resilience Act]; "Europe's Internet of Things Policy" (last visited 27 December 2022), online: *European Commission* <digital-strategy.ec.europa.eu/en/policies/internet-things-policy>.

67 See Mike Nelson, "EU announces first ever move to legislate cybersecurity for IoT," *IoT Business News* (12 October 2022), online: <iotbusinessnews.com/2022/10/12/63479-eu-announces-first-ever-move-to-legislate-cybersecurity-for-iot/>; "New EU cybersecurity rules ensure more secure hardware and software products" (15 September 2022), online: *European Commission* <digital-strategy.ec.europa.eu/en/news/new-eu-cybersecurity-rules-ensure-more-secure-hardware-and-software-products>.

68 Cyber Resilience Act, *supra* note 66; Nelson, *ibid.*

cybersecurity initiatives can be used as a foundation for an international, space-specific cybersecurity framework. An international framework would complement national regulations to ensure that there is centralized supervision and enforcement of cybersecurity principles in outer space. The United Nations Committee on the Peaceful Uses of Outer Space ("UNCOPUOS"), tasked with governing the use of outer space, could create a working group to develop guidelines on cybersecurity standards for the space domain.[69] In these guidelines, terms should be fully defined, liability should be clearly allocated, and guiding principles should cover the lifespan of space assets and address existing devices connected to networks. In this way, the "hard law" of outer space can be integrated with the "soft law" framework of cyberspace.[70]

5. CONCLUSION

The rapid expansion of networks and the growing global interconnectivity of devices present challenges to ensuring cybersecurity, further complicated by the IoT and aging devices lacking adequate protection.[71] The issue is compounded in the context of outer space, given the vast reliance on satellites and other space assets, as well as the unmodern and vague legal regime governing the domain.[72] To protect critical infrastructure and the global population, an international, space-specific cybersecurity standard should be developed. This standard would be a soft law instrument, using existing cybersecurity principles, a zero-trust framework, and the European Union's cybersecurity initiatives as foundations for its development. UNCOPUOS is a candidate for organizing and overseeing the development of this standard to ensure that all guidelines abide by international law principles.

Cyber resilience of space assets is crucial in ensuring continuous functionality of infrastructure by preventing, detecting, and managing cyberattacks.[73] By introducing a universal standard, space actors will be allowed to develop innovative technologies of the future, while keeping one eye on the past, all with a perspective of protecting the global community.

---

[69] See "Committee on the Peaceful Uses of Outer Space" (last visited 27 December 2022), online: *United Nations Office for Outer Space Affairs* <www.unoosa.org/oosa/en/ourwork/copuos/index.html>.

[70] International Institute of Space Law, *supra* note 28 at 58.

[71] Sanchez et al, *supra* note 9 at 925.

[72] See generally Livingstone & Lewis, *supra* note 36. See also Sanchez et al, *ibid*.

[73] See Julius Melnitzer, "Cyber resilience, not just cybersecurity, is the key to managing cyberattacks," *Law Times* (9 November 2022), online: <www.lawtimesnews.com/practice-areas/privacy-and-data/cyber-resilience-not-just-cybersecurity-is-the-key-to-managing-cyberattacks/371367>; "Why cyber resilience is important" (last visited 28 December 2022), online: *IBM* <www.ibm.com/topics/cyber-resilience#:~:text=A%20cyber%20resilience%20strategy%20is,financial%20loss%20and%20reputational%20damage>.