JOURNAL OF LAW, TECHNOLOGY & THE INTERNET • VOL. 13 • NO. 1 • 2021 – 2022

THE LAW OF SPACE CYBER OPERATIONS: GRIPPING MYSTERIES, ENTANGLED FRONTIERS, AND SECURITY CHALLENGES

Roy Balleste[*]

The developments of technologies applicable to cyberspace and outer space offer new opportunities. Each nation, institution, and individual must be involved in the security of cyberspace in order to secure outer space activities, while reinforcing the legitimacy of that commercial process. The stories that follow consider the intersection of outer space law and cybersecurity, describing vulnerabilities and the limitations of implementing international norms. The article assesses the cyberthreat landscape while offering recommendations. The article's subsequent sections are organized as follows: Part II, The Cruel Sky, considers a historical mystery to better understand the contradictory world of cyber operations. Along the way in looks at humanity and its role to play. Part III, the Human Condition, takes a closer look at activities on and near Earth. In particular, it assesses a potential computer fraud originating from outer space. Part IV, Reach for the Stars, treks in search of recommendations for the safety and future of space exploration.

[*] Dr. Roy Balleste is Assistant Professor of Law and Law Library Director at Stetson University. Professor Balleste has focused his scholarship on the evolving regulatory challenges of internet governance, cybersecurity law and policy, cybersecurity in outer space, cyber operations, and cyber conflict. Balleste is currently a core expert and member of the editorial board of the Manual on International Law Applicable to Military Uses of Outer Space (MILAMOS). Balleste holds a J.S.D. in Intercultural Human Rights (analyzing internet governance, St. Thomas University); LL.M. in Air and Space Law (McGill University); LL.M. in Intercultural Human Rights (St. Thomas University); M.S. in Cybersecurity (Norwich University); and a J.D. (St. Thomas University). Professor Balleste is a member of the Space Force Association and a member of the International Institute of Space Law (IISL). He is Director of Information Security for ABH Aerospace. This article is dedicated to his daughter Arya and her curiosity for the stars. Professor Balleste offers his deepest and most sincere gratitude to Dean Michèlle Alexandre and the administration of the College of Law, for the support during the drafting of this article. He offers his appreciation to Lauren Fleming, his research assistant.

Contents

"Something roars not twenty feet from him.
It could be the wind finding a new route through or around an icy serac or pinnacle, but Crozier knowns that it isn't." — Dan Simmons[1]

I. Northwest Passage

It was the first age of exploration. The tall ships circumnavigating the globe mastered the oceans, and its sailors were in search of dreams. The story of the Northwest Passage belongs in the annals of history as one of the most famous. While the Spanish conquistadors were risking all, including their lives, to find El Dorado,[2] four hundred years later, the Royal Navy and its brave men traversed the oceans searching for a new, valuable, and enigmatic place. Now that the Napoleonic Wars were over, the Admiralty had a new mission for a group of experienced mariners: to find the Northwest Passage.[3] This article is a journey that addresses that mission. This article is a story within stories designed to help the reader understand the complexities of the present cyber landscape as the world enters the second space age. The universes of human knowledge, thought, and creativity may lead to prosperity or disaster. The Internet has evolved dramatically in the last twenty-five years. In that time, humanity has benefitted from the enhancement of commerce, education, and social interactions. As if skillfully planned, criminal activities followed the commercialization of the Internet that now, in turn, threaten the present legal order of outer space.[4] The impending frontiers of human exploration will not be easily accessible. With this in mind, as technological advancements continue to grow and prosper, cyberthreats are becoming more prominent.[5] More specifically, these threats loom over the technological innovation and security in outer space.[6] The present state of affairs in the world is perilous. For example, the United States, in general, is a

---

[1] DAN SIMMONS, THE TERROR 7 (2007).
[2] *See, e.g.*, JOHN HEMMING, THE SEARCH FOR EL DORADO (2001).
[3] PIERRE BERTON, THE ARTIC GRAIL: THE QUEST FOR THE NORTH WEST PASSAGE AND THE NORTH POLE 1818–1909 16 (1988).
[4] Sean B. Hoar, *Trends in Cybercrime: The Dark Side of the Internet*, 20 CRIM. JUST. 4 (2005). *See also* Andre Kwok, *The growing threat of cybercrime in the space domain*, E. ASIA F. (Sept. 9, 2021), https://www.eastasiaforum.org/2021/09/09/the-growing-threat-of-cybercrime-in-the-space-domain/.
[5] John Shin, *Why Space is the Next Frontier for Cybersecurity*, FORBES (Aug. 20, 2021, 07:45am EDT), https://www.forbes.com/sites/forbestechcouncil/2021/08/20/why-space-is-the-next-frontier-for-cybersecurity/?sh=527a172a41b1.
[6] *Id*.

daily target of cyberattacks.[7] Within a twelve-month period during 2020–2021, the U.S. has been the target of seven major cyberattacks.[8]

Although, improbable that there have been many more, these seven attacks have been attributed to Russia in one form or another.[9] For example, the meat processing company, JBS, was hacked via a ransomware attack.[10] The hackers attempted to use the U.S. Agency for International Development's (USAID) email system to send phishing emails.[11] Colonial Pipeline shut down due to a ramson attack, and hackers breached several U.S. government agencies and companies "exploiting software made by SolarWinds."[12] The typical user of the Internet would expect that cyber operations are being governed by international law standards, in addition to national laws. However, in most cases, the interference of foreign powers has a more significant influence in policing cyberspace. The challenge that follows is one of accountability.

The idea of colonizing distant places of our solar system and beyond offers some tantalizing possibilities. This idea, in many ways, seems to border the imaginary. The beginning of space technologies originated with nations and has evolved into the realm of commercial partnerships over time.[13] The first age of exploration began at the start of 1957 when the Soviet Union's launched the first artificial satellite, Sputnik I, into space, and in that manner propelled the United States into a new frontier of space exploration.[14] Shortly after that, the first American satellite was launched into the void, designated as Explorer I.[15] On July

---

[7] *See generally 2021 Cyber Security Statistics the Ultimate List of Stats, Data & Trends,* PURPLESEC, https://purplesec.us/resources/cyber-security-statistics/ (last visited Mar. 2, 2022).
[8] *The 10 Biggest Ransomware Attacks of 2021*, TOURO COLL. ILL. (Nov. 12, 2021), https://illinois.touro.edu/news/the-10-biggest-ransomware-attacks-of-2021.php.
[9] BERTON, *supra* note 3, at 16.
[10] *JBS: FBI says Russia-linked group hacked meat supplier,* BBC NEWS (June 3, 2021), https://www.bbc.com/news/world-us-canada-57338896#:~:text=A%20Russian%20cyber%2Dcriminal%20group,the%20US%2C%20Canada%20and%20Australia.
[11] Joe Walsh, *Here Are Some Of The Major Hacks The U.S. Blamed On Russia In The Last Year*, FORBES (June 1, 2021), https://www.forbes.com/sites/joewalsh/2021/06/01/here-are-some-of-the-major-hacks-the-us-blamed-on-russia-in-the-last-year/?sh=3beb23e95b9e
[12] *Id*.
[13] Simonetta Di Pippo, *Space Technology and the Implementation of the 2030 Agenda*, UN CHRONICLE, https://www.un.org/en/chronicle/article/space-technology-and-implementation-2030-agenda (last visited Apr. 21, 2022).
[14] Vaibhav Gupta, *World's 1st Satellite was the Size of a Beach Ball,* INSHORTS (Oct. 4, 2016), https://inshorts.com/en/news/worlds-1st-satellite-was-the-size-of-a-beach-ball-1475582799404?utm_source=news_share&forward_to_store=true.
[15] Sarah Loff, *Explorer 1 Overview,* NASA (Aug. 3, 2017), https://www.nasa.gov/mission_pages/explorer/explorer-overview.html.

29, 1958, President Eisenhower ushered in the beginning of the National Aeronautics and Space Act, signing the nation's space agency into law.[16] Since those days, space exploration has remained a fascination to many in the US and worldwide, while seeking to understand the unknown and what lies beyond our solar system.

Since the launch of Sputnik I, the law has been that outer space is free for exploration and use by all States.[17] Article II of the Outer Space Treaty (OTS), specifically notes that: "[o]uter space, including the Moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means."[18] The first age of space exploration during the 1960s and 70s was dominated by two nations and guided by the wisdom of the Outer Space Treaty.[19] The age of the Apollo missions was one of high expectations, and it opened the door for the years of the space shuttle program.

At present, we are entering the second space age, colloquially known as '*NewSpace*.'[20] The concept of *NewSpace* involves technological, legal, commercial, and social innovations.[21] The result is a "decrease in the expenses related to the provision of new space products and services, and this, in turn, has served to widen the market."[22] The widening of the market is reflected in the emerging sectors of space mining, space tourism, on-orbit servicing, mega-constellations, and spaceflight.[23] This new space age is promising yet vulnerable to the same flaws of the human condition. OTS Article III delineates space activities within the context of international law, which includes the Charter of the United Nations.[24] And most relevant, Article VI states in part the following:

---

[16] Steven J. Dick, *The Birth of NASA,* NASA (Mar. 23, 2008), https://www.nasa.gov/exploration/whyweexplore/WhyWe29.html.
[17] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies art. I, Oct. 10, 1967, 610 U.N.T.S. 205 [hereinafter Outer Space Treaty].
[18] *Id*. at art. II.
[19] *See generally id*.
[20] *See* Ruvimbo Samanga, *NewSpace*, IISL SPACE LAW KNOWLEDGE CONSTELLATION (July 2021), https://constellation.iislweb.space/ruvimbo-samanga-newspace/.
[21] *Id*.
[22] *Id*.
[23] *Id*.
[24] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 272 (Michael N. Schmitt ed., 2017) [hereinafter TALLINN MANUAL 2.0].

> "States Parties to the Treaty shall bear international responsibility for national activities in outer space, including the moon and other celestial bodies, whether such activities are carried on by governmental agencies or by non-governmental entities, and for assuring that national activities are carried out in conformity with the provisions set forth in the present Treaty. The activities of non-governmental entities in outer space, including the moon and other celestial bodies, shall require authorization and continuing supervision by the appropriate State Party to the Treaty."[25]

The emerging privatization of outer space activities has brought commerce into a new age of successful space companies that significantly benefit from governments' consistent cooperation and support.[26] The age of *NewSpace* promises historical heights. Carl Sagan once noted that "[t]here is much that science doesn't understand, many mysteries still to be resolved. In a Universe of tens of billions of light-years across and some ten or fifteen billion years old, this may be the case forever. We are constantly stumbling on new surprises."[27] The NewSpace stakeholders move forward into a new contested frontier, while the global community watches with hopes for a better future.

How a nation is held accountable for its space activities is as significant as its achievements in space exploration. Reaching Mars and beyond is as notable as when it does not tolerate the use of its territory as a base of operations for illegal cyber activities. Given the connection between cyberspace and outer space, Article III of the Outer Space Treaty delineates space cyber operations within the context of international law.[28] In other words, governance of space activities, including those that utilize cyber means, extend to outer space uses and exploration.[29] These principles help to visualize norms applicable to cyber operations in support of space activities.

The years since the first moon landing have passed into memory. NASA's Apollo program landed twelve American men on the Moon and returned them safely to Earth in the short span of only five years.[30] No other nation has matched

---

[25] Outer Space Treaty, *supra* note 17, at art. VI.
[26] Omkar Nikam, *Opportunities Emerging from "New Space"*, SATELLITE MKT. & RSCH., http://satellitemarkets.com/news-analysis/opportunities-emerging-new-space (last visited Apr. 21, 2022).
[27] CARL SAGAN, THE DEMON-HAUNTED WORLD: SCIENCE AS A CANDLE IN THE DARK 29 (1997).
[28] TALLINN MANUAL 2.0, *supra* note 24, at 272.
[29] *Id*.
[30] DANIEL MORGAN, CONGR. RSCH. SERV., ARTEMIS: NASA'S PROGRAM TO RETURN HUMANS TO THE MOON (2021).

this extraordinary feat of innovation and ingenuity. The US government has committed to returning by 2024.[31] The story continues with "Artemis: NASA's Program to Return Humans to the Moon."[32] Indeed, NASA has expanded its mission to include taking not just men but also the first woman and first astronaut of color.[33] It is exciting to imagine the possibilities of the three planned Artemis missions, although only Artemis III will arrange for a crew that will travel around the Moon.[34] Other expeditions will follow.

However, despite calls for peaceful uses, humanity's access to outer space will carry the conflicts of the human condition into the heavens. These conflicts require additional preparation and planning for the industry's lawyers and chief information officers (CISOs). Hopefully, twenty years from now, NASA will celebrate establishing an outpost in the Moon as a tribute to those great souls of the Apollo missions and those that will follow. But stakeholders must also make plans that factor into the calculations the threats associated with space systems. The *NewSpace* age may be challenged by the simple failings of humanity. The idea of cybercrime in outer space may be unimaginable but not inconceivable. Yet, under those conditions, a CISO may discover a threat with significant consequences for the organization.

The stories that follow consider the intersection of outer space law and cybersecurity, describing the limitations of implementing international standards. This article assesses the cyberthreat landscape while offering recommendations. Part II, The Cruel Sky, considers a historical mystery to better understand the contradictory world of cyber operations. Along the way it looks at humanity and its role to play. Part III, *New Frontiers in the Expanse*, takes a closer look at the activities on and near Earth. In particular, it assesses the Computer Fraud and Abuse Act (CFAA). Part IV, *Reach for the Stars*, treks in search of a recommendation for the safety and future of space exploration.

II. The Cruel Sky

A new age of space activities promises historical heights. While new stakeholders move forward into a new contested frontier, the global community continues to watch with hopes for a better future. Nevertheless, there are political considerations that need to be considered based on the realities of outer space.

---

[31] *Id*.
[32] *What is Artemis?*, NASA (Feb. 28, 2021), https://www.nasa.gov/what-is-artemis.
[33] *Id*.
[34] *Id*.

Indeed, the race to Mars will face cyberattacks and the risks attached to them.[35] Additionally, the ethical ramifications of regulating private space activities are a new challenge and a new opportunity.[36] These activities are supposed to protect the enjoyment and use of outer space. The future will be ripe with opportunities to further evolve the dimensions of outer space commerce. Still, it will be successful only if stakeholders work together to redefine the security landscape of space objects. If humanity eventually manages to survive from its challenging present and evolves toward a brighter future, it will be because it has achieved an interstellar status.

In this second space age, governments are no longer at the center of space activities.[37] The industry has opened up to multiple market participants, including dozens of startups.[38] The race to Mars, Titan, and beyond is no longer an unexpected future event, but is an act of humanity's future that began a long time ago and continues to race in full force. In recent years, three missions were completed traveling 250 million miles toward Mars.[39] The United Arab Emirates arrived in early February 2021, and China shall arrive shortly after to place probes in orbit around the planet and a rover.[40] NASA also landed a new rover called Perseverance, the first of its kind to carry a helicopter-type drone.[41] It is safe to say that cyberspace is now tied to the activities in outer space or "space-enabled communication and information services," which in turn rely on the operation of satellites.[42]

---

[35] Emma Ashford, *Can the World Avoid War in Cyberspace–and in Space?*, FOREIGN POL'Y (July 23, 2021), https://foreignpolicy.com/2021/07/23/war-cyberspace-space-nso-pegasus-bezos-rocket/.
[36] *See generally* Brandon Dillon, *Profitable Risk: The Dangers of Consumer Spaceflight and Space Tourism*, VITERBI CONVERSATIONS ETHICS (Dec. 12, 2020), https://vce.usc.edu/volume-4-issue-2/profitable-risk-the-dangers-of-consumer-spaceflight-and-space-tourism/.
[37] *See* Matt Weinzierl & Mehak Sarang, *The Commercial Space Age Is Here*, HARV. BUS. REV. (Feb. 12, 2021), https://hbr.org/2021/02/the-commercial-space-age-is-here.
[38] *Id*.
[39] Erin Woo, *Startups Aim Beyond Earth,* N.Y. TIMES (July 7, 2021), https://www.nytimes.com/2021/07/07/technology/space-start-ups.html.
[40] Morgan McFall-Johnsen, *3 spacecraft are set to reach Mars this month, from NASA, China, and the UAE. Here's what they aim to learn*, BUS. INSIDER (Feb. 4, 2021), https://www.businessinsider.com/three-mars-missions-arrive-february-from-nasa-china-uae-2021-1.
[41] *Id*.
[42] David P. Fidler, *Cyber Crime in Outer Space: Houston, Do We Have a Problem?,* COUNCIL ON FOREIGN RELATIONS (Aug. 29, 2019), https://www.cfr.org/blog/cyber-crime-outer-space-houston-do-we-have-problem.

This commercialization of space highlights potential cybersecurity concerns, including rapid innovations in software and hardware lifecycles.[43] These activities intersect space transportation, tourism, mining, the Moon, and Mars.[44] While Article I of OTS recognizes "the exploration and use of outer space, including the moon and other celestial bodies . . . carried out for the benefit and in the interests of all countries . . . " stakeholders should be prepared to adopt cybersecurity best practices and collaborate on improving the implementation of security strategies.[45] The proliferation of cyber operations as an element that endures during peacetime forces the space industry CISO to consider questions about what would constitute the most egregious form of a cyberattack. "As of yet, there is no global consensus about what an act of war carried out by cyber means would look like, versus acts that would fall below the level of an act of war, and although still unlawful, would call for different responses under the law."[46]

A larger political problem involves the opposite view: States develop engagement protocols for cyber operations against other governments. "Dominant actors like the United States and Russia have reopened the possibility of pursuing weaponization of space to defend their interests and assert dominance."[47] This is that hazy ambiguity that afflicts the efforts to develop new norms for cyberspace in a peaceful outer space. If cyberspace is going to be considered a necessary part of the arsenal of a State much like international waters, then all of humanity shares a challenge and duty as a sentient species to at least mitigate the damage that may be caused to human life.

The sea is one of those domains that spur imagination. It invites any individual to journey into a new world of discovery. A voyage into that great maritime expanse is one of those enduring adventures with no beginning or end. One of those voyages began with one intrepid idea. It was in the Canadian Arctic Archipelago, one of the most desolate places on Earth, where the story begins.[48] Here, in 1845, two powerful British ships were dispatched to investigate the route

---

[43] *See generally* David P. Fidler, *The White House Adopts Cybersecurity Policy for Activities in Outer Space*, COUNCIL FOREIGN REL. (Sept. 23, 2020), https://www.cfr.org/blog/white-house-adopts-cybersecurity-policy-activities-outer-space.
[44] Fidler, *supra* note 42.
[45] Outer Space Treaty, *supra* note 17 at art. I.
[46] Catherine Lotrionte, *Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law*, 3 CYBER DEF. REV. 73, 73 (2018).
[47] P. J. Blount, *Peaceful Purposes for the Benefit of All Mankind: The Ethical Foundations of Space Security*, in WAR AND PEACE IN OUTER SPACE: LAW, POLICY AND ETHICS 119, 120 (Cassandra Steer & Matthew Hersch eds., 2021).
[48] OWEN BEATTIE & JOHN GEIGER, FROZEN IN TIME: THE FATE OF THE FRANKLIN EXPEDITION 11 (2017).

known as the Northwest Passage.[49] This sailing route promised its explorers a gateway between the Atlantic and the Pacific Oceans across the top of North America.[50] Sir John Franklin and his 129 men aboard the *HMS Erebus* and *HMS Terror* began the audacious journey and vanished without a trace.[51] The resolution of this mystery forced mariners and relevant stakeholders alike to wrestle with the true nature of technology and its limits.

It is true that these ships were built to be tough and the experienced crews "had shown that they were exceptionally resilient."[52] While these ships were powerful, they were made stronger by the retrofits to handle polar expeditions.[53] However, tougher defenses were not a guarantee of invulnerability. In contrast with present challenges, the technical nature of the Internet makes it nearly impossible to secure and control. Even with innovative technologies, legal questions arise with the evolution of cyberspace demonstrating a leap in human ingenuity along with juridical ambiguity. But these factors also represent unforeseen dangers. While in outer space borders are imperceptible, closer to the ground, legal challenges stress the threats to well-established legal notions that raise doubts for those securing satellite communications. This is simply the case because technology is constantly evolving. Hence, the nature of cyber operations arise with unresolved technological issues, security needs, and the related activities at the national and international levels. "An accurate description and assessment of any social process requires that initial attention be given to individuals and group participants."[54] In this case, it is helpful to begin by considering the challenges of North America through the lenses of the US and Canada.

The cyberthreat landscape does not afford any special privileges to the stakeholder of space exploration, which might expect that malicious cyber operations are being governed safely or that these will remain isolated in the land domain. This assumption of safety or invulnerability would be the beginning of failure. For the British Admiralty, the extraordinary men selected to lead their new expedition were the best. Sir John Franklin led the expedition and Francis

---

[49] Niraj Chokshi, *The HMS. Terror Sank in the 1840s. See What It Looks Like Now*, N.Y. TIMES (Aug. 30, 2019), https://www.nytimes.com/2019/08/30/science/hms-terror-wreck-franklin-expedition.html?searchResultPosition=1.
[50] GILLIAN HUTCHINSON, SIR JOHN FRANKLIN'S EREBUS AND TERROR EXPEDITION: LOST AND FOUND 41 (2017).
[51] Chokshi, *supra* note 49.
[52] HUTCHINSON, *supra* note 50.
[53] *Id*. at 42.
[54] Myres S. McDougal et al., *The World Community: A Planetary Social Process*, 21 U.C. DAVIS L. REV. 807, 811 (1988).

Crozier was appointed second in command and captain of the *HMS Terror*.[55] James Fitzjames was third in command and senior officer of the *HMS Erebus*.[56] The image of well-prepared sailors navigating difficult waters may be reassuring for those relying on the outcome of the mission. In the same manner, IT professionals must know that cyberattacks will happen because that is the new nature of cyberspace. Yet, it seems that any network system could potentially be hacked and for that reason, nothing matches preparation. It is fascinating and worrisome to see hackers easily defeat the security of a top tech giants.

The future space traveler will face threats indigenous to the cyber realm, in part, because the present state of affairs in the world is perilous. The United States is now under daily cyberattacks.[57] For the US, being the target of seven major cyberattacks during 2021 is worrisome.[58] Yet, the U.S. has likely faced many more attacks.[59] The Russian government and lone criminals based in Russia have been blamed for the seven major attacks on the US during 2021.[60] For example, the meat processor JBS was hacked via a ransomware attack, and hackers tried to use the U.S. Agency for International Development's (USAID) email system to send phishing emails.[61] The Colonial Pipeline attack was particularly malicious, with a shut down due to a ramson attack.[62] Another attack involved hackers breaching several U.S. government agencies and companies by exploiting software made by SolarWinds, and have included other targets such as state and local governments, hospitals, and COVID-19 vaccine researchers.[63] These examples demonstrate that dangerous cyber operations often involve foreign governments.[64] The mystery that arises is the added enigma associated with nations that knowingly tolerate the use of their territory as bases of illegal cyber operations to strike other governments and their businesses.[65]

---

[55] *Wrecks of HMS Erebus and HMS Terror National Historic Site*, PARKS CAN. (May 27, 2019), https://www.pc.gc.ca/en/lhn-nhs/nu/epaveswrecks/culture/histoire-history/qui-who.
[56] *Id*.
[57] *See generally* Nicole Perlroth, *How the United States Lost to Hackers*, N.Y. TIMES (Feb. 11, 2021), https://www.nytimes.com/2021/02/06/technology/cyber-hackers-usa.html.
[58] Walsh, *supra* note 11.
[59] *See* TOURO COLL. ILL., *supra* note 8.
[60] *Id*.
[61] *Id*.
[62] *Id*.
[63] *Id*.
[64] Christopher Wray, *Worldwide Threats to the Homeland: 20 Years After 9/11,* FBI (Sept. 22, 2021), https://www.fbi.gov/news/testimony/worldwide-threats-to-the-homeland-20-years-after-911-wray-092221.
[65] *See, e.g., Cyber Operations Tracker*, COUNCIL FOREIGN REL., https://www.cfr.org/cyber-operations/ (last visited Apr. 21, 2022).

Finding a solution to the cyberattacks that harass national infrastructures appears to be as elusive as the Northwest Passage.[66] But a solution is necessary for the success of this new age of exploration. "If a theory about international law is to be helpful, it must, of course, show how to identify the legal process in terms that enable the scientific observer or the active participant to isolate it for separate consideration."[67] Michel Bourély, a legal scholar, once noted, as to humanity's activities in space, that from the beginning "the international community was conscious of the need to organize [those activities] by adopting, as early as possible, a means of regulation."[68] Now humanity finds itself facing the need to organize cyber activities by adopting new standards or norms of behavior.[69] If cybersecurity experts and relevant stakeholders are to extend satellite services into deep space and beyond, then it is expected that better cooperation will exist in the space industry. Bourély adds that "[s]cholars as well as decision makers need to develop a comprehensive, yet convenient and economic, method that permits them to make adequate particular reference to the global community process in order to discharge effectively the intellectual tasks of inquiry and decision."[70] While space regulation materialized fairly quickly in the form of the Outer Space Treaty, in the cyber realm, this formalized evolution has been slow to change.[71] The problem is a symptomatic representation of historical developments that tied cyberspace to notions of control and cyberpower.[72] "By taking advantage of ambiguities in the law [some States] can sow doubt in the lawfulness of [defensive] responses, eliminating, limiting or delaying responses."[73] Cyber operations that support space activities represent various services, but no other potential military objectives. So, any use of force could trigger national liability and responsibility considerations, via Articles VI and VII of the Outer Space treaty.[74]

The US Joint Chiefs of Staff define the concept of a *cyber operation* as "the employment of cyberspace capabilities where the primary purpose is to

---

[66] *See* Daniel Wagner, *The Growing Threat of Cyber-Attacks on Critical Infrastructure*, IRMI, (June 2016), https://www.irmi.com/articles/expert-commentary/cyber-attack-critical-infrastructure.
[67] McDougal et al., *supra* note 54, at 811.
[68] Michel Bourély, *Space Commercialization and the Law*, 4 SPACE POL'Y 131, 132 (1988).
[69] *See id*.
[70] McDougal, et al., *supra* note 54, at 813.
[71] André Barrinha, *Could Cyber-Diplomacy Learn from Outer Space*, DIRECTIONS (Apr. 30, 2021) https://directionsblog.eu/could-cyber-diplomacy-learn-from-outer-space/.
[72] *See* Daniel T. Kuehl, *From Cyberspace to Cyberpower: Defining the Problem*, *in* CYBER POWER AND NATIONAL SECURITY, (Franklin D. Kramer et al. eds., 2009).
[73] Lotriionte, *supra* note 46, at 74.
[74] Sarah M. Mountin, *The Legality and Implications of Intentional Interference with Commercial Communication Satellite Signals*, 90 INTL. L. STUD. 101, 143–145, 148, 179 (2014).

achieve objectives in or through cyberspace."[75] Another approach to the same concept notes that it is also defined as the "planning and synchronization of activities in and through cyberspace to enable freedom of [maneuver] and to achieve military objectives."[76] These capabilities, for example, may involve "computers, software tools, or networks."[77]

The problem of security is not isolated to a particular industry or a particular nation. The risks are many and spread across all industry sectors. For example, Canada has faced severe difficulties in the cyber landscape similar to those experienced by the United States. For example, in 2018, "Canada's fourth and fifth largest bank confirmed that 'fraudsters' stole the personal and financial information of some of the banks' customers."[78] The Bank of Montreal and the Canadian Imperial Bank of Commerce's Simplii Financial acknowledged the loss of personally identifiable information.[79] The Canadian Centre for Cyber Security notes that "[c]yber threat actors are states, groups, or individuals who, with malicious intent, aim to take advantage of vulnerabilities, low cyber security awareness, or technological developments to gain unauthorized access to information systems in order to access or otherwise affect victims' data, devices, systems, and networks."[80] For example, Canada Post, the counterpart to the US Postal Service, fell victim to a cyber intrusion that lasted for years, although it was not reported until recently.[81] "The information affected is from July 2016 to March 2019, and 97 percent of it comprised the names and addresses of receiving customers."[82] In this case, the Canada Post vulnerability, similar to the US Target case, originated with a third party and was "a supply chain attack that allowed hackers to capture the names and addresses of almost one million senders and receivers of packages over a three-year period."[83] The direct target was

---

[75] U.S. JOINT CHIEFS OF STAFF, JOINT PUBLICATION 3-0, JOINT OPERATIONS (2017).
[76] Ministry of Defence, *UK Terminology Supplement to NATOTerm*, Joint Doctrine Publication 0-01.1 (Jan. 2019).
[77] CTR. FOR STRATEGIC LEADERSHIP, STRATEGIC OPERATIONS GUIDE (2021).
[78] Ms. Smith, *2 Canadian Banks Hacked, 90,000 Customers' Data Stolen*, CSO (May 29, 2018), https://www.csoonline.com/article/3276275/2-canadian-banks-hacked-90000-customers-data-stolen.html.
[79] *Id*.
[80] *Cyber threat and cyber threat actors*, CAN. CTR. FOR CYBER SEC. (last modified June 29, 2021), https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors.
[81] Twinkle Ghosh, *Canada Post Reports Data Breach to 44 Large Businesses, 950K Customers Affected*, GLOB. NEWS (May 26, 2021), https://globalnews.ca/news/7894760/canada-post-data-breach/.
[82] *Id*.
[83] Howard Solomon, *User Data on 950,000 Packages Exposed After Canada Post Falls Victim to Third-Party Hack*, IT WORLD CAN. (May 27, 2021), https://www.itworldcanada.com/article/user-data-on-950000-packages-exposed-after-canada-post-falls-victim-to-third-party-hack/447854.

Commport Communications, which supplied the Post with the electronic data interchange (EDI) solution that "manages the shipping manifest data of large parcel business customers."[84] In the US, the Cybersecurity and Infrastructure Security Agency (CISA) manages similar threats and collaborates with partners to secure the infrastructure.[85] CISA ensures that the systems, networks and critical infrastructure remain reliable "to better prepare for, respond to, and recover from natural or man-made disasters."[86] Now both nation collaborate as one unit with two nations reflected in the "Cybersecurity Action Plan," drafted to strengthen and integrate the cyber activities of the Department of Homeland Security and Public Safety Canada.[87]

The days before *Terror* and *Erebus* set sail were filled with social engagements and a general sense of excitement.[88] Without a doubt, "[n]o Arctic expedition had ever been so lavishly outfitted."[89] A lot has been discussed and written about governments' responsibility concerning their activities in all domains of human activity.[90] Yet, the conflicts in cyberspace are now a daily occurrence.[91] Another example, the Russian sponsored APT29 group, "also known as Cozy Bears," targeted British, American, and Canadian organizations to acquire secrets associated with developing the COVID-19 vaccine.[92] Disasters can be avoided if awareness accompanies the implementation of a plan guided by standards developed by the cybersecurity community. The specter of unanticipated vulnerabilities forces an honest examination of national policies. The worst possible scenario is one fueled by overconfident expectations. "Captain Sir John Franklin's two-ship expedition of 1845 was confidently expected to be the first to traverse the archipelago all the way from Baffin Bay to Bering Strait, linking the Atlantic and Pacific oceans by a Northwest Passage."[93]

---

[84] *Id*.
[85] *See Infrastructure Assessments and Analysis*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/infrastructure-assessments-analysis (last visited Apr. 21, 2022).
[86] *Id*.
[87] *Canada-United States Action Plan for Critical Infrastructure*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY https://www.cisa.gov/publication/canada-us-action-plan-critical-infrastructure (last visited Apr. 21, 2022).
[88] BEATTIE & GEIGER, *supra* note 48, at 39.
[89] *Id*. at 42.
[90] *See* Mark Raymond, *Managing Decentralized Cyber Governance: The Responsibility to Troubleshoot*, 10 STRATEGIC STUD. Q. 123, 140 (2016).
[91] *See* LOUK FAESEN ET AL., CONFLICT IN CYBERSPACE: PARSING THE THREATS AND THE STATE OF INTERNATIONAL ORDER IN CYBERSPACE 2–3 (2019).
[92] Kim Sengupta, *Cozy Bear: The Russian hacking group trying to steal the UK's coronavirus vaccine*, INDEPENDENT (July 16, 2020), https://www.independent.co.uk/news/uk/home-news/cozy-bear-russia-hacking-coronavirus-vaccine-oxford-imperial-college-a9623361.html.
[93] W. Gillies Ross, *The Admiralty and the Franklin Search*, 40 POLAR REC. 289, 289 (2004).

Unquestionably, the most remarkable threat is the numerous and complex cyberattacks that plague users' daily lives. These cyberattacks stand for opportunities of increased confusion and fear. The US and its allies most modernize and stay technologically ahead to maintain the needed superiority along with their national security. "The US stands alone as the only tier-one cyber power in the world, but China will rise as a highly capable peer competitor over the next decade, a new International Institute for Strategic Studies (IISS) report concludes."[94] The problem with a future cyberwar would be one of disruption and chaos. Defining new law for cyberspace, however, is currently unachievable.[95] A recent "report notes that China has evolved its cyber capabilities from 'a position of relative electronics backwardness' three decades ago to 'conduct[ing] large-scale cyber operations abroad, aiming to acquire intellectual property, achieve political influence, carry out state-on-state espionage and position capabilities for disruptive effect in case of future conflict.'"[96]

While a binding international cyber law may seem lost like the *Erebus*, the recent evolving norms seem to represent a hopeful opportunity.[97] Yet, the cyber-horizons that need navigating offer greater obstacles in outer space. On January 11, 2007, China launched an anti-satellite weapon (ASAT) into space to destroy its own FY-1 weather satellite located in low Earth orbit.[98] This intentional destruction of the Chinese weather satellite created a serious mess of debris in orbit, adding 300,000 new pieces of trash to the current debris problem around the planet.[99] The Chinese ASAT test caused global commotion and represented a sign that China had grown military capabilities in space.[100] Then there is China's willingness to hack US space assets, including "satellite operators, defense

---

[94] Brad D. Williams, *US 'Retains Clear Superiority' In Cyber; China Rising: IISS Study*, BREAKING DEF. (June 28, 2021), https://breakingdefense.com/2021/06/us-retains-clear-superiority-in-cyber-but-china-poised-to-challenge-study/.
[95] *See* Michael P. Fischerkeller, *Current International Law Is Not an Adequate Regime for Cyberspace*, LAWFARE: INT'L L. (Apr. 22, 2021), https://www.lawfareblog.com/current-international-law-not-adequate-regime-cyberspace.
[96] Williams, *supra* note 94.
[97] *See* Alejandro Guerrero et al., *International Cybersecurity and Data Privacy Outlook and Review–2022*, GIBSON DUNN (Jan. 31, 2022), https://www.gibsondunn.com/international-cybersecurity-and-data-privacy-outlook-and-review-2022/.
[98] *See* Phillip C Saunders & Charles D. Lutes, *China's ASAT Test Motivations and Implications*, JOINT FORCE Q., June 2007, at 39.
[99] *See* Joseph Stromberg, *There are 300,000 pieces of garbage orbiting earth, and it's a big problem*, VOX (Jan. 20, 2015), https://www.vox.com/2015/1/20/7558681/space-junk.
[100] *Id*.

contractors and telecommunications companies."[101] The case of Russia is equally troubling. On April 15, 2020, Russia conducted another ASAT test utilizing its Nudol interceptor.[102] Russia's cutting-edge spying tools now enables them to do much more in the form of cyberattacks.[103] Thoughts about the methods applied in space and their relations with information assurance bring the discussion in full circle to the human condition and those innate imperfections found in every human being. *Erebus* and *Terror* disappeared somewhere along their voyage, "seemingly swallowed by the ice and never heard from again, at least not from the explorers themselves."[104] The truth behind the ill-fated Arctic expedition seemed to disappear with the icy waters of the north.

III. The Human Condition

The Human condition could simply be understood as the participation of the human being in outer space activities.[105] The meaning of this idea has many ramifications and consequences. While space activities invite thoughts of cooperation and good will, these will not be omnipresent in those activities. As humanity moves into the space frontier, the activities of exploration and colonization will require the guidance provided by the rule of law. "The most intense strain on any concept of the rule of law is exercised in times of crisis."[106] It could be said that the need to colonize our solar system will be fuel by need more than curiosity. Then again, as new ways of militarization in outer space are developed, the shadow of conflict rises in the horizon of the human mind. "It has been argued that, especially in times of war and similar emergencies, the law recedes or even vanishes (*inter armas silent leges*)."[107] If this is the case, where would space law stand? Michael Bourély anticipated that these activities "responded to the idea that the new technologies being developed could

---

[101] Joseph Menn, *China-based campaign breached satellite, defense companies -Symantec*, REUTERS (June 19, 2018), https://www.reuters.com/article/china-usa-cyber/china-based-campaign-breached-satellite-defense-companies-symantec-idUSL1N1TL1K1.
[102] Mike Wall, 2020, *Don't panic about Russia's recent anti-satellite test, experts say*, SPACE (Apr. 30, 2020), https://www.space.com/russia-anti-satellite-weapon-fears-overblown.html.
[103] *See* Jack Stubbs, *SolarWinds hackers linked to known Russian spying tools, investigators say*, REUTERS (Jan. 11, 2021), https://www.reuters.com/article/us-global-cyber-solarwinds/solarwinds-hackers-linked-to-known-russian-spying-tools-investigators-say-idUSKBN29G0XT.
[104] Kat Eschner, *Tales of the Doomed Franklin Expedition Long Ignored the Inuit Side, but "The Terror" Flips the Script*, SQUARESPACE (April 6, 2018), https://kat-eschner.squarespace.com/blog/2018/4/6/tales-of-the-doomed-franklin-expedition-long-ignored-the-inuit-side-but-the-terror-flips-the-script.
[105] Shoaib Shafi, *Earth alienation: Hannah Arendt on outer space*, BIG THINK (Sept. 29, 2020), https://bigthink.com/hard-science/hannah-arendt-outer-space/.
[106] Siegfried Wiessner, *The Rule of Law: Prolegomena*, 41 ZDAR 85, 86 (2018).
[107] *Id*.

contribute to the moral and material progress of all the world's peoples."[108] Indeed, the space industry has the capabilities of pushing the boundaries to unexpected moral quandaries in the far reaches of outer space. The moral quandaries, or ethics of outer space, suggest the need for a new template of binding norms of cybersecurity in outer space.[109] If cyber norms are not applicable to all relevant situations, then what is the future of State-sponsored cyber operations? It is within this ambiguity that the spirit of the law conflicts with the letter of the law.[110] The modern landscape of outer space activities is one where "power allocation in space has changed a great deal as plethora of commercial actors have entered the domain, and a number of new State actors are asserting themselves, such as China and India."[111] The CEO, the military commanders, and relevant stakeholders must be cognizant of the ambiguity, which is more troublesome within the landscape of external and internal threats, their highest probability of occurrence and significant loss.[112] For example, the Ministry of State Security of China is one actor to be noted. "A federal grand jury in Spokane, Washington, returned an indictment . . . charging two hackers, both nationals and residents of the People's Republic of China, with hacking into the computer systems of hundreds of victim companies in the United States and abroad . . . "[113] The hackers stole terabytes of data, including data from medical device manufacturers.[114]

There is almost a sense of nostalgia of more inspiring times when men walked on the Moon. It was then, on December 7, 1972 that the final mission, Apollo 17, launched a Saturn V rocket from Kennedy Space Center traveling to the Moon and landing in the southeastern rim of Mare Serenitatis.[115] This mission transported the 11th and 12th astronauts to the surface of the Moon, and it was the first mission to include a scientist – a geologist – becoming the last voyage of its

---

[108] Michel Bourély, *Space commercialization and the law*, 4 SPACE POL'Y 131, 132 (1988).
[109] *See* John Shin, *supra* note 5.
[110] Blount, *supra* note 47, at 119.
[111] *Id*. at 120.
[112] *See* MICHAEL E. WHITMAN & HERBERT J. MATTORD, MANAGEMENT OF INFORMATION SECURITY 264 (6th ed. 2017).
[113] Press Release, Off. Pub. Aff., Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research (July 21, 2020), *available at* https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion.
[114] *See id*.
[115] *See* SMITHSONIAN NAT'L AIR & SPACE MUSEUM, *Apollo 17 (AS-512)*, https://airandspace.si.edu/explore-and-learn/topics/apollo/apollo-program/landing-missions/apollo17.cfm (last visited Apr. 21, 2022).

kind till today.[116] Almost fifty years later the lunar missions are seeing new life with the upcoming project named after the sister of Apollo: Artemis.[117] It is a new beginning or perhaps a continuation of the explorations from the age of empires.

The British government began seeking routes to the Pacific north of Eurasia in 1818.[118] The expeditions of the Royal Navy "into the North American Arctic pushed back the margin of the *terra incognita*, until the existence of one or more waterways through the islands north of the continental mainland seemed beyond doubt."[119] "At sea in the Arctic, it's easy to lose sight of where you are."[120] In the same way, a voyage of discovery in the High Arctic in late summer offers an environment "between the final melt and the next full freeze. Like clouds parting after a storm, the sea [cracks and drifts]."[121] In truth, the British chose the names of their ships to instill fear in the enemy during this unprecedented period of exploration and international interaction.[122] The same could be said of the enigmatic names utilized by the hacker groups and their destructive malware. Gillian Hutchinson, curator at the National Maritime Museum in London, noted that the ship name '*Erebus*' means "the darkness at the entrance to Hell."[123] For these ships, a journey into the darkness was about to begin. "The departure of *Erebus* and *Terror* to search for the North-West Passage was a major news story in Britain."[124] This journey serves as a reminder that there is a price to pay for space exploration and it is intertwined with the utilization of cyberspace. The law of cyber operations managed by the international community remains unresolved and in need of further clarification.[125] Space law expert Bin Cheng, explained:[126]

> In principle, even within a State's own territory, the State is not directly responsible for injuries caused to foreign States or their nationals by the acts of private

---

[116] *See* Elizabeth Howell, *Apollo 17: The Last Men on the Moon*, SPACE (Oct. 3, 2018), https://www.space.com/17287-apollo-17-last-moon-landing.html.
[117] Sarah Loff, *Artemis Overview*, NASA (July 19, 2019), https://www.nasa.gov/artemis/overview.
[118] *See* Elena Baldassarri, *The Northwest Passage as a Voyage to Myth and Adventure*, ENV'T & SOC. PORTAL, https://www.environmentandsociety.org/exhibitions/northwest-passage/northwest-passage-voyage-myth-and-adventure#top (last visited Apr. 21, 2022).
[119] Ross, *supra* note 93, at 289.
[120] *See* PAUL WATSON, ICE GHOSTS: THE EPIC HUNT FOR THE LOST FRANKLIN EXPEDITION (2017).
[121] *Id*.
[122] Hutchinson, *supra* note 50, at 41.
[123] *Id*.
[124] *Id*.
[125] *Id*.
[126] Bin Cheng, *Article VI of the 1967 Space Treaty Revisited: "International Responsibility," "National Activities," and "The Appropriate State"*, 26 J. SPACE L. 7, 11–12 (1998).

> persons, whether nationals or non-nationals, and whatever their number, from single individuals through mobs and rioters to whole revolutionary forces for as long as they remain unsuccessful revolutionaries.

The question that must follow should be: how will the CISOs know if a "private actor" is truly out of the purview of the State? As Rainn Ottis writes, "[o]ne of the biggest lessons [that emerged from the notorious 2007 Estonia cyberattack] is that in a modern "conflict, cyber-attacks [have become] increasingly more common and dangerous.[127] Any country with sufficiently well-developed network infrastructure is vulnerable to these attacks."[128] The overall national risk cannot be mitigated if it is not known or anticipated.[129] If we deconstruct this ethical ambiguity we uncover a much-needed rule of law applicable to cyberspace in outer space. It is this law that may offer the potential source of substantive justice, equality, and accountability.

The hopes and desires of the future are based on the belief that outer space is a realm of peaceful exploration and use. This applies to cyber operations that enhance space activities. It is of concern to assert that freedom of use to benefit humanity could become in danger with contested activities. However, space data poses new challenges for CISOs and other stakeholders. Indeed, the new race for the Moon and the subsequent race to Mars will face new cyberthreats, and risks will follow. Yet, these threats are antithetical to the enjoyment of human activities in space. The dark side of innovation raises many questions, but few answers are available. While most agree that international law applies in cyberspace, experts still wrestle with the universal consensus of how that law will be applied.[130] According to Anders Henriksen, "[i]n an anarchical cyberspace without 'rules of the road' and shared expectations of behavior, stronger states will be free to impose their will on weaker states and minor incidents may escalate and spin out of control."[131] For example, NASA is currently relying on potentially developing nuclear thermal propulsion (NTP) engine that would heat up liquid hydrogen to

---

[127] Rain Ottis, *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*, CCDCOE, https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.

[128] *Id*.

[129] MICHAEL E. WHITMAN & HERBERT J. MATTORD, PRINCIPLES OF INFORMATION SECURITY 231 (2016).

[130] Anders Henriksen, *The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace*, 5 J. CYBERSECURITY 1, 2 (2019).

[131] *Id*. at 1.

generate the required thrust.[132] These and other projects are promising as long as security is considered in the planning and subsequent processes.

The second age of exploration requires a move to modernize and stay technologically ahead. It is also necessary to keep a high level of awareness to maintain the superiority of national security. It is worrisome to note the frequency and severity of hacks. It is now a race that gains terrain with time, and time is a luxury that States lack. Captain Francis Crozier understood the dangers associated with overestimating dangerous conditions as noted in the story of *Terror*: "I suggest that we reverse course, avoid the pack ice to the southwest, and sail east and then south down the eastern coast of what may well be King William Island. At the very least, we will be sheltered . . . "[133] Unfortunately, the captain's suggestion was not put into action and the actual and final decision brought a certain doom to the crews. Over a dozen year period the British Admiralty dispatched a series of search expeditions, including private interests in both Britain and the United States.[134] But what will be the cost of space exploration if the gap between nations is filled with warfare? The world is now plagued with rising tensions that could ravage the globe as situations escalate into a conflict of military activities in outer space.[135] And, while the satellite industry predates the age of the Internet, which kept the space systems safe, satellites are now a component of the worldwide communications infrastructure that transfers data via cable and fiber.[136] These data transfers such as atmospheric imagery, television, navigation, and others provides redundancies since "satellite communications serve as a back-up to landlines."[137] While hacks of one of these systems could produce a simple shutdown, it could also give way to multiple catastrophic scenarios, including the jamming of signals to create confusion for operators of critical infrastructures.[138] Another scenario may entail a hacker manipulating the satellite's thrusters to crash it into another satellite, or even causing it to collide with the International Space Station.[139] In this new reality, organizations need to

---

[132] Jeff Foust, *Report Recommends NASA Accelerate Space Nuclear Propulsion Development*, SPACE NEWS (Feb. 12, 2021), https://spacenews.com/report-recommends-nasa-accelerate-space-nuclear-propulsion-development/.
[133] SIMMONS, *supra* note 1, at 79–80.
[134] Ross, *supra* note 93, at 289
[135] MYERS S. MCDOUGAL ET AL., LAW AND PUBLIC ORDER IN SPACE 17 (1963).
[136] Edward L. Bolton, Jr. *Cyber and Space – A Way Ahead*, 6 HIGH FRONTIER 8, 8 (Aug. 2010), *available at* https://www.afspc.af.mil/Portals/3/documents/HF/AFD-101019-079.pdf.
[137] *Id*.
[138] William Akoto, *Hackers Could Shut Down Satellites – Or Turn Them into Weapons*, THE CONVERSATION (Feb. 12, 2020), https://theconversation.com/hackers-could-shut-down-satellites-or-turn-them-into-weapons-130932.
[139] *Id*.

be more accepting of the idea that their business could be the next casualty of war.[140] Then again, information becomes that tool that makes all the difference. As the industry develops new technologies and begins to expand its horizons, it will be critical that organizations assess how cybersecurity awareness is incorporated into their future agendas.

Modern space activities have evolved for a new frontier that promises investors riches beyond the borders of the atmosphere.[141] Our modern age of communications offers new worlds within our own development and understanding. Consider that the Earth is about 238,855 miles away from the Moon.[142] Now consider the potential for a crime committed in outer space and the possibility that the Internet plays a part. Imagine if an astronaut receives terrible news from home, and in desperation, this otherwise intelligent individual accesses a bank account without permission, emptying the account in the process. The Space Force constable assigned a tour of duty to the space station may have to investigate such a novel case. The constable may discover that emails received by the astronaut from home were at the center of a divorce dispute. How would this crime be handled? Solutions will be needed to resolve new challenges arising out of private cyber activities during outer space activities. As human activities diversify in space, the relevant stakeholders will have to consider the expansion of what it means to participate in space activities. Visions of new worlds mingle with the lessons of the past. The borderless nature of cyberspace has turned outer space into a domain of uncertainty plagued by surreptitious activities. Yet, nations have a vested interest in protecting their space-based systems. These systems begin to operate in land and continue transmission in outer space. As nations seek ways to protect their national critical infrastructure sectors, the space industry community wrestles with challenges associated with innate vulnerabilities. However, not even the experienced mariners of the British Empire could have anticipated the horrors to be faced in the final months of their lives. "On July 9, 1845, two months after departing from Greenhithe, England, Warrant Officer John Gregory wrote a letter to his wife from Greenland in which he described seeing whales and icebergs for the first time,"[143] How then did this perfectly equipped and prepared expedition

---

[140] Rick Grinnell, *The Next Casualty of Cyberwar Could Be Your Business*, CIO (Jan. 28, 2020), https://www.cio.com/article/201923/the-next-casualty-of-cyberwar-could-be-your-business.html.
[141] *Id*.
[142] Tim Sharp, *How Far is the Moon?*, SPACE (Oct. 27, 2017), https://www.space.com/18145-how-far-is-the-moon.html.
[143] Bryan Pietsch, *His Ship Vanished in the Arctic 176 Years Ago. DNA Has Offered a Clue.*, N.Y. TIMES (May 5, 2021), https://www.nytimes.com/2021/05/05/science/hms-erebus-sailor.html.

end in disaster?[144] What transpired in the last days of the mission? "Gregory, who had never been to sea before, was aboard the *H.M.S. Erebus*," which came to be "stuck in ice in Victoria Strait, off King William Island in what is now the Canadian territory of Nunavut."[145]

IV. Reach for the Stars: Recommendations

Today, information-driven organizations offer services in an intriguing time of emerging outer space ventures. These ventures are unavoidably intertwined with cyber operations. The idea that a cyber operation is always an external threat is inaccurate. NASA' missions must factor security vulnerabilities and, at the same time, apply needed controls to counter potential issues.[146] NASA must also consider human behavior. To provide an example, a divorce sometimes takes perfectly reasonable individuals into a world of confused emotions. This is the real case of Summer Worden (a United States Air Force intelligence officer) and Anne McClain (a United States astronaut).[147] The case seemed simple enough: "Summer Worden ... [was] in the midst of a bitter separation and parenting dispute ... [and] was surprised when she noticed that her estranged spouse still seemed to know things about her spending. Had she bought a car? How could she afford that?"[148] By using her intelligence background and inquiring with the bank, Worden realized that her bank account had been accessed with her login credentials from outer space.[149] . Could this be the first case in outer space where the Computer Fraud and Abuse Act (CFAA) was applicable? In other words, did Anne McClain have permission to access the information in question? For the space constable, this case investigates, clarifies, and offers a normative approach for the benefit of potential new and complicated cases in the space domain.

---

[144] Robin McKie & Vanessa Thorpe, *What Happened on HMS Terror? Divers Plan Return to Franklin Wrecks*, THE GUARDIAN (Mar. 14, 2021), https://www.theguardian.com/science/2021/mar/14/what-happened-on-hms-terror-divers-plan-return-to-franklin-wrecks.

[145] Pietsch, *supra* note 143.

[146] *See* Bob Allin, *How to Implement a Security Awareness Program at Your Organization*, THREAT STACK, https://www.threatstack.com/blog/how-to-implement-a-security-awareness-program-at-your-organization (last visited Apr. 21, 2022).

[147] Mike Baker, *NASA Astronaut Anne McClain Accused by Spouse of Crime in Space*, N.Y. TIMES (Aug. 27, 2020), https://www.nytimes.com/2019/08/23/us/astronaut-space-investigation.html.

[148] *Id*.

[149] *Id*.

a. Recommendation #1: The CFAA

The Computer Fraud and Abuse Act (CFAA) of 1986 was drafted to criminalize computer crimes outside the scope of existing mail and wire fraud statutes, and originally covered unauthorized access of "federal interest" computers.[150] Yet, given its interstate reach, "it effectively criminalized any unauthorized computer access," and its reach expanded further in 1996 when amendments substituted the language "federal interest computer" with "protected computer."[151] The statute reads:[152]

> (a) Whoever-
> . . .
> (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains-
> (A) information contained in a financial record of a financial institution . . .

In the case at hand, "Ms. Worden's spouse, [astronaut] Anne McClain, was a decorated NASA astronaut on a six-month mission aboard the International Space Station."[153] Astronaut McClain admitted to accessing the bank account from outer space.[154] Yet, these facts alone do not solve the case. As noted by a commentator from the Council of Foreign Relations, this situation raises the larger question of "whether the United States [had] criminal jurisdiction over the astronaut in question and what criminal law applies to U.S. nationals in space."[155] The case centered on using the space station to connect with a terrestrial computer system, with possible criminal intent, thus entering the CFAA scope.[156] Ms. Worden "filed a complaint with the Federal Trade Commission and her family lodged one with NASA's Office of Inspector General, accusing Ms. McClain of identity theft and improper access to Ms. Worden's private financial records."[157] How might this case be resolved? The CFAA, as noted earlier, states that one cannot "intentionally access a computer without authorization or exceed

---

[150] William K. Kane & Melissa M. Mikail, *Extraterritorial Application of the Computer Fraud and Abuse Act*, 10 NAT'L L. REV. (Jul. 3, 2020), https://www.natlawreview.com/article/extraterritorial-application-computer-fraud-and-abuse-act#google_vignette.
[151] *Id*.
[152] *See* 18 U.S.C. § 1030(a)(2)(A) (2010).
[153] Baker, *supra* note 147.
[154] *Id*.
[155] Fidler, *supra* note 42.
[156] *Id*.
[157] Baker, *supra* note 147; 18 U.S.C. § 1030 (2010).

authorized access, and thereby obtain . . . information contained in a financial record of a financial institution . . . " Could the CFAA apply in outer space, and how would it apply to this case? The answer requires a closer look at the pertinent US law, treaty law, and a presidential directive.

The international law of outer space is guided by five treaties.[158] The main treaty, known colloquially as the Outer Space Treaty, is the most pertinent.[159] This treaty, ratified by the US, sets the stage for the law of outer space, yet does not provide a legal remedy for the criminal activity referenced in the case at hand.[160] "The law of outer space has developed as a discrete body of law within general public international law. Since the launch of Sputnik 1 in 1957, this process of evolution has been remarkably rapid, largely driven by the need to agree on rules to regulate activities in this new 'frontier.'"[161] A direct examination of the OST provides guidance in this particular case. This agreement, as noted earlier, declares, "Outer space, including the moon and other celestial bodies, shall be free for exploration and use by all States without discrimination of any kind, on a basis of equality and in accordance with international law, and there shall be free access to all areas of celestial bodies."[162] This freedom to explore permits the activities of NASA in outer space as the space agency of the US government but does not provide direct guidance regarding a potential crime carried out by an astronaut in outer space. OST Article VI states in relevant part that "States Parties to the Treaty shall bear international responsibility for national activities in outer space, including the moon and other celestial bodies . . . " and OST Article VIII notes that "[a] State Party to the Treaty on whose registry an object launched into outer space is carried shall retain jurisdiction and control over such object, and over any personnel thereof, while in outer space or on a celestial body."[163] As no other provisions of the space treaties address crime directly, other factors would prove useful for our constable.

The Internet was designed to be a free-flowing avenue of data transmission.[164] This network of networks was "conceived [as] a level playing

---

[158] *Space Law Treaties and Principles*, U.N. OFF. FOR OUTER SPACE AFF. (2022), https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties.html.
[159] *See generally* Outer Space Treaty, *supra* note 17.
[160] *Id*. (providing no specific criminal legal remedies).
[161] Ram Jakhu & Steven Freeland, *The Relationship Between the Outer Space Treaty and Customary International Law*, SSRN (June 13, 2019), https://ssrn.com/abstract=3397145.
[162] Outer Space Treaty, *supra* note 17, at art. I.
[163] *Id*. at art. VIII.
[164] Russell Brandom, *We Have Abandoned Every Principle of the Free and Open Internet*, THE VERGE (Dec. 19, 2017), https://www.theverge.com/2017/12/19/16792306/fcc-net-neutrality-open-internet-history-free-speech-anonymity.

field for different networks and protocols, with no sense that the same openness could enable a new kind of monopoly power. Most painfully, this new network was imagined as a forum for the free exchange of ideas, with no sense of how predatory and oppressive that exchange would become."[165] Indeed, that founding ideal began to collapse in 1988, when Robert Tappan Morris accidentally released the first malicious worm on the Internet, shutting down about ten percent of internet-connected computers.[166] The same idealism had echoed in the thoughts of the brave crews of the *Erebus* and *Terror*, who were "well on their way, nearing Iceland, when [the captain] reveled in the sight of porpoises, bounding out of the waves at the ships' bows, and a sea bird similar to a petrel."[167] However, for those British explorers, the unidentifiable nature of potential danger predicted disaster.

Our constable, on the other hand, must first be aware of the nature of cyber operations. "The sheer pace of change and the broadening of potential activities in outer space dictates that we need to continually monitor the scope and content of this framework, whilst at the same time recognizing that, at least from a strictly legal regulatory perspective, it will not (ever) be possible for the law to keep up with these changes."[168] Indeed, our marshal must gather all the tools available to understand this landscape. A legal parallel would be the next reasonable step. "Generally speaking, a parallel may be drawn between crimes committed on board an aircraft flying over the high seas or a ship on the high seas, and crimes perpetrated within the confines of a spacecraft."[169] If the state of registry or flag can determine jurisdiction over aircraft personnel, then in outer space, OST Article VIII determines jurisdiction over spacecraft personnel based on the launching party.[170] In this case, that space object is the International Space Station.

The International Space Station Agreement (or ISS Agreement) is the legal guidebook for activities related to the space station.[171] Article 5 notes in part that "each Partner shall retain jurisdiction and control . . . over personnel in or on the Space Station who are its nationals."[172] Article 22 of the agreement addresses

---

[165] *Id*.
[166] Jack Goldsmith, *How Cyber Changes the Laws of War*, 24 EUR. J. INT'L L. 129, 129 (2013).
[167] WATSON, *supra* note 120, at 121.
[168] Steven Freeland, *The Limits of Law: Challenges to the Global Governance of Space Activities*, 153 J. PROC. ROYAL SOC'Y N.S.W. 70, 71 (2020).
[169] Stephen Gorove, *Criminal Jurisdiction in Outer Space*, 6 INT'L LAW. 313, 317 (1972).
[170] *Id*.
[171] *See generally* Agreement Concerning Cooperation on the International Space Station, Jan. 29, 1998, T.I.A.S. 12927.
[172] *Id*. at art. V.

criminal jurisdiction.[173] Subsection (1) states in relevant part that "the United States may exercise criminal jurisdiction over personnel in or on any flight element who are their respective nationals." The agreement "uses the criminal law of the state of the nationality of individual astronauts."[174] In this manner, Article 22 provides the US with the power to exercise criminal jurisdiction over US personnel in the ISS. But the actual exercise of this jurisdiction requires an additional extraterritorial element. Federal law as delineated in 18 U.S. Code § 3238, states:[175]

> The trial of all offenses begun or committed upon the high seas, or elsewhere out of the jurisdiction of any particular State or district, shall be in the district in which the offender, or any one of two or more joint offenders, is arrested or is first brought; but if such offender or offenders are not so arrested or brought into any district, *an indictment or information may be filed in the district of the last known residence of the offender or of any one of two or more joint offenders, or if no such residence is known the indictment or information may be filed in the District of Columbia.*

This statute, in combination with the ISS Agreement Articles 5 and 22, offers our station constable and his colleague prosecutor an opportunity to tackle this case. The next step would be to explore how the development of new technologies interacts with US law. Specifically, "[i]t is important to recognize that the important issues that arise from the continuing development of cyber technology are increasingly relevant for the regulation of outer space, given the increasing rush towards a 'digitization' of space activities."[176] This recognition triggers the next legal inquiry that brings our astronaut under US terrestrial control. The provisions of US federal law, Special Maritime and Territorial Jurisdiction of the United States, as defined in 18 U.S.C. § 7(6) state:[177]

---

[173] *Id*. at art. XXII.
[174] *See id*.; Christopher J. Newman, *Exploring the Problems of Criminal Justice in Space,* ROOM—SPACE J. ASGARDIA (2016), https://room.eu.com/article/exploring-the-problems-of-criminal-justice-in-space.
[175] 18 U.S.C. § 3238 (2010).
[176] Freeland, *supra* note 168, at 71–72.
[177] 18 U.S.C. § 7 (2011).

> The term 'special maritime and territorial jurisdiction of the United States', as used in this title, includes:
> (6) Any vehicle used or designed for flight or navigation in space and on the registry of the United States pursuant to the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies and the Convention on Registration of Objects Launched into Outer Space, while that vehicle is in flight . . .

Indeed, there is little literature about this section of the law and has remained mainly unused except for a few aviation cases. This statute which is now very relevant seems to have escaped the attention of mainstream scholars that have concentrated their attention exclusively in the ISS Agreement and the Outer Space Treaty.[178] US law involves one final provision, that as of now, has not been changed or updated. A legacy of the Trump administration's, "Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems" delineates the cybersecurity policy for space systems.[179] Section 3 states that "[c]ybersecurity principles and practices that apply to terrestrial systems also apply to space systems . . . Effective cybersecurity practices arise out of cultures of prevention, active defense, risk management, and sharing best practices."[180] While the U.S. government has gone through a change in federal administration, "one thing that most experts say will stay the same in principle is Space Policy Directive 5."[181] Our constable and prosecutor, having demonstrated the interests of the U.S. government in protecting its communication network in outer space and having delineated the jurisdictional parameters, return to the CFAA. The CFAA brings significant factors together in finding jurisdiction.[182] In *United States v. Ivanov*, the court was analyzing an earlier cyber-ransom case involving the breach of computers belonging to an e-commerce company known as the Online Information Bureau (OIB).[183] The court's reasoning is applicable to a case

---

[178] Elizabeth Gaspar Brown, *Jurisdiction of United States Courts over Crimes in Aircraft*, 15 STAN. L. REV. 45, 71 (1962).
[179] Memorandum from the President of the U.S. to the Off. of Space Com. (Sept. 4, 2020), *available at* https://history.nasa.gov/SPD-5.pdf.
[180] *Id*.
[181] Joe Jabara, *Space Policy Directive 5 and Beyond: Challenges of Cybersecurity in Space,* CLEARANCEJOBS (April 29, 2021), https://news.clearancejobs.com/2021/04/29/space-policy-directive-5-and-beyond-challenges-of-cybersecurity-in-space/.
[182] Fraud and Related Activity in Connection with Computers, 18 U.S.C. § 1030(a) (2021).
[183] U.S. v. Aleksey Vladimirovich Ivanov, 175 F. Supp. 2d 367, 368–69 (D. Conn. 2001).

in outer space. In *Ivanov*, the court explained that regarding "subject matter jurisdiction over each of the charges against Ivanov, whether or not" the relevant statutes for the substantive offenses were "intended by Congress to apply extraterritorially, because the intended and actual detrimental effects of the substantive offenses . . . occurred within the United States" there was jurisdiction.[184]

The case of Anne McClain, it has been suggested, involves the CFAA's applicability to U.S. astronauts engaged in space activities.[185] First, these activities involved cyberspace. Second, Node #2 of the International Space Station, includes a U.S. "On-orbit Segment" that houses the quarters of four astronauts, which among other things, "provides a personal, private location for crew members to sleep, relax . . . call home . . . [and is] designed with . . . laptop connections, and internet connection to allow crew members personal communication with family and friends."[186] In *LVRC Holdings, LLC v. Brekka*, the employee accessed the employer's computer system without his knowledge or permission.[187] The question was whether an employee needed permission to access the organization's computers.[188] The court explained that "a person who 'exceeds authorized access,' has permission to access the computer, but [ends up accessing] information on the computer that the person is not entitled to access."[189] The *Brekka* court noted in relevant part that "§ 1030 is primarily a criminal statute, and §§ 1030(a)(2) and (4) create criminal liability for violators of the statute. Although this case arises in a civil context, our interpretation of §§ 1030(a)(2) and (4) is equally applicable in the criminal context . . . The Supreme Court has long warned against interpreting criminal statutes in surprising and novel ways that impose unexpected burdens on defendants."[190] The challenge here is the location of outer space. Could US law be extended beyond national boundaries? "The Constitution grants Congress broad powers to enact laws with extraterritorial scope . . . [and] provides criminal and civil remedies resulting from unauthorized access to computers used in interstate commerce or communications. And, it further provides for extraterritorial jurisdiction for

---

[184] *Id*. at 373.
[185] Fidler, *supra* note 42.
[186] Thilini Schlesinger et al., *International Space Station Crew Quarters On-Orbit Performance and Sustaining*, AEROSPACE RSCH. CENT. 1 (July 11, 2013), https://arc.aiaa.org/doi/abs/10.2514/6.2013-3515.
[187] LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1129 (9th Cir. 2009).
[188] *Id*. at 1132.
[189] *Id*. at 1133.
[190] *Id*. at 1134.

criminal or civil violations of the CFAA."[191] Could questions about the presumption against extraterritoriality arise given the location and involvement of astronauts of other nations? It is likely that the CFAA will be applicable in Cislunar space.

In the end, NASA must take into consideration the human factor. In the case at hand, Anne McClain insisted that she was merely shepherding the couple's still-intertwined finances.[192] Assuming all things being equal, the § 1030(a)(2) test was not met since her access was still authorized.[193] Yet, the question of the CFAA's applicability in outer space has not been fully assessed—and definitely—hardly tackled by the US governments or the courts. Anne McClain was eventually cleared of all charges. "U.S. Attorney Ryan Patrick from the United State Attorney's Office in the Southern District of Texas, [announced that] Worden [had] been charged with lying about the alleged offense."[194] Ms. McClain, on the other hand, was selected for the Artemis mission.[195] One fundamental lesson from this case is best stated as a question: what can the U.S. government do to prepare for the next crisis? Astronauts will carry their human failings to the Moon, Mars, and beyond. A federal court sooner or later must decide the applicability of the CFAA to a case in outer space. The answer to the protection of communications in outer space is tied to the modernization of the

---

[191] William K. Kane & Melissa M. Mikail, *Extraterritorial Application of the Computer Fraud and Abuse Act*, NAT'L L. REV. (April 13, 2022), https://www.natlawreview.com/article/extraterritorial-application-computer-fraud-and-abuse-act. *See also* RJR Nabisco, Inc. v. Eur. Cmty., 136 S.Ct. 2090, 2093–2094 (2016) (describing extraterritoriality further, the U.S. Supreme Court noted that "[t]he law of extraterritoriality provides guidance in determining RICO's reach to events outside the United States." First, the Court asks whether the presumption against extraterritoriality has been rebutted—*i.e.*, whether the statute gives a clear, affirmative indication that it applies extraterritorially. This question is asked regardless of whether the particular statute regulates conduct, affords relief, or merely confers jurisdiction. If, and only if, the statute is not found extraterritorial at step one, the Court moves to step two, where it examines the statute's "focus" to determine whether the case involves a domestic application of the statute. If the conduct relevant to the statute's focus occurred in the United States, then the case involves a permissible domestic application even if other conduct occurred abroad; but if the relevant conduct occurred in a foreign country, then the case involves an impermissible extraterritorial application regardless of whether other conduct occurred in U.S. territory. In the event the statute is found to have clear extraterritorial effect at step one, then the statute's scope turns on the limits).

[192] *Id*. at 1134.

[193] Baker, *supra* note 147.

[194] Chelsea Gohd, *Astronaut Anne McClain's Estranged Wife Charged with Lying about Alleged 'Space Crime,'* SPACE (Apr. 7, 2020), https://www.space.com/astronaut-anne-mcclain-wife-charged-lying-space-crime.html.

[195] Press Release, NASA, NASA Names Artemis Team of Astronauts Eligible for Early Moon Missions (Dec. 9, 2020), *available at* https://www.nasa.gov/press-release/nasa-names-artemis-team-of-astronauts-eligible-for-early-moon-missions.

statute. Congress must amend the CFAA once more to account for cyber activities and to fall in harmony with the Outer Space Treaty. However, "[l]aw does not arise automatically from technical necessities as perceived by an orderly mind. It is not a static body of rules enshrined in treaties, statutes, and textbooks."[196] As time passes and technologies evolve, it is reasonable to deduce that the law will need further amendments, while courts struggle to keep up. But then again, that is precisely the function of law. "Law is a continuing process of interaction in which, at the global level, decision-makers of individual territorial communities unilaterally put forward claims such as those relating to" cyber operations.[197] If we cannot evolve over time, confusion will compromise our nation's security, commercial organizations, and the trust of the consumers. In this day and age, our data is the most valuable commodity. Yet, at the moment, its protection is in doubt.

b. Recommendation #2: The Outer Space Treaty in Spirit

The outer space industry must be understood as more than a new frontier of exploration. It is a challenging and dangerous domain for the human species. The new space traveler is in harm's way when exploring the unknown simply because humanity must return to outer space. It is a new environment capable of supporting space activities and unimaginable challenges. It is threats raised now that concern the attention of security professionals. Experts can only wonder about the emerging threats that may arise from outer space. Indeed, it would be highly beneficial if the industry adopted a formalized process, which began with the Outer Space Treaty. A world united in peace is a better world. There is an overwhelming agreement about this particular statement.[198] In the ambit of outer space, this is amplified by the principles enshrined in the Outer Stace Treaty.[199] "The legal principles of current international space law, especially the Outer Space Treaty, recognize the inclusive interest of the international community — that is, the global public interest — in outer space by assuring all States the right of free access to outer space without discrimination of any kind."[200] Yet, there seems to be equally hidden forces at work that seek to overturn years of progress. Nowhere this is more obvious than in cyberspace. As the industry develops new

---

[196] Siegfried Wiessner, *The Public Order of the Geostationary Orbit: Blueprints for the Future*, 9 YALE J. WORLD PUB. ORD. 217, 235 (1983).
[197] *Id*.
[198] *See generally* Nenad Bach, *World Peace in One Hour*, U.N. CHRONICLE (Sept. 21, 2020), https://www.un.org/en/un-chronicle/world-peace-one-hour.
[199] *See generally* Outer Space Treaty, *supra* note 17.
[200] Ram Jakhu, *Legal Issues Relating to the Global Public Interest in Outer Space*, 32 J. SPACE L. 31, 32 (2006).

technologies and begins to expand its horizons, it will be critical that organizations assess how cybersecurity awareness is incorporated into the agendas of executives and staff, given that it can affect the success or failure of any company.[201] Fortunately, the Outer Space Treaty was drafted as a visionary document: "Desiring to contribute to international cooperation in the scientific and the legal aspects of the exploration and use of outer space, those who drafted the Outer Space Treaty intentionally kept its scope broad enough to govern all future space activities."[202]

Executives, military commanders, CISOs, and other relevant stakeholders must engage security issues with awareness, education, and training. The threats to organizational assets could be a form of meddling into a satellite or loss of data being transmitted by a satellite.[203] Legacy satellite platforms add another layer of threats with inconsistent software patching, weak encryption, and old equipment.[204] Furthermore, the space environment is also susceptible to human errors and the supply chain.[205] For example, some satellites components are manufactured outside the U.S., and "vulnerabilities can be built in by threat actors."[206] As stakeholders continue to learn new exploration methods, cyberspace has emerged as part of that frontier, where mysteries indigenous to the cyber realm begin to occupy those exploring outer space. However, a template for general rules of application relies of the nonbinding nature of norms of behavior designated by those who draft them. In contrast, "[t]he Outer Space Treaty is not a collection of idealistic goals without legal implications. The intention of the authors of the Treaty was clearly to create binding obligations. The Treaty's principles must be interpreted as legally authoritative norms that govern international relations in all matters relating to outer space."[207] The same should be said of international cyber norms.

The nature of these norms have been addressed multiple times by the United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International

---

[201] Michael Hansen, *How to Create Better Cyber Security Training for Managers and Your C-Suite*, EDGEPOINT, https://www.edgepointlearning.com/blog/cyber-security-training-for-managers/.
[202] Jakhu, *supra* note 200, at 32.
[203] Mark Holmes, *The Growing Risk of a Major Satellite Cyber Attack,* VIASATELLITE, http://interactive.satellitetoday.com/the-growing-risk-of-a-major-satellite-cyber-attack/ (last visited Apr. 21, 2022).
[204] *Id*.
[205] *Id*.
[206] *Id*.
[207] Jakhu, *supra* note 200, at 34.

Security.[208] Their work has been reflected in the General Assembly Resolutions 65/41 (adopted 8 December 2010), 68/243 (adopted 27 December 2013), and 70/174 (adopted 17 December 2015).[209] The 2018 United Nations's *Open-ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security* worked on similar issues as the GGE.[210] The OEWG final report observed that the [GGE] "recommended 11 voluntary, non-binding norms of responsible State behaviour and recognized that additional norms could be developed over time."[211] Later, the 2019-2020 UN GGE delineated critical observations, among them:

- "The measures recommended by previous GGEs and the OEWG represent an initial framework for responsible State behavior in the use of ICTs. As further guidance, and to facilitate such cooperation, the Group recommends that States put in place or strengthen existing mechanisms, structures and procedures at the national level such as relevant policy, legislation and corresponding review processes; mechanisms for crisis and incident management . . . "[212]

- "An affected State's response to malicious ICT activity attributable to another State should be in accordance with its obligations under the Charter of the United Nations and other international law . . . "[213]

- "With regard to this norm, ICT activity that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public can have cascading domestic, regional and

[208] *See* Group of Governmental Experts on Development in the Field of Info. and Telecomm. in the Context of Int'l Sec., ¶¶9–15, U.N. Doc. A/70/174 (July 22, 2015).
[209] G.A. Res. 106, 70/174, ¶ 5 (Dec. 17, 2015).
[210] *See* Rep. of the Open-Ended Working Group on Developments in the Field of Info. and Telecomm. in the Context of Nat'l Sec., ¶¶ 7–8, U.N. Doc. A/AC/.290/2021/CRP.2 (Mar. 10, 2021).
[211] *Id*. at ¶ 7.
[212] Rep. of the Group of Governmental Experts on Advancing Responsible State Behav. in Cyberspace in the Context of Int'l Sec., ¶ 21, U.N. Doc. A/76/135 (July 14, 2021).
[213] *Id*. at ¶ 25.

> global effects. It poses an elevated risk of harm to the population, and can be escalatory, possibly leading to conflict."[214]

While the discussions and work produced have merit, it is not enough in the ambit of cyber operations. In the future, the work of GGE and OEWG may become binding international law. But, at present, it is not useful at a time when it is needed most. While some nations "give lip service to the need to keep space secure, none seems to be willing to truly engage in substantive talks on maintaining multilateral space security and, instead, opt to entrench themselves within their own national interests."[215] Stakeholders from the cyber and space domains suffer from a lack of will. Cybersecurity threats and cyberattacks will overshadow the daily activities of governments and corporations if corrective action is not taken. "Interestingly, it is these same [nations] that [will] have the most to lose if there is an escalation to conflict in the space environment."[216] Moreover, the present state of the cybersecurity culture of the satellite industry is worrisome. A complete failure of outer space-critical infrastructure systems during an emergency would be disastrous. The question of the security of the critical infrastructure systems for the space industry has not been fully assessed—and possibly—hardly assessed by governments or the commercial sector. Assuring the confidentiality, integrity, and availability of information is critically important. It all begins with the nature of the data and what it means to humanity. A shift towards greater cooperation and harmonization of policies among various stakeholders in the cyber ecosystem will be beneficial. The GGE and OEWG are only the beginning. As nations seek ways to protect their critical national infrastructure, the space industry will grapple with extraordinary challenges associated with common vulnerabilities exploited by malicious online attacks. In order to apply international cyber law to space activities, Article III of the Outer Space Treaty must highlight cyber activities in outer space. The applicability of Article III rests in its language:[217]

> "States Parties to the Treaty shall carry on activities in the exploration and use of outer space, including the Moon and other celestial bodies, in accordance with international law, including the Charter of the

[214] *Id*. at ¶ 42.
[215] Blount, *supra* note 47, at 120.
[216] *Id*.
[217] Outer Space Treaty, *supra* note 17, at art. III.

> United Nations, in the interest of maintaining international peace and security and promoting international co- operation and understanding."

In this manner, Article III provides a bridge between international law and its protections. "The freedom of use of outer space does not include its 'misuse' or 'abuse.' Under international law, the concept of 'abuse of rights' provides that States are responsible for their acts 'which are not unlawful in the sense of being prohibited' but cause injury to other States."[218]

On the other hand, a warning currently is in order. Failing to ensure that an organization complies with all laws and regulations increases the odds of liability and irreparable damage to the organization's reputation.[219] An organization that signals a lax attitude is tempting for unscrupulous employees, while running a tight ship means that risk management is part of the corporate culture of accountability and responsibility.[220] The same can be said of nations that turn a blind eye to rogue actors within their borders. "The rule of law rather than the rule of unilateral force should apply not only to international relations on the Earth but also to all activities in and from outer space."[221] Thus, the spirit of the Outer Space Treaty should always be omnipresent. The treaty should temper cyber operations with the freedom of exploration and use of outer space.

V. Conclusion

The truth behind the ill-fated Arctic expedition was cloaked in mystery. Then, in 1984, "Owen Beattie, a Canadian anthropologist, exhumed . . . three Beechey Island graves in order to examine, X-ray and autopsy their contents."[222] While the totality of the disaster cannot be fully measured, one clue sheds some light on the mystery. In the same manner, the analysis presented here demonstrates the sources of recommendation for cyber policy. As technology evolves, the means to protect data becomes increasingly sophisticated. But will these means ever guarantee national security?? There is no doubt that there will be governments involved in cyber operations designed to interfere with

---

[218] Jakhu & Freeland, *supra* note 161, at 9.
[219] Mike Michalowicz, *5 Potential Consequences of Ignoring Business Risk Management*, AM. EXPRESS (Apr. 16, 2018), https://www.americanexpress.com/en-us/business/trends-and-insights/articles/5-potential-consequences-of-ignoring-business-risk-management/
[220] *Id*.
[221] Jakhu & Freeland, *supra* note 161, at 1.
[222] Leanne Shapton, *Artifacts of a Doomed Expedition*, N.Y. TIMES (Mar. 20, 2016), https://www.nytimes.com/interactive/2016/03/20/magazine/franklin-expedition.html.

organizations and national infrastructures abroad and in violation of international norms. National borders are what create the price differentials that drive the immense profits of illicit commerce. These also provide shields for criminals to hide behind, guarding them from law enforcement agencies and governments seeking to disrupt their activities."[223] This is precisely the problem that emerges within the activities of governments and those that abuse cyberspace. In other words, "it is about criminalized states and the future configuration of power within the state system.[224] The nature of cyber activities with apparent ties to foreign governments needs the immediate intervention of the international community. Some of these actors seem to serve a particular master, or at a minimum, they are significantly encouraged to harass other nations by that master. The landscape of cyberthreats is further complicated because of the disruption caused by these non-state actors. One prominent group that fits the definition is Sandworm. This group is known for its use of BlackEnergy, "a Trojan that is used to conduct DDoS attacks, cyber espionage, and information destruction attacks," but has been particularly effective in disrupting " Industrial Control Systems."[225] Sandworm is believed to be associated with the General Staff of the Armed Forces of the Russian Federation, also known as GRU.[226] BlackEnergy's M.O. is as follows: "using spear-phishing emails carrying malicious Excel documents [or Word] with macros to infect computers in a targeted network.[227] This type of attack may contain the destructive plugin known as KillDisk, which destroys the "data stored on the infected machine's hard drive by overwriting the content of files."[228] These hackers seemingly possess a level of sophistication beyond standard.[229] The question then would be: could Sandworm be defined as an agent of the Russian government? If the Russian government is aware, then Sandworm should be considered under the control of Russia. In this landscape, the rule of "law would indeed serve [stakeholders], not the other way around, and thus anchor the rule of law properly in [their] very own needs and

---

[223] Michael Miklaucic & Moisés Naím, *The Criminal State*, *in* CONVERGENCE: ILLICIT NETWORKS AND NATIONAL SECURITY IN THE AGE OF GLOBALIZATION 149, 151 (Michael Miklaucic & Jacqueline Brewer eds., 2013).
[224] *Id*. at 152.
[225] *BlackEnergy APT Attacks in Ukraine*, KASPERSKY, https://www.kaspersky.com/resource-center/threats/blackenergy (last visited Apr. 21, 2022).
[226] Andrew Marino, *Sandworm Details the Group Behind the Worst Cyberattacks in History*, THE VERGE (July 28, 2020), https://www.theverge.com/21344961/andy-greenberg-interview-book-sandworm-cyber-war-wired-vergecast.
[227] KASPERSKY, *supra* note 225.
[228] Eduard Kovacs, *BlackEnergy Malware Used in Ukraine Power Grid Attacks,* SEC. WEEK (Jan. 4, 2016), https://www.securityweek.com/blackenergy-group-uses-destructive-plugin-ukraine-attacks.
[229] KASPERSKY, *supra* note 225.

aspirations."[230] New space technologies represent a leap in human ingenuity and innovation. But these also represent unforeseen dangers. "A total of 39 missions were sent to the Arctic" in search of the lost ships.[231] A true mystery, one clue surfaced over time: the food.[232] "The expedition's tinned food, hailed as cutting-edge technology and stocked in abundance, had been contaminated by lead solder used to seal the tins and was the most likely culprit."[233] Yet, "the exact circumstances of their deaths" continue to be shadowed in mystery.[234]

The nations of the world, particularly in the emerging commercial space ventures, have a vested interest in protecting their activities in outer space, including those that rely on satellite network security. "Dream or nightmare, we have to live our experience as it is, and we have to live it awake. We live in a world which is penetrated through and through by science and which is both whole and real."[235] While new space stakeholders progress into a new contested frontier, the global community watches with hope for a better future. Nevertheless, there are political considerations that need to be examined based on the realities of outer space. Space data possess new challenges for CISOs. Indeed, the race to Mars and beyond will face cyberattacks and all the risks attached to them. Additionally, the ethical ramifications regarding the regulation of private activities in space are a new challenge and a new opportunity. The future will be ripe with opportunities to further evolve the dimensions of outer space commerce, but only if stakeholders work together to redefine the security landscape of space objects. The purpose, then, of this future process will be to address the present cyberthreats that now lurk in outer space. In the perspective of the foregoing discussion, it is perhaps becoming evident how fundamental the law of outer space is and how it must evolve with the changing realities of managing information security. The appropriate scope of inquiry, then, must be tied to solutions or recommendations that support the ultimate benefit: to protect and propel the sustainable development of the industry.

The final thought is about the actions at the national and international stage. It is about the primary motivations behind the present policies and the limitations described. This article assessed the cyberthreat landscape in outer space while offering recommendations. Hopefully this report offers guidance on

---

[230] Wiessner, *supra* note 106, at 85.
[231] *What happened to HMS Erebus and Terror?*, ROYAL MUSEUMS GREENWICH (2021), https://www.rmg.co.uk/stories/topics/what-happened-to-erebus-terror-crew-true-story.
[232] *Id*.
[233] *Id*.
[234] *Id*.
[235] JACOB BRONOWSKI, SCIENCE AND HUMAN VALUES 12 (1956).

information security improvements and new policy considerations. If modern buccaneers wreak havoc on the global landscape, then international cyber policy should draw inspiration from the rule of law recognized by the Outer Space Treaty. The lessons of cooperation are as important as the wisdom gained from future exploration. "An expedition led by Parks Canada [in September 2014] discovered the wreck of *HMS Erebus* in an area that had been identified by the Inuit. Two years later the wreck of *HMS Terror* was located."[236]

[236] PARKS CAN., *supra* note 55.