J. East Asia & Int'l L. Vol. 15/No.1 (2022); 93-108
Publication type : Research Article
Section : Notes & Comments
DOI : http://dx.doi.org/10.14330/jeail.2022.15.1.05

Global Internet Access from the Low Earth Orbit: Legal Issues regarding Cybersecurity in Outer Space

Chandaphan Suwijak* & Shouping Li**

The emergence of global internet access from the low Earth orbit (LEO) comes with cybersecurity vulnerabilities. Under international space law regimes, the concept of cybersecurity in outer space remains ambiguous. Furthermore, cyberattacks affecting the era's thoroughly segregated computer space systems were unimagined. Cyber borders are not the same as physical borders. Cyberspace does not admit the demarcation of territorial sovereignty, as it is not based on physical location, and assigning territorial sovereignty to cyberspace is time-consuming. This research proposes the concept of a multi-stakeholder international legal regime for space cybersecurity, as establishing cybersecurity standards and risk management mechanisms necessitates technical measures and a regulatory framework. International cooperation is the only way to provide a fully coordinated approach to cyberspace protection which is consistent with the fundamental premise of international cooperation and collaboration in space.

Keywords
Global Internet Access, Small-satellite Constellations, Cybersecurity in Outer Space, Low Earth Orbit

* Ph.D. candidate at Beijing Institute of Technology. LL.B. (Mae Fah Luang U.), LL.M. (Chulalongkorn). ORCID: http://orcid.org/0000-0002-1850-4077. The author may be contacted at: suwijak.cha@mfu.ac.th /Address: Beijing Institute of Technology, School of Law, No. 5th South Zhongguancun Street Haidian, Beijing 100081 P.R. China.

** Professor of International Law, Dean of the Law School, Director of the Space Institute at the Beijing Institute of Technology. Ph.D. (Wuhan) / Post-Doc (Fudan). The author may be contacted at: lishouping@bit.edu.cn /Address: Beijing Institute of Technology, School of Law, No. 5 South Zhongguancun Street, Haidian, Beijing 100081, China.
All the websites cited in this article were last visited on May 1, 2022.

1. An Overview of Satellite Internet Constellations in the Low Earth Orbit

As all elements of economic activity are reliant on the Internet communications, web-connectivity has emerged as a key component of every country's social and industrial infrastructure.[1] Despite the rapid expansion of the Internet connectivity around the world, however, substantial gaps remain in the Internet usage and infrastructure, especially in Asian countries, most of which are still developing.[2] Current applications of satellite technologies include fiber optic cables and other high-capacity technologies that are not economically viable in rural and remote communities of landlocked developing countries because of low population densities and long distances between high-capacity and last-mile networks.[3]

The Internet communication infrastructure is now more critical than ever due to Covid-19. The global pandemic has forced workers and children to stay at home, highlighting the need for universal connectivity.[4] Since the 1960s, the Internet satellites in geostationary orbits (GEO) have demonstrated their value for quite capable and lengthy service. Their altitude-more than 35,786 km above the Earth-provides a large field of view, enabling operators to cover most of the planet's surface with three satellites positioned at appropriate intervals.[5] Customers who reside in sparsely populated areas and who are not served by regular Internet service providers can still benefit from the service. Given the high costs of laying expensive cables or fiber, terrestrial service providers tend to concentrate their efforts on urban and suburban areas where there is a high concentration of people.[6]

In contrast to the Internet satellites in GEO, the latest small satellite constellations in low Earth orbit (LEO)-between 180 and 2,000 km above the Earth's surface[7]-provide the Internet connection worldwide, allowing faster communication (lower latency)

1 Vignan Velivela, *Small satellite constellations: The promise of Internet for all*, 107 ORF Issue Brief, 1 (2015), https://orfonline.org/wp-content/uploads/2015/12/IBrief1071.pdf.

2 John Garrity & Arndt Husar, *Digital Connectivity and Low Earth Orbit Satellite Constellations: Opportunities for Asia and the Pacific* 2-3 (ADB Sustainable Development Working Paper Series No. 76, Api. 2021), https://www.adb.org/sites/default/files/publication/696521/sdwp-076-digital-connectivity-low-earth-orbit-satellite.pdf.

3 *Id*. at 3.

4 ILO, Teleworking during the COVID-19 pandemic and beyond: A Practical Guide 5-6 (2020), https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/instructionalmaterial/wcms_751232.pdf.

5 Audrey Allison, The ITU and managing satellite orbital and spectrum resources in the 21st century 8 (2014).

6 Rock Networks, Fibre vs Satellite: Who is the Winner?, Rock Networks Website (Feb. 7, 2022), https://www.rocknetworks.com/fibre-vs-satellite-who-is-the-winner.

7 Kiran Nair, Small Satellites and Sustainable Development-Solutions in International Space Law 56 (2019).

with more capacity per user than GEO satellites.[8] According to the International Telecommunication Union (ITU), around 2.9 billion people around the world could not access the Internet in 2021.[9] This scenario offers an important business opportunity for the private sector, as there are already several companies working on the construction of small satellite constellations to provide the Internet access for their customers from LEO. These constellations are also considerably closer to the Earth's surface than traditional satellites, so that there is almost no delay in the transmission of data.[10] Consequently, the increasing number of small satellites in LEO will transform how we live and work in the ways that have not been witnessed since the Industrial Revolution, especially in terms of global Internet coverage.

2. Outstanding Projects for the Satellite Internet Constellations

Over the last few decades, significant efforts have been made in designing, manufacturing, and deploying satellites for various functions. Recently, satellite networks called satellite constellations have been established where the number of small satellites is constantly expanding up to tens of thousands primarily in LEO for various objectives, including delivering communication services to remote places.[11] Today, the use of these small satellites is dominating the satellite communications industries. Since the first Iridium (with 70 satellites), Globalstar (with 24 satellites) and Orbcomm (with 18 satellites) have been sent into LEO and served as pioneers of a new wave of satellite constellation phenomena.[12] The following section will discuss four noticeable constellation projects[13] being planned to connect the entire world via small satellite

8 Alberto Carazo, *Mega-Constellations: Legal Aspects*, *in* Promoting Productive Cooperation Between Space Lawyers and Engineers 141 (A. Pecujlic & M. Tugnoli eds., 2019).

9 ITU, Facts and Figures 2021: 2.9 billion people still offline, (Nov. 29, 2021), https://www.itu.int/hub/2021/11/facts-and-figures-2021-2-9-billion-people-still-offline.

10 Clement Hearey, *When You Wish Upon a "Starlink": Evaluating the FCC's Actions to Mitigate the Risk of Orbital Debris in the Age of Satellite "Mega-Constellations,"* 72 Admin. L. Rev. 753 (2020), https://administrativelawreview.org/volume-72-issue-4.

11 Stefano Gallozzi, et al., Concerns about ground based astronomical observations: A step to Safeguard the Astronomical Sky, arXiv website (Feb. 3, 2020), at 3, https://arxiv.org/pdf/2001.10952.pdf.

12 Nikita Bhakare, *The Need for Evolving Legal Framework for Regulation of Space Debris Caused by Satellite Constellations*, 8th European Conference on Space Debris Proc. 1 (2021), https://conference.sdo.esoc.esa.int/proceedings/sdc8/paper/310/SDC8-paper310.pdf.

13 The other proposals are SES 03B (with 84 satellites), Leosat (with 80 satellites), Samsung (with 4,600 satellites), Boeing (with 2,956 satellites), etc. *See* Shouping Li, Small Satellite Constellation (The Chinese Society of Astronautics & the

constellations.[14]

A. Starlink Project

SpaceX, a private spaceflight company, is developing a satellite constellation network known as "Starlink" to provide low-cost Internet access for, among other users, individuals and inhabitants of remote areas. To date, the United States Federal Communications Commission (FCC) has authorized SpaceX's proposal to launch a constellation of 4,425 satellites, which will be the first phase of their planned orbit fleet of approximately 42,000 satellites.[15] The Starlink satellite constellation differs from others in that its satellites are located at a lower altitude, at around 550 km above the Earth's surface. As a result, a more significant number of satellites is required. Those who live in remote places particularly experience the benefits of this initiative for the Internet access.[16] Currently, the Starlink project is the most advanced satellite deployment, having launched 1,880 satellites (as of February 10, 2021) into LEO.[17] In addition, the life of each satellite is expected to be five to seven years.[18]

B. OneWeb Project

With the same objective of the Starlink project, a startup "OneWeb" - an LEO satellite communications provider co-owned by the Bharti group and the United Kingdom government-intends to launch 650 satellites to 1,200 km above the Earth's surface, thereby establishing a mega-constellation.[19] OneWeb made an application to the FCC in April 2016 to gain access to the US market for their planned LEO satellite system. The OneWeb's constellation is expected to enable broadband connectivity in unserved or underserved regions and support services such as cellular backhaul, mobility, community and residential internet access, and emergency communications

International Academy of Astronautics trans., 2019).

14 This research examines each of these mega-constellations based on their respective United States Federal Communications Commission filings (since 2016).

15 *Supra* note 11, at 1.

16 Tekdeeps, Starlink constellation and legal issues, (June 4, 2021), https://tekdeeps.com/starlink-constellation-and-legal-issues.

17 Elizabeth Howell, NASA is concerned about SpaceX's new generation of Starlink satellites, Space.com (Feb. 26, 2022), https://www.space.com/nasa-collision-risk-starlink#:~:text=There%20are%20currently%20about%201%2C800,encounters%20in%20low%2DEarth%20orbit.

18 *Supra* note 2, at 16.

19 ET Bureau, *OneWeb launches 34 more satellites, expands in-orbit LEO constellation to 288 satellites*, Econ. Times, Aug. 23, 2021, https://economictimes.indiatimes.com/industry/telecom/telecom-news/oneweb-launches-34-more-satellites-expands-in-orbit-leo-constellation-to-288-satellites/articleshow/85555421.cms?from=mdr.

in the US and globally when fully deployed.[20] The OneWeb communication satellites weigh around 150kg a piece and are designed to operate for five to seven years. Each small satellite in the constellation is wired uniquely, with a few electrical devices connecting the various components.[21]

OneWeb has successfully launched 394 satellites into orbit (as of December 2021),[22] which is the second largest company with the number of satellite internet constellation.

C. Lightspeed Project

"Telesat" - the Canadian satellite communications company - is a well-known provider of GEO internet services. Since early stage of satellite communication, Telesat has been researching markets, evolving technology, and improving system design for LEO service.[23] In 2016, it announced the Lightspeed project, aiming to provide global internet coverage from LEO with the most innovative and cutting-edge broadband satellite network globally. The original plan began with an announcement to launch 120 satellites by 2021, whose first satellite was successfully launched in January 2018.[24] In 2020, however, Telesat applied for an extension to build a constellation of 1,600 satellites to meet future demand; the first phase is intended to launch 300 satellites, with 78 satellites in orbit in 2022 and 220 more in 2023.[25] The lifespan of each Lightspeed satellite is expected to be 10 to 12 years.[26] Recently, Telesat has conducted 20 tests with various operators and service providers, including Telefonica.

20 EoPortal Directory, OneWeb Minisatellite Constellation for Global Internet Service, (Feb. 26, 2022), https://directory.eoportal.org/web/eoportal/satellite-missions/o/oneweb#foot7%29.

21 Aerospace Technology, OneWeb Satellite Constellation (Feb. 7, 2020), https://www.aerospace-technology.com/projects/oneweb-satellite-constellation.

22 Tariq Mailik, Soyuz rocket launches 36 OneWeb internet satellites into orbit, Space.com (Dec. 27, 2021), https://www.space.com/soyuz-rocket-launches-one-web-satellites-dec-2021.

23 Larry Press, SpaceX Starlink vs. Telesat Lightspeed, CircleID Website (May 19, 2021), https://circleid.com/posts/20210519-spacex-starlink-vs-telesat-lightspeed.

24 Gerry Nagler, Telesat Begins Deploying Its Global Low Earth Orbit (LEO) Constellation with Successful Launch of Phase 1 Satellite, TELESAT Website (Feb. 27, 2022), https://www.telesat.com/press/press-releases/telesat-begins-deploying- its-global-low-earth-orbit-leo-constellation-with-successful-launch-of-phase-1-satellite.

25 Rachel Jewett, *8 Takeaways from Our SpaceX, Telesat LEO Constellation Webcast*, Via Satellite, July 23, 2020, https://www.satellitetoday.com/broadband/2020/07/23/8-takeaways-from-our-spacex-telsat-leo-constellation-webcast.

26 *Supra* note 2, at 16.

D. Kuiper Project

In 2019, "Amazon"-a US e-commerce company-unveiled the "Kuiper project," intending to deploy a constellation of 3,236 satellites into LEO over the next decade to deliver global low-latency broadband internet access.[27] The concept of the Kuiper project is similar to that of SpaceX's Starlink, OneWeb, and Telesat's Lightspeed, in that it aims to provide regular internet infrastructure for rural communities and other remote regions with the Internet difficulties.[28] Clients in developing countries, passengers on flights and boats, and commercial users who want real-time data from their equipment, such as oil rigs and ocean buoys, are also possible customers.[29] Although Amazon has not yet launched any satellites, they received permission from the FCC in 2020 to launch 3,236 satellites with a commercial service. The first half of the project is scheduled to launch by 2026, with the remaining part launched by 2029.[30] As their satellites are under development, the lifespan of each is still unknown.[31]

3. Rising Concerns over Cybersecurity in Outer Space

The International Organization for Standardization (ISO) defines 'cyberspace' as "a complex environment created by interacting people, software, and services on the internet via technology devices and networks connected to it, which does not exist in physical form."[32] In cyberspace, a cyberattack is an attempt to gain illegal access to a computer or computer system for the purpose of causing damage or harm.[33] Since the 1950s, outer space has been a security priority for spacefaring nations. Countries have

27 Joey Roulette, *Amazon to Launch First Two Internet Satellites in 2022*, N. Y. Times, Nov. 9, 2021, https://www.nytimes.com/2021/11/01/science/amazon-satellite-launch.html.

28 Mike Brown, Starlink Alternatives: 3 Spacex rivals you need to know, INVERSE Website (Feb. 27, 2022), https://www.inverse.com/innovation/starlink-alternatives.

29 Amazon Staff, Amazon receives FCC approval for Project Kuiper satellite constellation, amazon.com (July 31, 2020), https://www.aboutamazon.com/news/company-news/amazon-receives-fcc-approval-for-project-kuiper-satellite-constellation.

30 TECH2 New Staff, Amazon's Project Kuiper gets FCC approval: half of its 3.236 internet satellites to go up by 2026, TECH2 Website (Aug. 5, 2020), https://www.firstpost.com/tech/science/amazons-project-kuiper-gets-fcc-approval-half-of-its-3236-internet-satellites-to-go-up-by-2026-8674711.html.

31 *Supra* note 2, at 16.

32 ISO, Information Technology: Guidelines for cybersecurity, https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en *See also* Kristen E Eichensehr, *The cyber-law of nations*, 103 Geo. L. J, 325 (2014).

33 Merriam-Webster, Definition of cyberattack, Merriam-Webster Website (Mar. 2, 2022), https://www.merriam-webster.com/dictionary/cyberattack.

been competing with each other for prohibiting weapons of mass destruction in outer space and cooperating there for peaceful space uses. The more they are using outer space commericially, however, the more vulnerable cybersecurity will be in relation to global internet access from LEO for various reasons.[34] As mega-constellations employ cutting-edge technology and generate valuable data, they used to be targets of cyberattacks, which are typically directed at data or the systems such as ground stations, satellite antennae, or landlines connecting to terrestrial networks.[35]

Cyberattacks on the satellite systems can take various forms, inter alia, transmission of false data from an untrusted source, spoofing (wrong instructions to manipulate controls), jamming (degrading and disrupting connectivity by interfering with the signals for communication), and dazzling (blinding a satellite with a laser to disrupt and deny access to satellite capabilities).[36] Furthermore, malware can be used to infect ground-based systems such as satellite control centers, while hijacking operations target control systems or mission packages, perhaps taking control, shutting satellites down, or altering their orbit.[37] In addition, there is a kinetic anti-satellite (ASAT) operation, which uses lethal space weapons to enable other systems to track the target satellite. It transmits data to the interceptor spacecraft, which is then directed against the satellite. It damages or compromises the target satellite; harms the Earth's environment and various activities, depending on the data received; and creates space debris as a result of the destruction of the satellite. If the event occurs above the lower end of the LEO, it will likely generate a cloud of debris that will remain in orbit for the foreseeable future.[38]

One of the most severe potential consequences of satellite cyberattack is the loss of satellite control. There is no limit to the damage that can be inflicted if hackers gain control of satellites. An attack could cause a satellite to maneuver, decaying or lowering its orbit, causing it to re-enter the Earth's atmosphere and burn up. A sophisticated attack could also lead a satellite to collide with other satellite or space object.[39] Another scenario is that the attack could disrupt all communications and

34 David Fidler, Cybersecurity and the New Era of Space Activities, Council on Foreign Relations (Apr. 3, 2018), https://www.cfr.org/report/cybersecurity-and-new-era-space-activities.

35 *Id.*

36 The Space Domain and Allied Defence. No. 162 DSCFC 17 E rev.1 fin (2017), https://www.nato-pa.int/download-file?filename=sites/default/files/2017-11/2017%20-%20162%20DSCFC%2017%20E%20rev%201%20fin%20-%20SPACE%20-%20MOON%20REPORT.pdf.

37 Pingyue Yue et al., On the Security of LEO Satellite Communication Systems: Vulnerabilities, Countermeasures, and Future Trends, arXiv website (Jan. 9, 2022), https://arxiv.org/pdf/2201.03063.pdf.

38 Bill Boothby, *Space weapons and the law*, 93 Int'l L. Stud. 206-8 (2017).

39 David Livingstone & Patricia Lewis, Space, the Final Frontier for Cybersecurity?, Chatham House Website (Sept. 22, 2016), https://www.chathamhouse.org/2016/09/space-final-frontier-cybersecurity.

permanently damage the satellite by depleting its propellant supply or causing damage to its electronics and sensors.[40] Moreover, the data on board may be compromised or lost; more seriously, the satellite itself may be destroyed.[41] Cyber threats to space-based systems are classified into various groups. The aim of the attack could range from stealing intellectual property of another country to attempts to making financial gain by terrorist groups and individual hackers. It may either reduce national security, degrade communication, navigation, or observation satellites, or destroy an entire space vehicle. Satellite manufacturers frequently use off-the-shelf technology to reduce costs. Hackers can use some of these components to look for open-source technology and software flaws. Satellites are controlled by ground stations, which run computers with software that can be hacked. Some CubeSats could also be easily hacked using specialized ground antennae.[42]

Satellite cyberattacks have already occurred on several occasions. For instance, hackers took control of the US-German ROSAT X-Ray satellite in 1998. Having broken into computers at Maryland's Goddard Space Flight Center, the hackers instructed the satellite to point its solar panels directly at the sun.[43] In October 2014, a cyberattack on the US weather satellite system interfered with satellite feeds and several critical websites. Government officials were forced to shut down some of their services in order to stop the attackers.[44] Moreover, in May 2011, a Romanian hacker claims to have gained access to sensitive satellite data after breaching a computer server at NASA's Goddard Space Flight Center.[45] While military satellites are generally well protected,[46] commercial platforms used to be open to such attacks. With the construction and operation of small satellite constellations, the complexity and availability of satellite technology are increasing, which makes the space infrastructure even more vulnerable. If hackers gain control of these satellites, the consequences could be disastrous and jeopardize the safety of all space actors operating in LEO.

40 Luke Shadbolt, Technical Study Satellite Cyberattacks and Security, HDI Global Specialty SE Website (July 2021), https://www.hdi-specialty.com/downloads/_Global/HDIS209_Satellite_Cyberattack_whitepaper.pdf.

41 Vasudha Krishnamurthy, *Cyber-Attacks in Outer Space: A Study*, 20 Supremo Amicus 587-88 (2020).

42 Charlotte Van Camp & Walter Peeters, *A World without Satellite Data as a Result of a Global Cyber-Attack*, 59 Space Pol'y 4 (2022).

43 William Akoto, Hackers could shut down satellites – or turn them into weapons, The Conversation Website (Feb. 12, 2020), https://theconversation.com/hackers-could-shut-down-satellites-or-turn-them-into-weapons-130932.

44 Jose Pagliery, *U.S. weather system hacked, affecting satellites*, CNN, Dec. 29, 2014, https://money.cnn.com/2014/11/12/technology/security/weather-system-hacked/index.html.

45 Matt Liebowitz, NASA Computer Hacked, Satellite Data Accessed, Space.com (May 18, 2011), https://www.space.com/11700-nasa-computer-hacked-satellite-data-tinkode.html.

46 *Supra* note 40, at 4.

4. The Lack of Legal Regime related to Cybersecurity in Outer Space

In light of international space law regimes, the Outer Space Treaty (OST)[47] and the Liability Convention[48] only address the consequences of damage caused by space objects. In these treaties, however, the concept of cybersecurity in outer space remains ambiguous. Even though "space activities" had been broadly defined,[49] cyberactivities were not considered during the treaty negotiations in the 1960s. Moreover, unanticipated commercial space activities, including the operation of small satellite constellations, emerged recently and cyberattacks affecting thoroughly segregated computer space systems were unknown at that time.[50] As cyber borders are not the same as physical borders, assigning territorial sovereignty to cyberspace is time-consuming. Cyberspace does not allow for the demarcation of territorial sovereignty because it is not based on physical location.[51]

According to Article VI of the OST, States Parties shall bear international responsibility for national activities in outer space, whether performed by governmental or non-governmental entities. They have to take primary responsibility for authorizing and continuously supervising such activities. Article VI of the OST is elaborated by Article II of the Liability Convention, which holds launching States absolutely liable to pay compensation for damage caused by their space object on the Earth's surface or to aircraft in flight, and prescribes fault liability for damage caused in outer space. In terms of the damage caused by cyberattacks, Article VI of the OST lays down that the launching State exercises flight control over its space objects or oversees a space activity of its non-governmental entities. However, unauthorized intervention by a third party or State has been excluded from this idea thus far.[52]

Unauthorized cyberoperations can directly or indirectly interfere with a space object's flight control via the terrestrial section or peripheral systems. Let us suppose

47 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (Outer Space Treaty): adopted by the UN General Assembly in its resolution 2222 (XXI), (opened for signature on 27 January 1967, entered into force on October 10, 1967).

48 Convention on International Liability for Damage Caused by Space Objects (Liability Convention): adopted by the UN General Assembly in its resolution 2777 (XXVI), opened for signature on 29 March 1972, entered into force on September 1, 1972)

49 Stephan Hobe, et al., Cologne Commentary on Space Law: Outer Space Treaty 34 § 1 (2017).

50 Stefan Kaiser & Martha Mejia-Kaiser, *Cyber Security in Air and Space Law*, 64 ZLW 406 (2015).

51 *Supra* note 36, at 588.

52 *Supra* note 50, at 406-7.

that malicious cyberactivity interferes with the flight control of a space object and results in catastrophic damage to the launching State or another State on the Earth's surface. In that case, the launching State of this space object is deemed responsible under Article VI of the OST and liable for damages under Article II of the Liability Convention. The existing space legal regimes impose a disproportionate burden on the launching State, which becomes liable for cyberattacks it did not permit, loses its space object, and is responsible for third-party damage.[53]

5. The Current Motions regarding Cybersecurity Standards

Multi-stakeholder groups have spearheaded several informal initiatives outside the UN's auspices since 2018.[54] States and corporations have attempted to propose cybersecurity standards and advance international norms on cyberspace security. None is yet legally binding, however.

A. Paris Call for Trust and Security in Cyberspace

The Paris Call for Trust and Security in Cyberspace (hereinafter Paris Call) is a nonbinding declaration that encourages States, the private sector, and civil society organizations to collaborate in order to promote cybersecurity, combat disinformation, and address new threats endangering citizens and infrastructure.[55] French President Emmanuel Macron launched the Paris Call during the Internet Governance Forum and the Paris Peace Forum in November 2018. Approximately, 81 states, 36 public authorities and local governments, over 706 businesses, and 390 civil society organizations now support the Paris Call, totaling over 1200 supporters (as of March 2022). This motion is the largest group ever assembled to support a cybersecurity-focused agreement, a genuinely unprecedented action in international online security and stability.[56] It is based on the following nine fundamental principles for securing

53 *Id.*

54 Kaja Ciglic & John Hering, *A multi-stakeholder foundation for peace in cyberspace*, 6 J. Cyber Pol'y 1 (2021).

55 Democratic Institutions, Frequently asked questions-Paris Call: Trust and Security in Cyberspace, Government of Canada Website (May 5, 2020), https://www.canada.ca/en/democratic-institutions/news/2020/05/frequently-asked-questions---paris-call-trust-and-security-in-cyberspace.html.

56 Paris Call, Paris Call For trust and security in cyberspace (May 5, 2020), https://pariscall.international/en/.

cyberspace:[57] (1) Protect individuals and infrastructure;[58] (2) Protect the internet;[59] (3) Defend electoral processes;[60] (4) Defend intellectual property;[61] (5) Non-proliferation;[62] (6) Lifecycle security and supply chain security;[63] (7) Cyber hygiene;[64] (8) No private hack back;[65] and (9) International norms.[66]

B. Digital Geneva Convention

On February 14, 2017, Microsoft President Brad Smith delivered a passionate speech to the Rivest, Shamir, and Adleman (RSA) Conference attendees in San Francisco in which he urged all members of the private sector to join forces to establish a "Digital Geneva Convention" (DGC). Smith claims that "the world of potential war has migrated from land to sea, to air, and now to cyberspace."[67] The DGC's objective is to commit nations to defend people in times of peace from nation-state aggression. Furthermore, as Article 10 of the Fourth Geneva Convention 1949 recognizes that protecting civilians necessitates the active participation of the Red Cross, defense against nation-state cyberattacks necessitates the active participation of technology businesses. Given that the technology sector is uniquely playing the role of the internet's first responders, collaborative action should be committed to make the Internet a safer place, asserting their role as a neutral Digital Switzerland which supports customers worldwide and maintains the world's trust. The six principles of DGC that Microsoft proposed are:[68] (1) No targeting of tech companies, private sector, or critical infrastructure;[69] (2) Assist private sector efforts to detect, contain, respond to, and recover from events;[70] (3) Report vulnerabilities to vendors rather than

57 Paris Call, The 9 Principles (May 5, 2020), https://pariscall.international/en/principles.

58 *Id*. princ. 1.

59 *Id*. princ. 2.

60 *Id*. princ. 3.

61 *Id*. princ. 4.

62 *Id.* princ. 5.

63 *Id*. princ. 6.

64 *Id*. princ. 7.

65 *Id*. princ. 8.

66 *Id*. princ. 9.

67 Valentin Jeutner, *The Digital Geneva Convention: A Critical Appraisal of Microsoft's Proposal*, 10 J. Int'l Humanitarian Legal Stud. 159 (2019).

68 Brad Smith, The need for a Digital Geneva Convention, Microsoft Website (Feb. 14, 2017), https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention.

69 *Supra* note 57, princ. 1.

70 *Id*. princ. 2.

stockpile, sell, or exploit them;[71] (4) Exercise restraint in developing cyberweapons and ensure that any developed are limited, precise, and not reusable;[72] (5) Commit to nonproliferation activities in regard to cyberweapons;[73] and (6) Limit offensive operations to avoid a mass event.[74]

C. Cybersecurity Tech Accord

The Cybersecurity Tech Accord (hereinafter Accord), launched in April 2018, was signed by 34 multinational technology and security companies, including Microsoft and Facebook, a diverse group of international telecommunications and hardware manufacturers, open-source software providers, and cybersecurity threat intelligence firms. The Accord established an agreement and public commitment to protect and enhance trust and security in cyberspace[75] and offers a platform for debate, discovery, and decisive action on cybersecurity concerns by pooling the resources and skills of the global technology industry. This motion has developed dramatically over the last three years, with 150 signatories from five continents (as of April 2022) unified in the campaign against cybercrime.[76] It aims to make the Internet safer by fostering collaboration among global technology businesses committed to adopting important principles to secure their customers and users and assist them in defending themselves against dangerous threats.[77] The following summarizes the Accord's primary principles as follows:[78] (1) Protect the safety of all users and customers everywhere;[79] (2) Oppose cyberattacks on innocent citizens and enterprises from anywhere;[80] (3) Empower users, customers, and developers to strengthen cybersecurity protection;[81] and (4) Partner with each other and with likeminded groups to enhance cybersecurity.[82]

71 *Id*. princ. 3.

72 *Id*. princ. 4.

73 *Id*. princ. 5.

74 *Id*. princ. 6.

75 Robert Gorwa & Anton Peez, *Big Tech Hits the Diplomatic Circuit: Norm Entrepreneurship, Policy Advocacy, and Microsoft's Cybersecurity Tech Accord*, *in* Governing Cyberspace: Behavior, Power, and Diplomacy 265 (D. Broeders & B. van den Berg eds., 2018).

76 Joe Clay, *Celebrating 3 years of the Cybersecurity Tech Accord*, Trend Micro Website (Apr. 14, 2021), https://www.trendmicro.com/en_us/research/21/d/celebrating-3-years-of-the-cybersecurity-tech-accord.html.

77 Cyber Tech Accord, 2018 In Review Cyber Tech Accord, Cyber Tech Accord Website (Mar. 4, 2022), https://cybertechaccord.org/uploads/prod/2019/03/2018report.pdf.

78 Cyber Tech Accord (Mar. 4, 2022), https://cybertechaccord.org/accord.

79 *Id*. princ. 1.

80 *Id*. princ. 2.

81 *Id*. princ. 3.

82 *Id*. princ. 4.

D. Charter of Trust for Secure Digital World

The Charter of Trust for a Secure Digital World (CoT) was initiated by Siemens and eight industry partners at the Munich Security Conference in 2018.[83] Originating from a desire to protect digital technologies, CoT's founding members signed it to demonstrate their commitment to working together to achieve the organization's purpose of fostering trust in the digitally connected world. Since its beginnings, the CoT has grown from nine to 17 members (as of March 2022).[84] This movement demands binding regulations and standards to foster and enhance cybersecurity in digitalization.[85] The CoT's key objectives are to protect individual and business data; prevent damage to individuals, businesses and infrastructures; and establish a trustworthy foundation upon which confidence in a networked, digital world can take root and grow.[86] The ten principles for ensuring digital security adoption are central to the CoT. The following principles revolve around protecting data, people, and organizations, enabling the partners to collaborate effectively, while creating a secure digital world:[87] (1) Ownership of cyber- and IT security;[88] (2) Responsibility throughout the digital supply chain;[89] (3) Security by default;[90] (4) User-centricity;[91] (5) Innovation and co-creation;[92] (6) Education;[93] (7) Certification for critical infrastructures and solutions;[94] (8) Transparency and response;[95] (9) Regulatory framework;[96] and (10) Joint initiatives[97]

83 Florian Martini, The Charter of Trust takes a major step forward to advance cybersecurity, Siemens Website (Mar. 4, 2022), https://press.siemens.com/global/en/feature/charter-trust-takes-major-step-forward-advance-cybersecurity#:~:text=on%20Cyber%20Security.-,Initiated%20by%20Siemens%2C%20the%20Charter%20of%20Trust%20calls%20for%20binding,data%20of%20individuals%20and%20businesses.

84 Axel Stepken, Charter of Trust: Making the Digital World Safer, TÜV SÜD Website (Mar. 4, 2022), https://www.tuvsud.com/en/themes/charter-of-trust.

85 *Supra* note 83.

86 Charter of Trust, About, Charter of Trust Website (Mar. 4, 2022), https://www.charteroftrust.com/about.

87 Principles and Benefits of the Charter of Trust, TÜV SÜD Website (Mar. 4, 2022), https://www.tuvsud.com/en/themes/charter-of-trust/principles-and-benefits.

88 *Id*. princ. 1.

89 *Id*. princ. 2.

90 *Id*. princ. 3.

91 *Id*. princ. 4.

92 *Id*. princ. 5.

93 *Id*. princ. 6.

94 *Id*. princ. 7.

95 *Id*. princ. 8.

96 *Id*. princ. 9.

97 *Id*. princ. 10.

6. The Need for Multistakeholder International Legal Regime for Space Cybersecurity

While outer space has been used and explored by humans for more than 60 years, it is only recent that the vulnerability of cybersecurity has become of practical importance, not least due to the critical importance of space systems and space applications in almost all spheres of modern life and critical infrastructure.[98] The complexity of all issues has sparked concerns about the capabilities and tools required to prevent cyberattacks in satellite constellations. Cybersecurity competencies for satellites are advancing, but currently incur significant installation costs. Nonetheless, the competitive character of the private sector and financial incentives to maximize profits are leading businesses to construct and deploy thousands of satellites that are inherently vulnerable to cyberthreats, whether they are doing so voluntarily or not. Consequently, it is only a matter of time before a catastrophic calamity occurs.[99]

Cybersecurity in outer space has the potential to affect both global economy and national sovereignty.[100] Therefore, to deal with this issue, a cyber regime on outer space is needed.[101] The ideal cybersecurity regime would encompass all the respective interests of the various stakeholders, including corporate and military actors as well as scientists and end-users. It would address the myriad technical, economic, social, and political interests through a pragmatic combination of bottom-up and top-down approaches. It is critical to identify the most important aspect to protect, whether it be broadband access or something else, and shape related policy interventions. More importantly, the approach should be non-hierarchical, addressing the concerns of all stakeholders equitably. It also ensures that each participant is individually knowledgeable and empowered as a valued contributor within the sector.[102] Like any other aspect of space law and policy, in outer space governance, the following three

98 Federico Bergamasco, et al., Cybersecurity: Key Legal Considerations for the Aviation and Space Sectors 1193 (2020).

99 Edward Verco, *Satellites are Cyber Insecure: We Need Regulation to Avoid a Disaster*, 2 ANU J. L. & Tech. 58 (2021).

100 Pavan Duggal, Cybersecurity law, its regulation and relevance for outer space, United Nations Office for Outer Space Affairs Website (Mar. 7, 2022), https://www.unoosa.org/documents/pdf/hlf/HLF2017/presentations/Day2/Session_7b/Presentation5.pdf.

101 Patricia Lewis & David Livingstone, The cyber threat in outer space, Bull. the Atomic Scientists (Nov. 21, 2016), https://thebulletin.org/2016/11/the-cyber-threat-in-outer-space.

102 Ruvimbo Samanga, *Policy Solutions for Cybersecurity in Space*, Space Legal Issues (Dec. 7, 2020), https://www.spacelegalissues.com/policy-solutions-for-cybersecurity-in-space.

points can be considered:[103] (1) A cybersecurity regime necessitates implementing a system backed by a policy that allows legitimate users while increasing the costs for illegitimate ones; (2) Governing cyberspace is a collaborative effort that should involve multiple stakeholders; and (3) To be sustainable as a regulatory regime, it should include a self-governing body and a lightly regulated effort from all stakeholders.

There are currently no specific international legal regimes governing cybersecurity.[104] In addition, the term "cybersecurity" does not appear in any international treaties that govern outer space activities.[105] Absent the clear definition in the existing legal regime, States are increasingly relying on their domestic legislation to address cybersecurity breaches.[106] Nevertheless, municipal law is incapable of dealing with the international characteristics of cyberspace. Considering that data transfer around the world processes and stores information in networks globally, national law's territorial scope is too narrow and it can only have legal effect in those parts of the cyberinfrastructure located within the given State.[107]

Establishing cybersecurity standards and risk management mechanisms necessitates technical measures and a regulatory framework. International cooperation is the only way to provide a fully coordinated approach to cyberspace protection which is consistent with the fundamental premise of international space law. Rather than amending existing legal regimes, the concept of a multistakeholder may be applied to international legal regime for space cybersecurity. Negotiating acceptable regulatory rules between nations on an international level will be difficult when most actors are private enterprises. As a result, all stakeholders must collaborate to build a successful system.[108] In terms of technical measures, the new legal regime should employ existing non-legally binding security standards proposed by States and corporate sectors, as discussed in the previous chapter, for consideration, such as the Paris Call, DGA, Accord, and CoT, as well as develop new standards for space systems where needed.[109]

103 *Id*.

104 *Supra* note 34.

105 *Supra* note 98, at 1195.

106 *Supra* note 100.

107 *Supra* note 50, at 397.

108 *Supra* note 99, at 86.

109 Gregory Falco, *Cybersecurity principles for space systems*, 16 J. Aerospace Info. Systems 6 (2019).

Received: February 15, 2022
Modified: April 1, 2022
Accepted: May 1, 2022