Title: *Securing the Moon: Exploring the Cybersecurity Dimensions of Sustainably Managing Lunar Resources*

Abstract

Given the increasing number of public and private sector actors active in Lunar exploration, there is a growing need to ensure the sustainable and peaceful use of lunar resources including ice deposits. Such deposits are only available in certain places on the Moon's surface such as Shackleton crater, making it a prime target for adjacent lunar bases. In future geopolitical conflicts this critical infrastructure could become a prime target, as has already been the case with both terrestrial water utilities and space-based infrastructure facing cyber attacks. This paper analyzes the applicable legal regimes governing space resources—focusing on water—and the cybersecurity of related infrastructure. With existing multilateral and multi-stakeholder forums such as the UN Committee for the Peaceful Uses of Outer Space and the UN First Committee struggling to introduce new legally binding rules, space powers are filling governance gaps with non-multilateral norm building efforts such as the Artemis Accords. We investigate the applicability of these efforts to space cybersecurity, and suggest insights drawn from the literature on polycentric governance, the Ostrom Design Principles, and the Institutional Analysis and Development (IAD) Framework. The article concludes with a suggestion for a code of conduct to guide space actors in the peaceful and sustainable development of lunar resources.

Authors: Scott Shackelford, Gustavo Torrens, Eytan Tepper, James Romano

Keywords: cybersecurity, space, Internet governance, common pool resource (CPR)

Table of Contents

Introduction

In March 2024, a 38-year-old software engineer named Andres Freund may have "saved the internet' from one of the most significant cyber attacks in history.[1] His day job at Microsoft involves maintaining open-source database software, but Andres also is one of many volunteers who makes the Internet run, in this case by looking for bugs in the Linux operating system. While flying home to San Francisco from Germany, he discovered a secret backdoor in Linux, the telltale sign for which was that an application that is used to login into remote computers was running slower than normal.[2] Someone, it turns out, had implanted malware in the latest version of Linux, which runs on the vast majority of the world's servers from Fortune 500 companies to community clinics. With it, the attacker could hijack connections and run their own code, potentially controlling systems worldwide at will. Kevin Roose from the *New York Times* described the find with a useful metaphor: "In the cybersecurity world, a database engineer inadvertently finding a backdoor in a core Linux feature is a little like a bakery worker who smells a freshly baked loaf of bread, senses something is off and correctly deduces that someone has tampered with the entire global yeast supply."[3]

There are three salient facts to this tale. First, important components of the Internet governance ecosystem are largely run by volunteers managing open-source software, which can be hijacked by both public and private sector cyber powers with the will and resources to spend. Second, critical infrastructure providers are reliant on these shared networks, which do not respect either sectoral or national borders. Third, such supply chain attacks are growing in

[1] Kevin Roose, *Did One Guy Just Stop a Huge Cyberattack?*, N.Y. TIMES (Apr. 3, 2024), https://www.nytimes.com/2024/04/03/technology/prevent-cyberattack-linux.html.
[2] *Id*.
[3] *Id*.

prominence up by 23% according to one study between 2022 and 2023,[4] threatening water utilities and satellites in orbit alike.

Indeed, there has been a growing chorus of concern regarding the cybersecurity of water utilities. In March 2024, the Biden Administration sent a letter to all U.S. governors warning them of the threat of cyber attacks on their water and wastewater systems.[5] This effort came on the back of a series of Russian state-sponsored cyber attacks targeting water utilities across the nation, laying bare the many networks with inadequate security measures such as outdated software, weak passwords, and infrastructure that should have been 'air-gapped' (physically segregated and incapable of connecting with other computers or networks, including the Internet), or unplugged from the publicly accessible Internet.[6]

Similar issues have arisen in the wake of the war in Ukraine, when Russia launched a cyber attack on the day of its invasion on Viasat, a U.S. commercial space company, to disrupt broadband satellite Internet access to the Ukraine military and government using a wiper worm called "AcidRain."[7] Other cyber attacks have targeted satellites directly, along with ground-based control infrastructure, along with NASA and leading defense contractors.[8] The cybersecurity of the aerospace sector has become a top area of concern for policymakers and practitioners.[9]

---

[4] *Supply Chain Security Breaches Increased in 2023*, SUPPLY CHAIN BRAIN (Dec. 4, 2023), https://www.supplychainbrain.com/articles/38672-supply-chain-breaches-increased-from-2022-to-2023#:~:text=The%20average%20number%20of%20supply,according%20to%20a%20recent%20study..

[5] *See, e.g.*, Raphael Satter, *US Warns Hackers are Carrying out Attacks on Water Systems*, REUTERS (Mar. 20, 2024), https://www.reuters.com/technology/cybersecurity/us-warns-that-hackers-are-carrying-out-disruptive-attacks-water-systems-2024-03-20/.

[6] *See* Sean Lyngaas, *US officials find weak security practices at water plants breached by pro-Russia hackers*, CNN (May 1, 2024), https://www.cnn.com/2024/05/01/politics/water-plants-hackers-weak-security-practices/index.html.

[7] *See* Case Study: Viasat, https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat (last visited May 3, 2024).

[8] *See, e.g.*, Scott J. Shackelford & Scott Russell, *Above the Cloud: Enhancing Cybersecurity in the Aerospace Sector*, 10 FLORIDA INTERNATIONAL UNIVERSITY LAW REVIEW 635 (2015).

[9] *See* Chuck Brooks, *Cyber-Securing Space Systems a Growing Global Concern*, FORBES (Apr. 9, 2024), https://www.forbes.com/sites/chuckbrooks/2024/04/09/cyber-securing-space-systems-a-growing-global-concern/?sh=215794053a9c.

Given the increasing number of public and private sector actors active in lunar exploration, there is a growing need to ensure the sustainable and peaceful in-situ use of lunar resources including ice deposits. Such deposits are only available in certain places on the Moon's surface such as Shackleton crater, making it a prime target for adjacent lunar bases.[10] In-situ resource utilization (ISRU) is using resources found on the Moon (in this context), as opposed to bringing resources from Earth or exporting lunar resources to earth. In future geopolitical conflicts this critical infrastructure could become a prime target, as has already been the case with terrestrial water utilities and space-based facing cyber attacks. While cyber vulnerabilities and threats to critical water and space infrastructures are on the rise, and cyber attacks on such infrastructures are already taking place, the governance responses lag far behind. Multilateral forums struggle to introduce new legally binding rules or even widely accepted norms. This is the case with the UN Committee for the Peaceful Uses of Outer Space on matters of civil space exploration and the UN First Committee, and the Conference on Disarmament on matters of space security. Even the multistakeholder Open-ended Working Group (OEWG) on Reducing Space Threats Through Norms, Rules and Principles of Responsible Behaviours, a less formal group established to facilitate the introduction of shared norms, failed so far to make much progress. As West noted, the OEWG's "discussions on norms, rules, and principles of responsible behaviour ended in September without consensus on a procedural description of the meetings, let alone an outcome report."[11] She further provides insights into the reasons for this

[10] *See* Charles Q. Choi, *Huge Moon Crater's Water Ice Supply Revealed*, Space.com (June 20, 2012), https://www.space.com/16222-moon-water-ice-shackleton-crater.html.
[11] Jessica West, *Getting outer space diplomacy off the treadmill*, PLOUGHSHARES (Dec. 1, 2023), https://www.ploughshares.ca/publications/getting-outer-space-diplomacy-off-the-treadmill.

failure, noting that "[t]he current race to nowhere is fueled by strategic competition among military space powers to ensure the minimal number of restrictions on their own actions."[12]

This paper analyzes the applicable legal regimes governing space resources—focusing on water—and the cybersecurity of related human-made infrastructure. Furthermore, it investigate alternative forums and efforts to introduce rules for space exploration, and their applicability to space cybersecurity, and suggests insights drawn from the literature on polycentric governance and the Institutional Analysis and Development (IAD) Framework. It concludes with a suggestion for a code of conduct to guide space actors in the peaceful and sustainable development of space resources. First, though, we review the nature of the polycentric Internet governance ecosystem and introduce the utility of an Ostromiam approach to analyzing collective action cybersecurity challenges.

1. Introducing the Polycentric Internet Governance Ecosystem

An important element of the application of Ostromian thought to the Internet is the utility of polycentric governance to conceptualize the stakeholders and relationship that make cyberspace possible. As was mentioned in the introduction, some of these same dynamics feed the pervasive insecurity that can lead to compromised critical infrastructure, including in the aerospace and water sectors. In general, the field of polycentric (multi-centered) governance, may be understood as a multi-level, multi-purpose, multi-functional, and multi-sectoral model,[13] which has been championed by scholars including Nobel laureate Professor Elinor Ostrom and Professor Vincent Ostrom. According to Professor Michael McGinnis, "[t]he basic idea [of

[12] *Id*. On the OEWG see also Almudena Azcárate Ortega & Sarah Erickson, *OEWG on Reducing Space Threats: Recap Report*, UNIDIR (2024), https://doi.org/10.37559/WMD/24/Space/01.
[13] Michael D. McGinnis, *An Introduction to IAD and the Language of the Ostrom Workshop: A Simple Guide to a Complex Framework*, 39 POL'Y STUD. J. 163, 171–72 (2011), http://php.indiana.edu/~mcginnis/iad_guide.pdf.

polycentric governance] is that any group . . . facing some collective problem should be able to address that problem in whatever way they best see fit," which could include using existing governance structures or crafting new systems.[14] This model, which came of age thanks to the work of Professor Michael Polanyi in his 1951 book, *The Logic of Liberty*,[15] challenges orthodoxy by recognizing the benefits of self-organization, understood here as networking regulations "at multiple levels," and the extent to which national and private control can coexist with communal management.[16]

The concept of polycentricity is advantageous especially in a field with as complex and cross-border problems and governance and institutions as space exploration. Rather than a single monocentric governmental unit, or minilateral club of nations, a polycentric approach recognizes that diverse organizations working at multiple levels can create different types of policies that can increase levels of cooperation and compliance, enhancing "flexibility across issues and adaptability over time."[17] While this deviates from the initial structure of space governance, which was monocentric, centered around the UN Committee on the Peaceful Uses of Outer Space, it better suits both the current complex geopolitical reality, in which the introduction of top-down regulation is practically impossible, and the nature of the problems which ascend national borders.[18]

---

[14] Michael D. McGinnis, *Costs and Challenges of Polycentric Governance: An Equilibrium Concept and Examples from U.S. Health Care*, Workshop on Self-Governance, Polycentricity, and Development, at 1–2 (Conference on Self-Governance, Polycentricity, and Development, Renmin University, in Beijing, China) (2011), http://php.indiana.edu/~mcginnis/Beijing_core.pdf.
[15] *See* MICHAEL POLANYI, THE LOGIC OF LIBERTY (1951).
[16] *See* Elinor Ostrom, *Polycentric Systems as One Approach for Solving Collective-Action Problems* 1–2 (Ind. Univ. Workshop in Pol. Theory and Pol'y Analysis, Working Paper Series No. 08–6, 2008), http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/4417/W08-6_Ostrom_DLC.pdf.
[17] Robert O. Keohane & David G. Victor, *The Regime Complex for Climate Change*, 9 PERSP. ON POL. 7, 15 (2011).
[18] Eytan Tepper, *The Big Bang of Space Governance: Towards Polycentric Governance of Space Activities*, 54(2) NYU J. OF INT'L L. & POLITICS 485 (2022).

But there are no panaceas, as Elinor Ostrom always maintained. Fikret Berkes, for example, maintains that polycentric networks may be deemed "inefficient,"[19] and are susceptible to institutional fragmentation and gridlock caused by overlapping authority that must still "meet standards of coherence, effectiveness, [and] . . . sustainability."[20] Examples of polycentric systems that have exacerbated, not solved, collective action problems are replete, such as the U.S. healthcare system.[21] Further, the meaning of the term can become opaque given prevailing geopolitical tensions – Russian President Vladimir Putin has used the term to refer to an alternative, non-Western world order featuring multiple power centers.[22] Morever, Paszak suggests that "[t]he principal factor in the Russia-China collaboration is both countries' aim to undermine the US's superiority and creating a polycentric international system, which would guarantee a stronger influence and position for them."[23]

Still, the term remains popular by many who seek to describe the Internet governance ecosystem such as Fadi Chehadé.[24] After all, the Internet does not have a single source of authority, nor a central command and control. Instead, it was erected to begin with, and on purpose, as a polycentric system, the decentralized nature of which helps to ensure its resiliency. It is nearly impossible to take down the Internet because there is no single physical or virtual

---

[19] FIKRET BERKES, COASTS FOR PEOPLE: INTERDISCIPLINARY APPROACHES TO COASTAL AND MARINE RESOURCE MANAGEMENT 129 (2015).
[20] Keohane & Victor, *supra* note 17, at 7 (arguing that "the structural and interest diversity inherent in contemporary world politics tends to generate the formation of a regime complex rather than a comprehensive, integrated regime.").
[21] *See, e.g.*, Michal D. McGinnis, Commons, Institutional Diversity, and Polycentric Governance in US Health Policy, https://mcginnis.pages.iu.edu/McGinnis_Health%20Commons%20chapter%20final%20version.pdf
[22] *See* William Burke-White, *Putin's Election Meddling Didn't Backfire- He Got More Than He Ever Bargained For,* UPENN (Aug. 15, 2017), https://global.upenn.edu/perryworldhouse/news/putins-election-meddling-didnt-backfire-he-got-more-he-ever-bargained.
[23] Paweł Paszak, Xi Jinping's diplomacy: 2013-2020 (Institute of New Europe, September 14, 2020), https://ine.org.pl/en/xi-jinpings-diplomacy-2013-2020-2/.
[24] *See, e.g.*, Nancy Scola, *ICANN Chief: "The Whole World is Watching" the U.S.'s Net Neutrality Debate*, WASH. POST (Oct. 7, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/10/07/internet-operations-chief-snowden-disclosures-make-my-job-easier/.

infrastructure the disruption of which will disrupt the internet. Likewise, there are multiple institutions that adopt standards for the Internet, ICANN being just one of them, and they themselves are multistakeholder institutions. As Joe Nye suggested on cyber governance, "While there is no single regime for the governance of cyberspace, there is a set of loosely coupled norms and institutions that ranks somewhere between an integrated institution that imposes regulation through hierarchical rules, and highly fragmented practices and institutions with no identifiable core and non-existent linkages."[25]

Ostrom and her colleagues conducted groundbreaking research on the effectiveness of polycentric governance systems in addressing collective action challenges related to the management of common pool resources. They questioned the traditional view that rational actors would not cooperate to achieve optimal outcomes in scenarios like the tragedy of the commons, where individuals act in their self-interest to the detriment of the group. She challenged the conventional theory of collective action,[26] which held that rational actors would not cooperate to achieve a socially optimal outcome in a prisoner's dilemma scenario. Contrary to the belief that only centralized, state-imposed regulations could foster cooperation, Ostrom's studies, including those on water resource management in California,[27] irrigation systems in Nepal,[28] and forest

[25] Joseph S. Nye, Jr., The Regime Complex for Managing Global Cyber Activities, CIGI & Chatham House Global Commission on Internet Governance Paper Series, 2014), https://www.cigionline.org/static/documents/gcig_paper_no1.pdf.

[26] The traditional theory of the collective action problem was first articulated in the 1960s by Mancur Olson, an economist and social scientist from the University of Maryland. *See generally* MANCUR OLSON, THE LOGIC OF COLLECTIVE ACTION: PUBLIC GOODS AND THE THEORY OF GROUPS (1965) (providing the first comprehensive explication of the collective action problem). Professor Olson theorized "only a *separate and 'selective' incentive* will stimulate a rational individual in a latent group to act in a group-oriented way." *Id.* at 51. In other words, members of a large group will not act in the group's common interest unless the individual member has some reason to expect personal gain (e.g., economic, social, reputational) from doing so.

[27] *See, e.g.*, Elinor Ostrom, Public Entrepreneurship: A Case Study in Ground Water Basin Management (1965) (unpublished Ph.D. dissertation, Univ. of Calif., Los Angeles), https://dlc.dlib.indiana.edu/dlc/handle/10535/3581.

[28] *See, e.g.*, IMPROVING IRRIGATION GOVERNANCE AND MANAGEMENT IN NEPAL (Ganesh Shivakoti & Elinor Ostrom, eds., 2002).

conservation in Latin America, [29] demonstrated that many people and groups of resource users do cooperate to solve collective action problems.[30] This prompts the question of whether similar cooperative behavior can emerge in the realm of cybersecurity.

2. Ostromian Analysis of Cybersecurity

Is cyberspace a commons amenable to the tools developed at the Ostrom Workshop to better understand the governance of common-pool resources? There is evidence both for and against this question. From a certain perspective, cyberspace can be seen as a system that is open to all. This system traditionally consists of areas that are not regulated, where property rights are not clearly defined. It also faces challenges in enforcing rules and dealing with overuse, as evidenced by issues like spam and Distributed Denial of Service (DDoS) attacks.[31] The open-source "creative commons" initiative, as well as the TCP/IP framework that serves as the foundation of cyberspace, both exemplify the shared characteristics of cyberspace.[32] However, much of the Internet's infrastructure is owned and operated by private firms and, as such, is subject to the jurisdiction of myriad laws and regulations around the world.[33] Witness the U.S. Congressional move to ban TikTok in 2024 as among the latest examples of digital barriers going up in the name of national security, and Internet sovereignty.[34] Thus, cyberspace does not fit

---

[29] *See, e.g.*, Elinor Ostrom & Harini Nagendra, *Insights on Linking Forests, Trees, and People from the Air, on the Ground, and in the Laboratory*, 103 PROC. NAT'L ACAD. SCI. 19224, 19224–25 (2006).
[30] An earlier version of this research was published as, Jamie D. Prenkert & Scott J. Shackelford, *Business, Human Rights, and the Promise of Polycentricity*, 47 VAND. J. OF TRANSNAT'L L. 451, 455–67 (2014).
[31] *See* David Feeny et al., *The Tragedy of the Commons: Twenty-Two Years Later*, 18 HUM. ECOLOGY 1, 4 (1990) (describing the open access system of property rights as one in which access to the resource is available to everyone, free, and unregulated). Feeny also explains that open access systems lead to degradation of the resource due to overuse and an inability to enforce regulations or exclusion mechanisms. *Id.* at 6, 9.
[32] Ronald Deibert, *Cybersecurity: The New Frontier*, *in* FOR. POL'Y ASS'N GREAT DECISIONS 2012, at 45, 56–57 (2012).
[33] *Id.*
[34] *See, e.g.*, Bobby Allyn, *President Biden signs law to ban TikTok nationwide unless it is sold*, NPR (Apr. 24, 2024), https://www.npr.org/2024/04/24/1246663779/biden-ban-tiktok-us.

neatly within the classic definition of a global commons but is perhaps best considered a "shared global infrastructure."[35]

One of Elinor Ostrom's primary arguments was that all over the world there are examples of commons that have been managed well through diverse mechanisms. She argued that often relatively small, self-governing collectives are able to successfully manage common-pool resources (CPRs), from fisheries to forests.[36] This may potentially apply even to the Internet when the network of networks is conceptualized as a regime complex of micro communities and networks. Regime complexes occur, according to Robert Keohane and David Victor, when several different regimes "coexist in the same issue-area without clear hierarchy."[37] Elaborating, Nye has argued that, "[o]n a spectrum of formal institutionalization, a regime complex is intermediate between a single legal instrument at one end and fragmented arrangements at the other."[38] In light of the prevailing dynamics of international politics, "loosely coupled" regime complexes exhibit considerable benefits over singular regimes. This includes certain United Nations' consensus-based multilateral treaties, or even disjointed national policy formulation.[39] Indeed, while regime complexes may seem problematic, they foster significant advantages, as demonstrated by Kal Raustiala and Victor in an article that introduced and defined the concept of

---

[35] *Cybersecurity: Next Steps to Protect Our Critical Infrastructure: Hearing Before the S. Comm. on Commerce, Sci., & Transp.*, 111th Cong. 16 (2010) [hereinafter *Cybersecurity: Next Steps*] (statement of James A. Lewis, Director and Senior Fellow, Technology and Public Policy Program, Center for Strategic and International Studies) (rejecting the idea that cyberspace is a global commons because the resources used in cyberspace are often privately owned by entities located in different jurisdictions). Lewis reinforces this conclusion by highlighting the observations that "private efforts to secure networks will be always be overwhelmed by professional military and criminal action[,]" and that "absent government intervention, security may be unachievable" due in part to the fact that "[c]ybersecurity is a public good that the market has failed to produce in sufficient quantities." *Id.*

[36] *See* Philip J. Weiser, *Internet Governance, Standard Setting, and Self-Regulation*, 28 N. KY. L. REV. 822, 822 (2001).

[37] Robert O. Keohane & David G. Victor, *The Regime Complex for Climate Change,* 9 PERSP. ON POL. 7, 10 (2011).

[38] Joseph S. Nye, Jr., *The Regime Complex for Managing Global Cyber Activities*, GLOBAL COMM'N ON INTERNET GOVERNANCE 7 (Chatham House, 2014), https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.

[39] Keohane & Victor, *supra* note 37, at 10, 15 (discussing the advantages of regime complexes in the climate change context).

regime complexes.[40] Nye noted one such advantage particularly relevant to cyber governance: "[w]hat regime complexes lack in coherence, they make up in flexibility and adaptability. Particularly in a domain with extremely volatile technological change, these characteristics help both states and non-state actors to adjust to uncertainty."[41] This feature of regime complexes multiples the number and type of institutions shaping global commons governance, including cybersecurity.[42]

The nature of the Internet, and cybersecurity, defies monocentric governance. Indeed, Nye suggested:

> It is unlikely that there will be a single overarching regime for cyberspace any time soon . . . The evolution of the present regime complex, which lies halfway between a single coherent legal structure and complete fragmentation of normative structures, is more likely. Different sub-issues are likely to develop at different rates… Some areas, such as crime, in which states have common interests against third-party free riders… And some areas, such as war, may not be susceptible to formal arms control agreements, but may see the evolution of declaratory policy, confidence-building measures and rough rules of the road. Rather than global agreements, like-minded states may act together to avoid destabilizing behaviour, and later try to generalize such behaviour to a broader group of actors through means ranging from formal negotiation to development assistance.[43]

---

[40] Raustiala K, Victor DG. The Regime Complex for Plant Genetic Resources. International Organization. 2004;58(2):277-309.

[41] Joseph S. Nye, Jr., The Regime Complex for Managing Global Cyber Activities, CIGI & Chatham House Global Commission on Internet Governance Paper Series, 2014), https://www.cigionline.org/static/documents/gcig_paper_no1.pdf.

[42] *See* ERIC ALSTON ET AL., INSTITUTIONAL AND ORGANIZATIONAL ANALYSIS: CONCEPTS AND APPLICATIONS 17 (2018), https://extranet.sioe.org/uploads/sioe2016/alston_alston_mueller_nonnenmacher.pdf (arguing that "[a] set of institutions that reduce transaction costs compared to alternative set of institutions is better able to sustain commitments and transactions of greater scale and complexity given the same set of underlying resource endowments.").

[43] Joseph S. Nye, Jr., The Regime Complex for Managing Global Cyber Activities, CIGI & Chatham House Global Commission on Internet Governance Paper Series, 2014), https://www.cigionline.org/static/documents/gcig_paper_no1.pdf.

Regime complexes are, in essence, polycentric systems, and the above review and analysis on the regime complex of cyber governance and its advantages and disadvantages may also be considered a description of the polycentric nature of cyber governance and its advantages.[44]

a. Collective Action Challenge of Cyber Attacks

No individual, organization, or nation is an island in cyberspace, as may be seen by the series of ransomware attacks hitting clinics, hospitals, schools, towns, water utilities, and satellite services around the world. Even though cyber attacks are commonplace today, as headlines in any leading newspaper regularly attest, they are nothing new and in many ways date back to at least the 1980s.[45] What has changed then in the proceeding time is not that cyber attacks are taking place, but rather how quickly they are proliferating in numbers, sophistication, and severity.[46] Cyber assailants are exploiting the reality that no system is completely impervious to breaches. For instance, even the U.S. Central Command, a heavily fortified hub of the U.S. military, was compromised due to a serviceman inadvertently using a flash drive infected with malware. This device was found and inserted into a laptop at a U.S. military base in the Middle East, leading to a "digital beachhead" that spread across a variety of both classified and unclassified networks.[47] Space constraints prohibit a thorough investigation of the myriad issues surrounding cyber war, espionage, crime, terrorism, but suffice it to say that cyber attacks range widely in terms of the vulnerabilities they exploit, their targets, and impacts. One facet that many

---

[44] On the convergence of concepts of regime complexes and polycentric governance see Tepper, *supra* note 18, at 485.
[45] *See* SCOTT J. SHACKELFORD & SCOTT O. BRADNER, FORKS IN THE DIGITAL ROAD: KEY DECISIONS IN THE HISTORY OF THE INTERNET (2024).
[46] *See, e.g.*, Harriet Taylor, *Huge Cybersecurity Threats Coming in 2016*, CNBC (Dec. 28, 2015, 1:17 PM), https://www.cnbc.com/2015/12/28/biggest-cybersecurity-threats-in-2016.html.
[47] Elinor Mills, *Bad Flash Drive Caused Worst U.S. Military Breach*, CNET (Aug. 25, 2010), https://www.cnet.com/news/bad-flash-drive-caused-worst-u-s-military-breach/.

share in common, though, is the degree to which they may be considered collective action challenges.

Collective action "predicts that no one will change behavior . . . unless an external authority imposes enforceable rules that change the incentives faced by those involved."[48] But the classic theory of collective action should not be uncritically assumed. Professor Ostrom has identified two broad reasons why reliance on this conventional theory is unwise: (1) a lack of empirical support that exists because "a surprisingly large number of individuals facing collective action problems do cooperate,"[49] and, (2) the existence of multiple externalities at all scales.[50] In the cybersecurity context, these debates are widespread given calls for more robust cybersecurity controls, including on water utilities and more recently on space-based infrastructure.

b. Illustrative Example: Water Utilities

In the United States, there are sixteen sectors that have been designated by the U.S. Department of Homeland Security (DHS) as critical infrastructure, including water.[51] As of this writing, there is a bipartisan bill pending in Congress that would make the space sector into another critical infrastructure sector, even though it may now currently be thought of as

---

[48] Elinor Ostrom, *A Polycentric Approach for Coping with Climate Change* 5 (World Bank, Pol'y Res. Working Paper No. 5095, 2009), http://www.iadb.org/intal/intalcdi/pe/2009/04268.pdf.
[49] *Id*. at 10 (arguing that there is a lack of empirical support for the free rider aspect of the conventional theory of collective action, and that while some free riding is observed, surprisingly large numbers of communities cooperate and hence mitigate collective action problems).
[50] *See id.* at 9. The traditional theory of the collective action problem was first articulated in the 1960s by Mancur Olsen, an economist and social scientist from the University of Maryland. *See generally* MANCUR OLSON, THE LOGIC OF COLLECTIVE ACTION: PUBLIC GOODS AND THE THEORY OF GROUPS (1965) (providing the first comprehensive explication of the collective action problem). Professor Olson theorized "only a *separate and 'selective' incentive* will stimulate a rational individual in a latent group to act in a group-oriented way." *Id.* at 51.
[51] *See* DHS Critical Infrastructure Sectors, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors (last visited May 17, 2024).

embedded in various existing sectors. As we have seen with cyber attacks on other critical infrastructure sectors including power utilities[52] and healthcare,[53] the increasing number of cyber attacks on water utilities are resulting in urgent warnings from DHS along with a push to issue new regulations from the Environmental Protection Agency (EPA).[54] After successful breaches of water utilities in Florida, and urgent warnings from the White House, though, the regulatory push has faltered with potentially dire implications for water security in the United States. The saga also has important lessons for how we consider securing water resources on the Moon.

3. Governing Lunar Resources

The Soviet Union launched the first artificial Earth satellite, the first human to go to space, first woman, first space walk and several more 'firsts,' but it is the U.S. that is thought to have won the first space race (between the Soviet Union and the U.S.) by being the first (and only to date) to land a human on the Moon. NASA's flagship Artemis Program to establish a self-sustained lunar habitat would likewise be a crown jewel of the current space race between the U.S. and the joint Chinese and Russian space programs with their planned "International Lunar Research Station."[55] NASA's habitat will thus become the most prestigious target for anyone who dislikes U.S. hegemony on earth and its potential dual hegemony on earth and in space. Cyber attacks on space systems have been proven to be a cost effective asymmetric

---

[52] Scott J. Shackelford et al., *From Russia with Love: Understanding the Russian Cyber Threat to U.S. Critical Infrastructure*, 96 NEBRASKA LAW REVIEW 320 (2017).
[53] Scott J. Shackelford et al., *Securing the Internet of Healthcare*, 19 MINNESOTA JOURNAL OF LAW, SCIENCE AND TECHNOLOGY 405 (2018).
[54] *See, e.g.*, Christian Vasquez, *EPA calls off cyber regulations for water sector*, CYBERSCOOP (Oct. 12, 2023), https://cyberscoop.com/epa-calls-off-cyber-regulations-for-water-sector/#:~:text=In%20a%20major%20blow%20to,water%20utilities%20through%20sanitary%20surveys.
[55] *See, e.g.*, Harry Baker, *Russia and China announce plan to build shared nuclear reactor on the moon by 2035, 'without humans'*, SPACE.COM (May 12, 2024), https://www.space.com/russia-china-shared-nuclear-reactor-2035-moon#.

threat.[56] Among the various challenges facing NASA's lunar habitat, cybersecurity is near the top. This section reviews the applicable space governance forums and multilateral agreements before discussing their application to cybersecurity of space systems.

a. The Role of COPUOS

International lawmaking in space began with several U.N. General Assembly Resolutions creating the United Nations Committee on the Peaceful Uses of Outer Space (COPUOS), which became the locus for the advancement of international space law.[57] COPUOS became a permanent U.N. committee in 1959 and has since grown to become one of the largest UN committees boasting 102 Member States,[58] resulting in five international treaties and numerous bilateral and multilateral agreements concerning outer space that were enacted between 1962 and 1979, many of which began life at COPUOS.[59] Progress was made easy in part because the technology for economical space travel had not yet been realized, thereby limiting the number of stakeholders interested in governance.[60] The rapid evolution of space law was also facilitated by precedents that already existed in the form of the law of the sea, air law and the Antarctic Treaty and customary air law.[61] The most important of the five UN space law treaties is the 1967 Outer

---

[56] Eytan Tepper, Scott J. Shackelford, James B. Romano, and Sergei Dmitriachev, The Sixth Warfighting Domain? Governing The Space-Cyber Nexus, 59 Georgia Law Review (forthcoming 2024).
[57] These include G.A. Res. 1348, U.N. GAOR, 13th Sess., Supp. No. 18, U.N. Doc. A/4090 at ¶ 13 (Dec. 13,1958); G.A. Res. 1472, U.N. GAOR, 14th Sess., Supp. No. 16, U.N. Doc. A/4354 at ¶ 13 (Dec. 12, 1959); G.A. Res. 1721, U.N. GAOR, Supp. No. 17, U.N. Doc. A/5100 at ¶16 (Dec. 20, 1961); G.A. Res. 1802, U.N. GAOR, 17th Sess., U.N. Doc. A/RES/1802 at ¶ 17(Dec. 14 1962); G.A. Res. 1962, ¶ 18, U.N. GAOR, Supp. No. 15, U.N. Doc. A/5515, at ¶ 15 (Dec. 13, 1963).
[58] UN Office of Outer Space Affairs, Members of the Committee on the Peaceful Uses of Outer Space, https://www.unoosa.org/oosa/en/members/index.html (retrieved May 27, 2024); BUCK, *supra* note **Error! Bookmark not defined.**, at 146–47.
[59] LOTTA VIIKARI, FROM MANGANESE NODULES TO LUNAR REGOLITH: A COMPARATIVE LEGAL STUDY OF THE UTILIZATION OF NATURAL RESOURCES IN THE DEEP SEABED AND OUTER SPACE 87-89 (2002). *See* BIN CHENG, STUDIES IN INTERNATIONAL SPACE LAW 155–57 (1997). For a more complete analysis of the golden age of space law and the failure of the Moon Treaty, see Scott J. Shackelford, *The Tragedy of the Common Heritage of Mankind*, 28 STAN. ENVTL. L.J. 109, 141–51 (2009).
[60] *See* BUCK, *supra* note **Error! Bookmark not defined.**, at 145.
[61] see also *Id*. at 152.

Space Treaty[62] which may be considered as the 'constitutions of space' and is widely accepted, including on all the space powers.

b. Applicable Legal Regimes

The following sections outline the relevant, primary multilateral treaties pertaining to the governance of outer space including the Moon, noting their relevance to cybersecurity. Today, the outer space legal regime is defined by five principle treaties: the Outer Space Treaty (OST), the Rescue Agreement, the Liability Convention, the Registration Convention, and the Moon Treaty[63] negotiated during the so-called "golden age of space law" extending from the 1960s to the 1980s. We focus here on the OST, and the Moon Treaty. Cybersecurity is not discussed explicitly in these treaties given that they were negotiated before cybersecurity was a leading geopolitical concern, let alone for space systems. The leading treaty framework for multilateral cybercrime mitigation is the Council of Europe's Convention on Cybercrime, in force since July 1, 2004, and commonly known as the "Budapest Convention," which provides an operative but limited vehicle through which to harmonize divergent national cybercrime laws and encourage law enforcement collaboration.[64] Work is underway in the UN a multilateral treaty on cybercrime, in which Russia plays a leading role,[65] and negotiations have significantly advanced with an adoption possibly in sight as of this writing, though "the latest meeting of the Committee members in February 2024 did not conclude with an agreed draft, with countries unable to agree

[62] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, 18 U.S.T. 2410 610 U.N.T.S. 205, 61 I.L.M. 386 (1967).
[63] BUCK, *supra* note **Error! Bookmark not defined.**, at 146.
[64] Convention on Cybercrime, Council of Europe, Mar. 2002, C.E.T.S. 185, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 [hereinafter Cybercrime Convention].
[65] Rishi Iyengar, Robbie Gramer & Anusha Rathi, *Russia Is Commandeering the U.N. Cybercrime Treaty*, FOREIGN POL'Y (Aug. 31, 2023), https://foreignpolicy.com/2023/08/31/united-nations-russia-china-cybercrime-treaty/.

on wording that would balance human rights safeguards with security concerns."[66] Such an agreement, if made, would help to catalyze the positive efforts made on cyber norms with a codified treaty framework.

i. The Outer Space Treaty

The first and most important of the five UN space law treaties is the 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies,[67] known as the Outer Space Treaty. It is a constitution-like treaty providing the basic norms and rules for human space exploration, and is widely accepted, having been ratified by 112 countries and signed (but not ratified) by another 23 countries. The other four UN space law treaties are largely elaborations of norms and provisions of this treaty. The analysis of the regulation of space activities under this treaty,[68] including Article IV(1), prohibits the placement "in orbit around the Earth [of] any objects carrying nuclear weapons or any other kinds of weapons of mass destruction," but does not prohibit the placement of conventional weapons in orbit and may be considered to allow[69] for the nonaggressive military use of orbital space. In contrast, OST article IV(2) preserves the Moon and other celestial bodies "exclusively for peaceful purposes"[70] the "establishment of military bases, installations and fortifications, the testing of any type of weapons and the conduct of

[66] UN, Global Cybercrime Treaty: A delicate balance between security and human rights (February 25, 2024), https://news.un.org/en/interview/2024/02/1146772.
[67] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, 18 U.S.T. 2410 610 U.N.T.S. 205, 61 I.L.M. 386 (1967).
[68] Armel Kerrest, *Outer Space as International Space: Lessons from Antarctica*, SPACE DIPLOMACY 133, 136 (2011), http://www.atsummit50.org/media/book-18.pdf.
[69] *See* OST, art. IV. *Cf.* Antarctic Treaty art. I(1)., Dec. 1, 1959, 12 U.S.T. 794, 402 U.N.T.S. 72 (defining "peaceful purposes" in Antarctica as banning "any measures of a military nature . . . .").

military maneuvers on celestial bodies."[71] There is therefore a clear distinction between Earth orbit, in which non-peaceful uses are allowed, including the placement of conventional weapons, and the Moon which is reserved *exclusively* for peaceful uses and on which no weapons may be placed.[72]

Articles IX and III of the OST also come into play. Article III makes it explicit that international law, and by that the laws of war, apply to space activities. Article IX addresses the "harmful contamination" of outer space, but it falls short of requiring action to mitigate space.[73] Moreover, Article IX provides that states should conduct their space activities "with due regard to the corresponding interests of all other States Parties to the Treaty."[74] The meaning of "due regard" is not unlike the debate over cybersecurity due diligence.[75]

The Mc*Gill Manual on International Law Applicable to Military Activities in Outer Space* (MILAMOS)[76] suggests that "Cyber activities that constitute space activities, including military space activities, are governed by international space law, as well as the applicable rules of general international law."[77] While the first section of OST Article IV suggests a more permissible regime for military uses of Earth orbit, and therefore potentially also cyber attacks, the second part of the Article seems to preclude cyberattacks on the lunar surface. Moreover, the due regard principle may be interpreted to prohibit any cyber attacks on space assets, as these may be considered space activities that must be conducted with due regard to the interests of

---

[71] *Id*.
[72] *See* Kerrest, *supra* note 125, at 136–37.
[73] OST, art. IX.
[74] *See* Ram Jakhu, *Towards Long-term Sustainability of Space Activities: Overcoming the Challenges of Space Debris*, IAASS LEGAL & REGULATORY COMM., at 10 (Feb. 15, 2011), http://www.oosa.unvienna.org/pdf/pres/stsc2011/tech-35.pdf.
[75] *See, e.g.*, Scott J. Shackelford, *Human Rights and Cybersecurity Due Diligence: A Comparative Study*, 50 MICHIGAN J. OF L. REFORM 859 (2017).
[76] MANUAL ON INTERNATIONAL LAW APPLICABLE TO MILITARY USES OF OUTER SPACE, https://www.mcgill.ca/milamos/.
[77] MILAMOS Rule 112 – Cyber Activities that Constitute Space Activities.

other countries, a standard that cannot sustain cyber attacks on critical infrastructure such as water facilities.

ii. The Moon Agreement

The Agreement Governing the Activities of States on the Moon and Other Celestial Bodies,[78] colloquially known as the Moon Agreement, is the last of the five UN space law treaties. It is intended to elaborate on the Outer Space Treaty in providing a framework for the exploitation of space resources. The Moon Agreement does not per se prohibit the commercial utilization[79] but it does provide in Article 11 that the "Moon and its natural resources are the common heritage of mankind."[80] The common heritage of mankind concept is commonly thought of as providing for a communal property regime amenable to Ostromian analysis but its application to space resources is the main reason for the failure of the Moon Agreement; only 17 states have ratified the Agreement (after Saudi Arabia withdrew in 2023) and four signed but not ratified. None of the ratifying states boast human space exploration programs or are otherwise one of the leading spacefaring nations.[81] Lee even suggests that the Moon Treaty may conflict with Outer Space Treaty provisions depending on the interpretation of the common heritage of mankind concept.[82] Article 11 of the Moon Agreement establishes equitable benefit sharing for resources found on the Moon, though the international regime envisioned in the Moon

[78] Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, 1363 U.N.T.S. 22, 18 I.L.M. 1434 (1979).
[79] *See* Moon Treaty, art. XI (laying out the purpose of the proposed future international regime for the exploitation of lunar resources).
[80] *Id*. at art. XI(1, 5).
[81] The Moon Agreement was ratified by: Armenia, Australia, Austria, Belgium, Chile, Kazakhstan, Kuwait, Lebanon, Mexico, Morocco, Netherlands, Pakistan, Peru, Philippines, Turkey, Uruguay, and Venezuela, and signed, but not ratified, by France, Guatemala, India, Romania.
[82] *See* RICKY J. LEE, LAW AND REGULATION OF COMMERCIAL MINING OF MINERALS IN OUTER SPACE 160–62, 261 (2012) (laying out some of the various possible interpretations of ambiguous space law treaty provisions relating to the commercial use of space).

Agreement has not yet been created,[83] and may never will, considering the failure of the Agreement to date and challenges experienced by the somewhat analogous International Seabed Authority discussed in Part V. This means that the introduction of alternative norms and policies around in-situ resource utilization will be of paramount importance in crafting a sustainable regime for mining lunar ice deposits.

iii. In-Situ Resource Utilization

In-Situ Resource Utilization (ISRU) according to NASA is the "harnessing of local natural resources at mission destinations, instead of taking all needed supplies from Earth, to enhance than capabilities of human exploration."[84] It also differs from the extraction of space resources for the purpose of bringing them to Earth. Other space agencies such as the European Space Agency (ESA)[85] and the Japan Aerospace Exploration Agency (JAXA) are both exploring ISRU technologies to sustain future space exploration missions.[86] The China National Space Agency (CNSA) is likewise exploring in-situ resource utilization on the Moon in particular with its Chang'E-8 (CE-8) mission, which is scheduled to be launched in 2028.[87] The ongoing

[83] Moon Treaty, art. 11(7)(d); U.N. Convention on the Law of the Sea arts. 117, 137, ¶ 2, *opened for signature* Dec. 10, 1982, 1833 U.N.T.S. 397 (entered into force Nov. 16, 1994).
[84] *In-Situ Resource Utilization (ISRU)*, NASA, https://www.nasa.gov/mission/in-situ-resource-utilization-isru/.
[85] *In-Situ Resource Utilisation*, ESA https://www.esa.int/Science_Exploration/Human_and_Robotic_Exploration/Exploration/In-Situ_Resource_Utilisation; *First 'in situ' Composition Measurements Made in Titan's Atmosphere*, ESA (Nov. 30, 2005), https://www.esa.int/Science_Exploration/Space_Science/Results_from_Mars_Express_and_Huygens/First_in_situ_composition_measurements_made_in_Titan_s_atmosphere.
[86] *Cooperation with JGC Corporation on the Concept of a Lunar ISRU Plant has Started*, JAXA (Jun. 6, 2021), https://humans-in-space.jaxa.jp/en/news/detail/001529.html.
[87] *Announcement of Opportunities for International Cooperation of the Chang'E-8 Mission*, CNSA 1 (Dec. 2, 2023); Chang'e Ba Hao Renwu Guoji Hezuo Jiyu Gonggao (嫦娥八号任务国际合作机遇公告) [Chang'e 8 Mission International Cooperation Announcement] ,Guojia Hangtian Ju (国家航天局) [China National Space Administration (CNSA)] 1-2, (Dec. 2, 2023).

national interests in pursuing ISRU viability and technologies is not unwarranted, as the use of such resources could significantly aid ongoing space exploration and human space habitation.

ISRU presents several benefits for the future of space exploration, with water being the primary resource for the sustainment of future missions. NASA's flagship Artemis Program[88] aims to establish a self-sustained habitat on the Moon, and the use of local resources is essential for a self-sustaining habitat. Interest in Lunar ISRU (L-ISRU) vary in complexity but are essentially focused on the extraction of oxygen and hydrogen from water. These methods in order of complexity are: "(i) physical extraction of indigenous water ice directly; (ii) thermal processing of lunar volatiles to extract hydrogen; (iii) use of regolith processed into civil engineering structures, and (iv) thermochemical or electrochemical processing of lunar minerals to extract oxygen."[89] Water ice is indeed present in permanently shadowed craters on the moon and in polar regions.[90] The lunar regolith, a layer of fine-grained particles on the moon's surface may also be a source for water, oxygen, and hydrogen,[91] in addition to use for civil engineering structures as previously mentioned. The Chandrayaan-1, Deep Impact and Cassini missions demonstrated the presence of hydroxyl (OH) and water (H_2O) on the lunar surface in non-shadowed regions; however, the highest retention of these molecules occurs in the colder polar regions.[92] Similar methods of employing ISRU mining technologies for the production of oxygen, buffer gas (used to dilute oxygen for breathing), and water have likewise been posited for use in Mars missions.[93]

---

[88] Artemis, NASA, https://www.nasa.gov/specials/artemis/index.html (last visited May 29, 2024).
[89] Alex Ellery, *Sustainable in-situ Resource Utilization on the Moon*, 184 PLANETARY & SPACE SCI. 1, 2 (2020).
[90] Mahesh Anand et al., *A Brief Review of Chemical and Mineralogical Resources on the Moon and Likely Initial in situ Resource Utilization (ISRU) Applications*, 74 PLANETARY & SPACE SCI. 42, 43-44 (2012).
[91] *Id.* at 43, 44.
[92] *Id.* at 44.
[93] Sridhar, K.R. et al., *In-situ Resource Utilization Technologies for Mars life Support Systems*.

Water, and the elements from which it is derived, have the potential to sustain future space exploration by supporting human life support systems, providing propellants for future missions, and allowing humans to explore further into space. In-situ water resources on the lunar surface can be used to support life support systems and features prominently in ESA's 2019 resource strategy report.[94] The 'Validation of Lunar Water Extraction and Purification Technologies for In-Situ Propellant and Consumables Production' (LUWEX) project from the German Aerospace Center is focused on this very topic, researching methods of water extraction and purification on the lunar surface.[95] Water is a necessary resource for life support and fuel, particularly for NASA's aspirational Artemis Program which will establish "the first long-term human presence on the lunar surface."[96] NASA's Polar Resources Ice Mining Experiment-1 (PRIME-1), which will utilize the Regolith and Ice Drill for Exploring New Terrain (TRIDENT) and the Mass Spectrometer observing lunar operations (MSolo), will also be deployed for the purpose of extracting water for life support and fuel.[97]

With the emergence of ISRU technologies for the extraction of water comes the inevitable question of resource allocation. However, this question does not yet have a universal consensus, as there are conflicting interpretations of the Outer Space Treaty on this issue and the more elaborated Moon Agreement failed to gather wide support. In the absence of a multilateral arrangement, alternative forums and instruments are gaining importance. This includes the

---

[94] *ESA Space Resources Strategy*, ESA (2019), https://sci.esa.int/documents/34161/35992/1567260390250-ESA_Space_Resources_Strategy.pdf.
[95] Lunar Water for Drinking and Rocket Propellant, Deutches Zentrum für Luft- und Raumfahrt [German Aerospace Center] (Apr. 2023).
[96] Emily Furfaro, *How Will We Extract Water on the Moon? We Asked a NASA Technologist: Episode 47*, NASA (Aug. 16, 2023), https://www.nasa.gov/general/how-will-we-extract-water-on-the-moon-we-asked-a-nasa-technologist-episode-47/.
[97] *Id.*

Hague International Space Resources Governance Working Group,[98] an informal, multistakeholder forum that introduced the non-legally binding Building Blocks for the Development of an International Framework on Space Resource Activities.[99] Nations are also helping to fill such governance gaps, most notably the U.S. Commercial Space Launch Competitiveness Act of 2015,[100] which rules on space resource exploitation served as a model for similar laws adopted by Luxembourg and the UAE. The most important of these alternative instruments are the Artemis Accords, to which 39 countries have already joined, as of May 2024.[101] The Artemis Accords were introduced by the United States in 2020 and to date only U.S.-allied countries have joined them. Russia and China are the most notable countries that did not join the Accords, as they consider too U.S.-centric.[102]

c. Artemis Accords

NASA took a leading role in crafting a non-binding set of norms and principles organized as the "Artemis Accords"[103] and "[g]rounded" in the [Outer Space Treaty] itself to help guide human space exploration in its return to the Moon and missions beyond.[104] Launched in 2020, the effort has 40 signatory nations as of May 2024 including a range of space powers and NASA

---

[98] The Hague International Space Resources Governance Working Group, https://www.universiteitleiden.nl/en/law/institute-of-public-law/institute-of-air-space-law/the-hague-space-resources-governance-working-group (last visited May 29, 2024).
[99] *Building Blocks for the Development of an International Framework on Space Resource Activities*, HAGUE INT'L SPACE RESOURCES GOVERNANCE WORKING GROUP (2019), https://www.universiteitleiden.nl/binaries/content/assets/rechtsgeleerdheid/instituut-voor-publiekrecht/lucht--en-ruimterecht/space-resources/bb-thissrwg--cover.pdf.
[100] U.S. Commercial Space Launch Competitiveness Act, Pub. L. No. 114-90, 129 Stat. 704 (2015).
[101] *Artemis Accords*, U.S. DEP'T ST., https://www.state.gov/artemis-accords/#:~:text=Artemis%20Accords%20signatories%20as%20of,the%20Republic%20of%20Korea%2C%20Romania.
[102] *See* Christopher Newman, *Artemis Accords: why many countries are refusing to sign Moon exploration agreement*, CONVERSATION (Oct. 19, 2020), https://theconversation.com/artemis-accords-why-many-countries-are-refusing-to-sign-moon-exploration-agreement-148134.
[103] Artemis Accords, *supra* note 101.
[104] Artemis Accords, U.S. Dep't St., https://www.state.gov/artemis-accords/ (last visited May 23, 2024).

partners such as Australia, Canada, Italy, Japan, Luxembourg, the UAE, and the United Kingdom.[105]

The Artemis Accords "establish a practical set of principles to guide space exploration cooperation among nations participating in the agency's 21st century lunar exploration plans."[106] Section 10 of the Artemis Accords is dedicated to space resources and their utilization. The four sub-sections of Section 10 provide that: (1) "the utilization of space resources can benefit humankind by providing critical support for safe and sustainable operations," (2) "the extraction and utilization of space resources . . . should be executed in a manner that complies with the Outer Space Treaty and in support of safe and sustainable space activities . . . [and] does not inherently constitute national appropriation under Article II of the Outer Space Treaty," (3) the Signatories commit to inform the UN, the public and the international scientific community of their space resource extraction activities, and (4) "[t]he Signatories intend to use their experience under the Accords to contribute to multilateral efforts to further develop international practices and rules applicable to the extraction and utilization of space resources, including through ongoing efforts at the COPUOS."[107] The Accords also call for interoperability in the name of redundancy, safety, and importantly the deconfliction of activities.[108] This latter category could have special relevance for the avoidance of cyber attacks on critical space infrastructure, including water mining operations, which would be further reinforced by the eleven principles of responsible state behavior in cyberspace agreed to by the G20, and more recently the UN, which

[105] *Id*.
[106] From the original NASA press release https://www.nasa.gov/news-release/nasa-international-partners-advance-cooperation-with-first-signings-of-artemis-accords/.
[107] *Id*.
[108] Artemis Accords, *supra* note 104.

include prohibitions on launching cyber attacks.[109] Yet such efforts are at best a beginning since they lack enforcement measures, not to mention that the Artemis Accords so far have not attracted support from other leading space powers including Russia and China that are planning their own lunar base. As such, governance gaps and great power competition are making further progress challenging, hence the important role that Ostromian analysis can play in charting a path ahead.

4. Applying Insights from the IAD Framework to Space Cybersecurity

Economically, technically, and even legally, cyberspace and outer space are becoming ever more intertwined. NASA's Jet Propulsion Laboratory was under sustained cyber attack for years, according to Congressional testimony,[110] prompting an investigation by the NASA Office of Inspector General.[111] In the same vein, a governmental audit revealed that the Federal Aviation Administration was susceptible to cyber threats due to the use of obsolete equipment in their air traffic control facilities.[112] Indeed, entities from defense contractors such as Lockheed Martin to SpaceX have been the focus of attacks, and occasionally infiltrated, leading to the compromise of trade secrets that bear significant implications for both economic competitiveness and national security.[113] Satellites have already been hacked not only by nations, but by non-state groups such

---

[109] *See, e.g.*, Advancing the framework of responsible State behaviour in cyberspace through the Harms Methodology, Cyber Peace Inst. (Mar. 21, 2024), https://cyberpeaceinstitute.org/news/advancing-responsible-state-behaviour-in-cyberspace-harms-methodology/.
[110] Marc Boucher, *NASA Has Been Under Heavy Cyber Attack*, NASA WATCH (Mar. 5, 2013), http://nasawatch.com/archives/2013/03/nasa-has-been-u.html; Emil Protalinski, *NASA: Hackers Had 'Full Functional Control,'* ZDNET (Mar. 2, 2012), http://www.zdnet.com/blog/security/nasa-hackers-had-full-functional-control/10443.
[111] *See* NASA OFF. INSPECTOR GEN., *supra* note **ERROR! BOOKMARK NOT DEFINED.**. This research was first published as Shackelford & Russell, *supra* note **Error! Bookmark not defined.**.
[112] Lolita C. Baldor, *Cyber Security Still Issue for FAA*, BOSTON GLOBE (Aug. 13, 2010), http:// www.boston.com/news/nation/washington/articles/2010/08/13/cyber_security_still_ issue_for_faa.
[113] *See, e.g.*, Siobhan Gorman, August Cole, & Yochi Dreazen, *Computer Spies Breach Fighter-Jet Project*, WALL ST. J., Apr. 21, 2009, http://online.wsj.com/article/SB124027491029837401.html; Andrea Tse, *See What Elon*

as the Liberation Tigers of Tamil Eelam from Sri Lanka.[114] In this highly networked and visible arena, the cyber threat to the aerospace sector has already garnered attention from the U.S. government, and the international community.[115]

The international experts who drafted the *Tallinn Manual 2.0* noted "the importance of outer space with regard to cyber activities ranging from civilian communications and navigation to military operations."[116] When contemplating the interconnectedness of these realms, the authors observed that resources based in space are not only targets for cyber attackers, but also infrastructure that could be manipulated to initiate cyber attacks. These attacks could retrieve, modify, meddle with, or disrupt data, potentially leading to scenarios such as taking control of "a satellite, or its payload."[117] To help guard against such an outcome, Rule 58 maintains that "[c]yber operations on the moon and other celestial bodies may be conducted only for peaceful purposes . . . [while] cyber operations in outer space are subject to the international law limitations on the use of force."[118] Cyber attacks, then, which constitute an unlawful threat or use of force in violation of the U.N. Charter are barred,[119] while the authors contend that cyber operations conducted for the purposes of "establishing communications, research, or observation

---

Musk's Right Hand Man Has to Say About Cyber Hackers, ST. (Feb. 25, 2014), http://www.thestreet.com/story/12441320/1/see-what-elon-musks-right-hand-man-has-to-say-about-cyber-hackers.html.

[114] Meredith Rutland Bauer, *Is the US Military Prepared for Cyberattacks on Satellites*?, FIFTH DOMAIN (Nov. 14, 2017), https://www.fifthdomain.com/dod/2017/11/14/is-the-us-military-prepared-for-cyberattacks-on-satellites/.

[115] Ruwantissa Abeyratne, *Cyberterrorism: The Next Great Threat to Aviation,* 24 AIR & SPACE L. 4, 4–6 (2011); Protocol on the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, 24 Feb. 24, 1988, U.N. Stat. 1990:440; Convention for Suppression of Unlawful Acts Against the Safety of Civil Aviation (Sabotage), entered into force Jan. 26, 1973, 24 U.S.T. 564, T.I.A.S. No. 7570, 974 U.N.T.S. 178.

[116] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 270 (Michael N. Schmitt ed., 2017). For purposes of full disclosure, it is worth noting that the author was one of the reviewers for *Tallinn Manual 2.0*.

[117] *Id*. at 270–71 (describing the differences between "space-enabled cyber operations and cyber-enabled space operations").

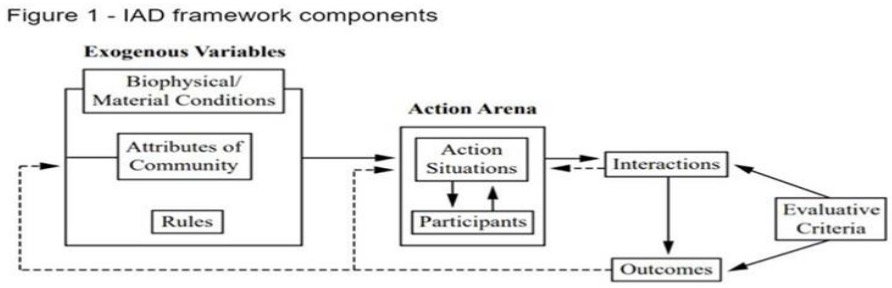
[118] *Id*. at 273. Rule 59(b) builds from this foundation, noting: "A state must conduct its cyber operations involving outer space with due regard for the need to avoid interference with the peaceful space activities of other States." *Id*. at 277. Astronauts are also protected by cyber activities given their status as "envoys of mankind." *Id*. at 279.

[119] For more on this topic, see Chapter 6 in SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE (2014).

facilities on the moon or other celestial bodies . . . are lawful."[120] The bounds of "peaceful use," though, is contested, but does not equate to "non-military" given the long history of the military use of space.[121]

How can the methodological tools developed at the Ostrom Workshop help to better understand these disputes over resources and rules-in-use? The IAD Framework can prove helpful since it can improve our "understanding of information and information flows under alternative institutional arrangements; (b) diagnose problems (or dilemmas) in existing institutional arrangements; and (c) in select cases predict outcomes under alternative institutional arrangements."[122] Indeed, Professor Ostrom believed that the IAD Framework had wide application, including "to microeconomic theory, game theory, transaction cost theory, social cost theory, public choice, and constitutional and covenantal theory, along with theories of public goods and common-pool resources."[123]

Figure 1: IAD Framework[124]



[120] TALLINN MANUAL 2.0, *supra* note 116, at 273, 274 (noting that "it might be permissible to sue cyber force in self-defence against a satellite that is being used to facilitate armed attacks (Rule 71) occurring on the earth.").
[121] *Id*. at 275.
[122] *Id*. at 46.
[123] *Id*. at 49.
[124] Adopted from Ostrom, E., Gardner, R., Walker, J. (1994). Rules, Games, and Common-pool Resources.

Digging in to the IAD Framework, there are an array of characteristics to consider including "facilities through which information is accessed" such as the Internet itself, as well as "artifacts . . . including . . . computer files" and the "ideas themselves."[125] The "artifacts" category is especially relevant in cybersecurity discussions given that it includes trade secrets protections, which are closer to a pure private good than a public good, and are also the currency of global cybercrime.[126] Internet governance institutions (or "facilities" in this vernacular) can also control the rate at which ideas are diffused, including on the Moon given NASA's recent efforts to craft common understandings around time zones and even a lunar 5G network.[127]

The next box on the left side of the IAD Framework as seen in Figure 1 titled, "Attributes of the Community," refers to the network of users making use of the given resource.[128] In this scenario, adjacent lunar bases would potentially share mining rights over valuable ice deposits. Next, the rules-in-use component of the IAD Framework comprises both community norms along with formal legal rules.[129] One of the driving questions in this area is identifying the appropriate governance level at which to formalize norms into rules, e.g., whether that is at a constitutional level, collective-choice level, etc.[130] The research task in this variable, according to Dan Cole, "in applying the IAD framework, is to determine, and diagnose perceived problems with, the rules-in-use that govern day-to-day ('operational-level') interactions in the action situations under study."[131] That is easier said than done in the cybersecurity context given the wide range of industry norms, standards, state-level laws, sector-specific federal laws, and

[125] *Id*. at 53.
[126] For more on this topic, see Scott J. Shackelford et al., *Using BITs to Protect Bytes: Promoting Cyber Peace and Safeguarding Trade Secrets through Bilateral Investment Treaties*, 52 AM. BUS. L.J. 1 (2015).
[127] *See* Sue Nelson, Talking on the Moon: The quest to establish a lunar mobile phone network, BBC (Mar. 10, 2024), https://www.bbc.com/future/article/20240308-talking-on-the-moon-the-quest-to-establish-lunar-wifi.
[128] Cole, *supra* note **Error! Bookmark not defined.**, at 55.
[129] *Id*.
[130] *Id*.
[131] *Id*.

international laws regulating everything from satellite communications to protecting water facilities.

The "action arena" is just that, the place where decisions are made, where "collective action succeeds or fails."[132] Such arenas exist at three levels within the IAD Framework—constitutional, collective-choice, and operational.[133] Decisions made at each of these governance levels, in turn, impact a range of rules and community attributes, which is an important feature of the Framework that makes it "uniquely compatible with multiple theories and models, including: neoclassical theory, game theory, public choice theory, and behavioral economics, with the exception of (usually deterministic) models of irrational behavior."[134] Examples of decisionmakers in each arena in the space cybersecurity context include, at the constitutional level, judges deciding the bounds of "reasonable care" and "due diligence,"[135] federal and state policymakers at the collective-choice (e.g., policy) level such as regarding satellite security and, at the operational level, e.g., firms, and everyone else.[136]

The final IAD Framework box is, according to Cole, "the most neglected and underdeveloped" of the Framework.[137] Ostrom, for example, offered the following "evaluative criteria" in considering how best to populate it, including: "(1) economic efficiency; (2) fiscal equivalence; (3) redistributional equity; (4) accountability; (5) conformance to values of local actors; and (6) sustainability."[138] In this context, the considerations here could be crafting a set of

[132] Cole, *supra* note **Error! Bookmark not defined.**, at 59.
[133] *Id*.
[134] *Id*.
[135] *See* Shackelford et al., *supra* note **Error! Bookmark not defined.**.
[136] Cole, *supra* note **Error! Bookmark not defined.**, at 60.
[137] Dan H. Cole, *Learning from Lin: Lessons and Cautions from the Natural Commons for the Knowledge Commons, in* GOVERNING KNOWLEDGE COMMONS 45, 62 (Brett M. Frischmann, Michael J. Madison, & Katherine J. Strandburg eds., 2014).
[138] *Id*.

norms in nested community governance structures to sustainably and peacefully managed shared resources, such as lunar ice discussed in the next section.

5. Proposing a Sustainable Lunar Mining Code of Conduct for CPRs

Efforts to craft sustainable codes of conduct governing the mining of various global CPRs have been fraught. Witness the controversies surrounding such efforts in the deep seabed mining context spearheaded by the International Seabed Authority (ISA). There, the ISA has been mired by corruption allegations even as the science that is essential to better understand the ecosystems that mining would doubtless disrupt in the deep seabed remains nascent.[139]

Although there are not vulnerable natural ecosystems on the Moon in the way that they exist in the deep seabed, there are nevertheless competing priorities including the protection of heritage exploration sites and the fact that the most valuable lunar real estate is actually quite limited. Thus, absent cooperation first movers will have a significant advantage, leaving out most non-space faring states in the process. To help avoid that outcome and ensure that the benefits are shared more widely across humanity, there are different options available that would share the benefits of lunar resources while ensuring that their exploitation is done sustainably, and securely.

To this end, we propose the following additional protocol to the Artemis Accords focusing on instilling cybersecurity due diligence in the utilization of lunar resources. Just as the Artic Council found early success by focusing on low-hanging fruit issues such as search and

[139] *See, e.g.*, Karen McVeigh, *Seabed regulator accused of deciding deep sea's future 'behind closed doors*', GUARDIAN (Apr. 1, 2022), https://www.theguardian.com/environment/2022/apr/01/worlds-seabed-regulator-accused-of-reckless-failings-over-deep-sea-mining.

rescue agreements, we propose that similar momentum could begin by recognizing shared interests and safety and deconfliction.[140]

While there is not a single, definitive definition of cybersecurity due diligence, much like cyber peace, for the context of this study, it is viewed as a responsibility under international law that requires a specific "form of conduct" from a nation to align with its international law obligations towards other states..[141] Although public international law primarily focuses on inter-state relations, the obligation of cyber due diligence also involves domestic entities and laws. In order to meet its responsibilities under international law, a state may need to exert control over Information and Communication Technology (ICT) and crucial information infrastructure within its territory and jurisdiction. However, this is a challenging and intricate task due to issues related to jurisdiction, attribution, unclear norms, and the widespread ownership of critical infrastructure by the private sector, a trend that began with the liberalization and privatization of public infrastructure in the late 1970s.[142] To further their cybersecurity due diligence mandates, nations should, among other steps, establish domestic policy regimes including laws, frameworks (such as NIST), and initiatives that incentivize or even cajole private actors under their jurisdiction to behave in accordance with prevailing legal obligations.[143] Even the experts who crafted the

[140] For more on this topic, see Scott J. Shackelford, GOVERNING NEW FRONTIERS IN THE INFORMATION AGE: TOWARD CYBER PEACE (2020).
[141] Nicholas Tsagourias, *Economic Cyber Espionage and Due Diligence*, SYRACUSE UNIV. CONTROLLING ECONOMIC CYBER ESPIONAGE' WORKSHOP (June 18–19, 2015), http://insct.syr.edu/wp-content/uploads/2015/06/Tsagourias_Due_Diligence.pdf.
[142] *See, e.g.*, J.P. Singh, *The Institutional Environment and Effects of Telecommunication Privatization and Market Liberalization in Asia*, 24 TELECOMM. POL'Y 885, 886 (2000).
[143] For a comparative analysis of how a subset of nations—in particular the United States, China, and Germany—are defining cybersecurity due diligence, see Scott J. Shackelford, Scott Russell, & Andreas Kuehn, *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*, 17 CHI. J. INT'L L. 1 (2016).

Tallinn Manual, for example, all agreed that the rule exists, but could not reach a consensus on its scope and meaning.[144]

With that context in mind, what follows is a tentative proposal for such a Lunar Mining Code of Conduct, building from insights gleaned by applying the IAD Framework:

Lunar Mining Code of Conduct

Preamble

Recognizing the importance of sustainable and responsible lunar mining activities, this Code of Conduct is established in accordance with the principles of the Artemis Accords, international space law including the Outer Space Treaty, and prioritizes safety and cybersecurity.

Principles

- **Peaceful Purposes**: All lunar mining activities must be conducted for peaceful purposes.
- **Transparency**: Entities must publicly describe their lunar mining policies and plans.
- **Interoperability**: To ensure effective cooperation, all systems should be designed to be compatible with each other.
- **Safety**: The safety of human life and the protection of the lunar environment must be a priority.
- **Cybersecurity**: Entities must develop and implement robust cybersecurity measures to protect space systems from cyber threats.
- **Community Participation**: Stakeholders are encouraged to participate in the governance and management of lunar resources.

Guidelines

- **Sustainable Extraction**: Lunar resources should be utilized in a manner that does not exhaust them or cause unnecessary harm to the lunar environment.
- **Risk-Based, Cybersecurity-Informed Engineering**: Space systems, including those used for lunar mining, should be developed and operated using risk-based, cybersecurity-informed engineering such as secure-by-design.
- **Cybersecurity Incident Response Plans**: Entities should proactively develop and implement cybersecurity incident response plans for their space systems should a breach occur.
- **Collaboration**: Stakeholders should collaborate across sectors and borders to promote the development of best practices and share threat, warning, and incident information within the space industry.

[144] *See* TALLINN MANUAL 2.0, *supra* note **Error! Bookmark not defined.**, at 30–33.

- **Institutional Arrangements**: Diverse institutional arrangements should be encouraged building from subsidiarity that facilitate the sustainable management of lunar resources.

Implementation

Entities are encouraged to incorporate these principles and guidelines into their national regulatory frameworks for space activities. International cooperation is encouraged to promote and enhance adherence to this Lunar Mining Code of Conduct.[145]

Of course, this early draft of such an agreement leaves much to be desired. For example, it does not specify the types of institutional or common property arrangements that should be used in practice, but rather sets up a mechanism by which the parties could begin to work this out for themselves. Leading space powers could continue to help fill this void through further national, bilateral, minilateral, and multilateral partnerships, as can the private sector through multi-stakeholder dialogues and public-private partnerships in keeping with polycentric theory.

Conclusion

This paper has argued that cybersecurity concerns span critical infrastructure sectors, including space and water, and that new frontiers such as the Moon are bringing both together in a manner that lays bare the governance gaps and ambiguities underlying both space and cybersecurity governance. By applying insights from Ostromian literatures, it is possible to begin to address, and fill in, these gaps by learning from the failures of other global CPR regimes and leveraging polycentric efforts to craft multi-stakeholder compromises.

[145] Drawn from: Artemis Accords, NASA (2020); Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205; Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, Dec. 18, 1979, 1363 U.N.T.S. 3; Convention on International Liability for Damage Caused by Space Objects, Mar. 29, 1972, 961 U.N.T.S. 187.