POLYCENTRIC GOVERNANCE OF COMPLEX SYSTEMS: BUILDING RESILIENCY INTO TAIWAN'S SPACE-BASED INFRASTRUCTURE

by

Simon Sun & Eytan Tepper*

SYNOPSIS

ABSTRACT 344
RÉSUMÉ 344
KEYWORDS 344
I. INTRODUCTION 345
II. TAIWAN'S INTERNET INFRASTRUCTURE: CHALLENGES AND RESPONSES 345
A. CHALLENGES 345
B. RESPONSES 349
III. COMPLEX SYSTEMS AND POLYCENTRIC GOVERNANCE OF SPACE-BASED INFRASTRUCTURE 352
A. SPACE-BASED INFRASTRUCTURE WITHIN THE EARTH-MOON SYSTEM AS COMPLEX SYSTEMS 352
B. POLYCENTRIC GOVERNANCE OF COMPLEX SYSTEMS AND RESILIENCE 357
IV. DIGITAL RESILIENCE VIA POLYCENTRICITY 361
A. INTRODUCTION: THE SPACE-CYBER NEXUS 362
B. TAIWAN AS AN INSTITUTIONAL ENTREPRENEUR 365
C. INFORMATION SHARING TO BUILD TRUST 366
D. TAIWAN'S CYBERSECURITY CULTURE 368
V. CONCLUSION 370

* Simon Sun is an Assistant Professor at the National Yang Ming Chiao Tung University School of Law. Eytan Tepper is a Research Professor, Space Governance & Security, and Director, Space Governance Lab at Indiana University Bloomington.

ABSTRACT

Based on Taiwan's policy objective of digital resilience, this article discusses the challenges of internet connectivity in the region. It will focus on the transition from reliance on submarine cables to the adoption of a space-based infrastructure to provide internet. This article will position this space-based infrastructure as a complex system and proposes that Taiwan could build its resiliency by employing "polycentric governance." This theory, proposed by Nobel Prize Laureate Elinor Ostrom and the Bloomington School of Political Economy, revolves around multiple decision-making centers, with none of which has absolute authority or even priority over the others. Polycentric governance responds to a broad range of challenges and disturbances with greater agility, emphasizing the need for multiple, interconnected governance structures to enhance resilience. This article will make three substantial proposals. First, Taiwan should position itself as an institutional entrepreneur by forming alliances within the region. Second, Taiwan should establish a local chapter of the Space Information Sharing and Analysis Center to build trust. Third, the National Institute of Cyber Security should foster a cybersecurity culture by its local industry considering the flexibility of its institutional design.

RÉSUMÉ

Basé sur l'objectif de résilience numérique de Taïwan, cet article examine les défis de la connectivité internet dans la région. Il analyse la transition des câbles sous-marins vers une infrastructure spatiale pour l'internet. L'article considère cette infrastructure comme un système complexe et propose que Taïwan renforce sa résilience par la « gouvernance polycentrique ». Cette théorie, proposée par Elinor Ostrom, repose sur plusieurs centres de décision sans autorité absolue. L'article présente trois propositions : Taïwan devrait devenir un entrepreneur institutionnel en formant des alliances régionales et créer une section locale du Centre pour le partage spatial et l'Institut national de cybersécurité devrait développer une culture de cybersécurité dans l'industrie locale.

KEYWORDS

Polycentric Governance; Complex Systems; Taiwan; Space Policy; Internet Connectivity; Security

I. INTRODUCTION

The global internet infrastructure is sustained by a sophisticated interplay between submarine cables and space-based infrastructure systems. Taiwan (the Republic of China) faces a challenge to its internet connectivity due to geopolitical tensions with China (the People's Republic of China). The fifteen submarine cables, having a pivotal role in the island's internet connection, are susceptible to disruption, and the international regulations governing their security remain antiquated. If these cables are damaged, Taiwan could lose its connectivity to the world. To address this risk, the government is building its "digital resilience" with plans to develop a space-based broadband internet services similar to that provided by SpaceX's Starlink. Ensuring the functionality of Taiwan's communication systems through space-based infrastructure has become a pressing priority for the island.

II. TAIWAN'S INTERNET INFRASTRUCTURE: CHALLENGES AND RESPONSES

A. CHALLENGES

Taiwan's internet infrastructure — specifically, the submarine cables that sustain its connectivity — is confronting the pressing challenge of potential disconnection. In February 2023, Taiwan's National Communications Commission (NCC) — an independent agency tasked with overseeing the regulation and development of the nation's telecommunications and broadcasting sectors — confirmed that two submarine cables connecting Taiwan to the Matsu Islands had been severed. The incidents were attributed to damage caused by Chinese fishing vessels and cargo ships.[1] While there is no evidence of deliberate action by China, Chunghwa Telecom, Taiwan's largest telecom provider, reports that the underwater cables to Matsu — an island near China's Fujian province — have been damaged over twenty times in the past five years, a frequency considered notable. This time marked the first instance of two cables being damaged within a span of just six days.[2]

---

[1] Brian Hioe, "Cut Submarine Cables Between Taiwan and Matsu Raise Concerns About Chinese Interference", (17 February 2023), online: <newbloommag.net/2023/02/17/matsu-submarine-cable-cut/>.

[2] Tzu-ti Huang, "Taiwan undersea cable cuts linked to Chinese vessels", (17 February 2023), online: <taiwannews.com.tw/en/news/4812970>.

While it remains uncertain whether the incident was orchestrated by China, the People's Liberation Army is reported to have extensively prepared for invasion scenarios, focusing on key infrastructure like submarine cable landing stations.[3] In a potential invasion, China could deploy submarines or uncrewed underwater vehicles to find and cut submarine cables, initiate cyber-attacks to disrupt data flow, and use devices that emit Electromagnetic Pulses (EMPs) to damage submarine cables or the connected infrastructure.[4] As such, these cables present great vulnerability to the nation's security. Submarine cables play a crucial role in internet connectivity, transporting a significant portion of global data traffic. As of June 2024, there are over 600 active and planned submarine cables spanning the ocean floor, linking to over 1,300 coastal landing stations.[5] Approximately 99% of internet traffic between countries and continents is transmitted through cables.[6] Submarine cables rely on fiber-optic technology, where lasers transmit information by encoding it onto waves of light that travel through thin glass fibers.[7] These fiber-optic cables carry nearly all transoceanic digital communications, spanning around 1.2 million kilometers and connecting virtually every country with a coastline.[8] The cables rest on the ocean floor with terminations, or landings, at either end.[9] A cable landing station is strategically chosen for its location, typically in areas with less marine traffic.[10] This piece of cable infrastructure, where the cable makes landfall, is a critical component of the entire system.[11]

---

[3] Christine McDaniel & Weifeng Zhong, "Submarine Cables and Container Shipments: Two Immediate Risks to the US Economy If China Invades Taiwan" (2022) Mercatus Center (Mercatus Policy Brief Series), online: <www.mercatus.org/research/policy-briefs/submarine-cables-and-container-shipments-two-immediate-risks-us-economy-if>.

[4] Chen Chengliang, "China's black hands extend to undersea cables. Foreign media; Taiwan should fight back", (23 March 2023), online: <news.ltn.com.tw/news/life/paper/1573543>.

[5] TeleGeography, "Submarine Cable FAQs", online: <www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions>.

[6] Hitoshi Takeshita et al, "Past, Current and Future Technologies for Optical Submarine Cables", *2019 IEEE/ACM Workshop on Photonics-Optics Technology Oriented Networking, Information and Computing Systems (PHOTONICS)*, (US, 2019), online(pdf): <ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8950690> at 36.

[7] Doug Brake, "Submarine Cables: Critical Infrastructure for Global Communications" (2019) Information Technology & Innovation Foundation, online(pdf): <www2.itif.org/2019-submarine-cables.pdf>.

[8] *Ibid* at 2.

[9] Phil Gervasi, "Diving Deep into Submarine Cables: The Undersea Lifelines of Internet Connectivity", (28 March 2023), online: <www.kentik.com/blog/diving-deep-into-submarine-cables-undersea-lifelines-of-internet-connectivity/>.

[10] *Ibid.*

[11] *Ibid.*

The submarine cable industry comprises two primary types of companies: cable system owners and cable suppliers.[12] Cable system owners, which include national telecommunications carriers, private companies, and investment banks, are responsible for owning and/or operating the cable systems.[13] Given the high cost of trans-oceanic cables — up to US$500 million — these companies often form consortiums of around twenty to thirty telecommunications providers to collectively fund the design, construction, and maintenance of new cables, each receiving a proportional share of the cable's capacity in return.[14] Cable suppliers, on the other hand, are responsible for the system's technical aspects, including its design, planning, and manufacture.[15] These suppliers also cover marine services for cable installation, as well as providing joints and equipment for repairs.[16] Established in 1958, the International Cable Protection Committee is an industry-based organization that includes members who own, operate, and supply over 97% of global submarine cable systems. Unlike vessels, cables do not carry a national registration.[17] While network operators have traditionally been the primary investors, content providers like Google, Amazon, Microsoft, and Meta are also expanding their investments to ensure seamless interconnection between their data centers.[18] Government entities, on the other hand, have ownership or partial ownership of around 1% of submarine cables.[19]

Despite their pivotal role in the digital economy, submarine cables are susceptible to attacks. Physical threats pose the most apparent risks, including shark bites, ship anchor impacts, seismic activity, malicious sabotage, and more.[20] Severing a cable can serve various objectives, including disrupting military or government communications in the early stages of a conflict, cutting off internet access for a targeted population, sabotaging economic competitors, or causing economic disruptions for geopolitical reasons.[21]

---

[12] Tara Davenport, "Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis" (2015) 24:1 Catholic UJL & Tech 57 at 65.

[13] *Ibid.*

[14] *Ibid.*

[15] *Ibid* at 66.

[16] *Ibid* at 66.

[17] *Ibid* at 66.

[18] Colin Wall & Pierre Morcos, "Invisible and Vital: Undersea Cables and Transatlantic Security" (2021), online: <www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security>.

[19] Gervasi, *supra* note 9.

[20] McDaniel & Zhong, supra note 3 at 5.

[21] Wall & Morcos, *supra* note 18.

Tapping cables to intercept and steal data for espionage purposes is also possible. This tapping is achieved by plugging into the network and diverting a small amount of light to a separate receiver.[22] It should be noted that the United States and the United Kingdom have engaged in surveillance by tapping directly into the internet backbone, revealed by Edward Snowden.[23] However, the international legal regime governing submarine cables remains antiquated. The relevant conventions, including the 1884 Convention for the Protection of Submarine Telegraph Cables (1884 Convention), the 1958 Convention on the Continental Shelf, and the 1982 United Nations Convention on the Law of the Sea (UNCLOS), only offer a certain level of peacetime protection to submarine cables. Their relevance during times of conflict is debatable.[24] Submarine cables, thus, remain legitimate wartime targets. For example, the 1884 Convention explicitly states that the obligations to protect within the Convention "do not in any way restrict the freedom of action of belligerents."[25] That being said, some argue that submarine cables between neutral countries, even in wartime, are deemed inviolable and cannot be seized or destroyed except in cases of absolute necessity.[26] The safeguarding of the cable commons becomes a gray zone, some phrase as "the orphans of international law."[27]

Article 113 of UNCLOS mandates that States establish laws and regulations to penalize the willful or negligent breaking or damaging of a submarine cable by vessels flying their flag or by individuals under their jurisdiction.[28] However, Tara Davenport notes several limitations. First, many UNCLOS States Parties have not fulfilled their Article 113 obligations. Second, Article 113 does not confer universal jurisdiction. Third, it only requires States to criminalize intentional damage, without granting the authority to board or arrest vessels suspected of cable interference. Fourth, UNCLOS applies only to the portions of cables laid on the seabed, excluding landing sites.[29]

---

[22] The Fiber Optic Association, Inc, "How To Tap Fiber Optic Cables", online: <www.thefoa.org/tech/ref/appln/tap-fiber.html>.

[23] Davenport, *supra* note 12 at 103-106.

[24] McDaniel & Zhong, *supra* note 3 at 6.

[25] *Convention for the Protection of Submarine Telegraph Cables*, March 14, 1884, 24 Stat 989, T S No 380, art 15.

[26] Davenport, *supra* note 12; *Convention (IV) Respecting the Laws and Customs of War on Land*, October 18, 1907, 36 Stat 2277, 2308, T S No. 539, art 54.

[27] Robert C Beckman, "Protecting Submarine Cables from Intentional Damage—The Security Gap" in Douglas R Burnett et al, eds, *Submarine cables: the handbook of law and policy* (Leiden: Martinus Nijhoff Publishers, 2014) 281.

[28] *United Nations Convention on the Law of the Sea*, December 10, 1982, 1833 UNTS 397, art 113.

[29] Davenport, *supra* note 12 at 83-85.

Taiwan currently maintains connections to fifteen submarine cables, with landing stations located in three areas: New Taipei City, the town of Toucheng in the north, and Fangshan in the south.[30] These landing stations connect high-capacity cables, some of which have received significant investments by US technology companies.[31] For instance, the Pacific Light Cable Network, owned by Google and Meta, has landing points in Toucheng, Taiwan; Baler, the Philippines; and El Segundo, California.[32] According to estimates from the National Communications and Cyber Security Center, Taiwan experienced fifty-one undersea cable service disruptions between 2018 and 2022.[33] Regarding damage to undersea cables caused by natural disasters, two earthquakes near the Hengchun Peninsula in December 2006 damaged two undersea cables, severely disrupting telecommunications services in Taiwan, Hong Kong, South Korea, Japan, and Singapore for about a day.[34] Additionally, this event led to a 50% to 60% reduction in Chunghwa Telecom's overall communication capacity.[35]

B. RESPONSES

In response to the potential loss of the island's internet connectivity, the Taiwanese Ministry of Digital Affairs (MODA) have announced that its core mission is to foster "digital resilience" among its citizens.[36] Digital resilience, in this context, refers to "using digital tools to enable Taiwan to not only withstand various adverse situations but also to quickly recover from setbacks, learn from them, and strengthen its resilience."[37] One prime example, as explained by MODA, is Ukraine's ability to maintain uninterrupted communication due to the support of the low Earth orbit satellite network (SpaceX's Starlink) during the war with Russia.[38]

---

[30] McDaniel & Zhong, *supra* note 3 at 6.

[31] *Ibid*.

[32] *Ibid*.

[33] Matthew Fulco, "Boosting Digital Infrastructure Resilience", (15 February 2024), online: <topics.amcham.com.tw/2024/02/boosting-digital-infrastructure-resilience/>.

[34] *Ibid.*

[35] *Ibid.*

[36] Ministry of Digital Affairs, "Minister Huang Unveil the three arrows for Digital Development: Anti-Fraud, Digital Resilience, and Digital Economy", (3 June 2024), online: <moda.gov.tw/en/press/press-releases/12878>.

[37] Ministry of Digital Affairs, "The core concept of the Digital Development Department is 'strengthening the digital resilience of the whole population.' What is 'digital resilience'?",(21 September 2022), online: <moda.gov.tw/press/clarification/2512> [title translated by author].

[38] *Ibid.*

Taiwan has made significant progress in building its network defenses. To mitigate the impact of natural and human-made disturbances, Taiwan plans to strengthen its undersea cable network and install a brand-new backup satellite internet network.[39] Measures include enhancing network capabilities, investing in information technologies, setting cybersecurity standards, and establishing an additional cyber department within the Ministry of National Defense.[40] The National Science and Technology Council has ordered the National Center for High-Performance Computing to establish a cloud server center, an internet cable landing point, and a backup auxiliary point, "to enhance system redundancy and security" with the plan to be completed by 2025.[41] The Southeast Asia-Japan 2 Cable (SJC2), which connects Taiwan, Japan, South Korea, and Singapore, is expected to be ready for service in 2025.[42] System operators have chosen to set up two landing points, ensuring that failure at one site will not sever Taiwan's connection to the network.[43] The 10,500-kilometer-long fiber optic cable system was originally scheduled for completion in 2020.[44] However, the progress of laying the cable through the South China Sea was delayed due to China deliberately slowing down the issuance of permits.[45]

In addition to this cable project, Taiwan is developing a backup satellite network entirely made in and controlled from Taiwan.[46] The government is currently taking a two-pronged approach to enhance network resilience for emergency applications through the National Space Organization's B5G Low Earth Orbit (LEO) Communication Satellite Program and related projects by the Ministry of Digital Affairs to enhance reliance on communications networks during emergencies.[47] MODA plans to establish 700 hotspots, 70 low-Earth orbit satellite backhaul links, and 3 overseas hotspots to enhance infrastructure resilience.[48]

---

[39] Fulco, *supra* note 33.

[40] *Ibid.*

[41] *Ibid.*

[42] TeleGeography, "Submarine Cable Map", online: <www.submarinecablemap.com/ready-for-service/2025>.

[43] Fulco, *supra* note 33.

[44] *Ibid.*

[45] *Ibid.*

[46] Meaghan Tobin & John Liu, "Why Taiwan Is Building a Satellite Network Without Elon Musk", *The New York Times* (14 March 2024), online: <www.nytimes.com/2024/03/14/business/taiwan-starlink-satellite.html>.

[47] Fulco, *supra* note 33.

[48] Ministry of Digital Affairs, "A project to strengthen the digital resilience of communication

The main companies driving this project include Chunghwa Telecom and Eutelsat OneWeb.[49] Based on the best practices of diversity and heterogeneity for resilience, MODA has declared that it will not restrict or favor any single satellite operator.[50] As long as satellite system operators do not have Chinese capital or use Chinese-branded equipment and comply with national security and cybersecurity regulations, executing units are expected to evaluate the possibility of cooperation with global satellite operators and explore the feasibility of using heterogeneous solutions to achieve the goal of enhancing communication resilience for this project.[51]

Taiwan's strategy for digital resilience, especially given its concerns regarding China, is not an isolated case. Rather, it resonates with other regions facing comparable geopolitical and cybersecurity challenges — primarily small and highly developed countries in conflict with adversaries capable of disrupting critical services. Israel is another small and highly developed nation, in active conflict with Iran and its proxies which includes cyber-attacks.[52] Ukraine has suffered the first space based cyber-attack as part of a military campaign and its infrastructure is routinely attacked by conventional and cyber means.[53] Finland's recent accession to the North Atlantic Treaty Organization (NATO) has intensified tensions with neighboring Russia.[54] The United Arab Emirates — a small, developed nation with a rapidly expanding space sector — finds itself situated in a region fraught with multiple security threats and on the edge of regional conflict.[55]

---

networks using emerging technologies in times of crisis or war", (15 March 2024), online: <moda.gov.tw/digital-affairs/communications-cyber-resilience/programs/4187> [MODA] [title translated by author].

[49] Fulco, *supra* note 33.

[50] MODA, *supra* note 48.

[51] *Ibid.*

[52] Agence France-Presse, "Report: Iran cyberattacks against Israel surge after Gaza war", (15 October 2024), online: <www.voanews.com/a/report-iran-cyberattacks-against-israel-surge-after-gaza-war/7823577.html>.

[53] Eytan Tepper, "The First Space-Cyber War and the Need for New Regimes and Policies", (16 May 2022), online: <www.cigionline.org/publications/the-first-space-cyber-war-and-the-need-for-new-regimes-and-policies/>.

[54] Amarachi Orie, "Putin warns of 'problems' with neighboring Finland after West 'dragged it into NATO'", *CNN* (17 December 2023), online: <www.cnn.com/2023/12/17/world/putin-warns-problems-finland-nato-intl/index.html>.

[55] *State of the UAE Cybersecurity Report*, (Cyber Security Council, 2024), online(pdf): <www.cpx.net/media/hocl331j/state-of-the-uae-cybersecurity-report.pdf>.

These examples underscore that the global challenges of cybersecurity and geopolitical tension are not confined to any one region, but rather signal a larger, interconnected shift toward safeguarding critical infrastructure, and particularly space-based infrastructure in an age of increasing cyberthreats. As nations grapple with evolving threats, the need for comprehensive strategies to ensure resilience in the face of warfare becomes ever more urgent.

III. COMPLEX SYSTEMS AND POLYCENTRIC GOVERNANCE OF SPACE-BASED INFRASTRUCTURE

Taiwan's efforts to secure its submarine cable connections and expand its space-based infrastructure leads to a broader conversation around a theoretical framework for digital resilience. After all, a stable internet connection is essential not only in times of conflict but also for advancing technologies like Artificial Intelligence. The task of securing this connection is especially challenging due to the unpredictable nature, technical complexities, and geopolitical intricacies of space governance itself. In this light, we begin by defining the nature of space-based infrastructure and its corresponding governance structure. The aim is to ensure that space governance institutions are prepared for swift and effective responses.

A. SPACE-BASED INFRASTRUCTURE WITHIN THE EARTH-MOON SYSTEM AS COMPLEX SYSTEMS

We consider space-based infrastructure within the Earth-Moon System as a complex system. Satellites are part of a larger category of space-based infrastructure, which also includes launch facilities, communication networks, orbital platforms, propulsion and transportation systems, life extension services, and surface infrastructure.[56] The Earth-Moon System encompasses the spatial expanse extending between the Earth and Moon.[57] Around Earth, there are several bandwidths of orbital space with particular significance for space security. This includes Geosynchronous orbit (GSO) and Medium Earth Orbit (MEO), each distinguished by the time required for a space vehicle to complete one orbit around Earth.[58]

---

[56] "Space Infrastructure: Foundations for Planetary Exploration", (30 August 2024), *Space Impulse,* online: <spaceimpulse.com/2024/08/30/space-infrastructure/>.

[57] Richard J Chasdi, *Rudiments of a Space Security Policy Framework*, CIGI Papers, No. 267 (Waterloo: Centre for International Governance Innovation, 2022) at 2.

[58] *Ibid.*

These orbital layers align with specific on-board functions that are optimized for their respective rotation periods and altitudes.[59] The Earth-Moon System is of particular interest, as it serves as the primary domain for both commercial ventures and the strategic ambitions of States.[60]

While there is not yet a single agreed upon definition of what complexity means, a complex system can be generally understood as:

> a system in which large networks of components with no central control and simple rules of operation give rise to complex collective behavior, sophisticated information processing and adaptation via learning or evolution.[61]

Some differentiate between Complex Adaptive Systems (CAS), in which adaptation plays a large role, and nonadaptive complex systems, such as hurricanes or turbulent rushing rivers.[62] Typically, a system that exhibits nontrivial *emergent* and *self-organizing* properties can be considered a complex system.[63] As explained by Professor Melanie Mitchell:

> [s]ystems in which organized behavior arises without an internal or external controller or leader are sometimes called 'self-organizing.' Since simple rules produce complex behavior in hard-to-predict ways, the macroscopic behavior of such systems is sometimes called 'emergent.'... The central question of the sciences of complexity is how this emergent self-organizing behavior comes about.[64]

Classic examples of complex systems include insect colonies, where millions of individual ants, each with their own roles, collectively build intricate structures.[65] Professor Douglas Hofstadter draws an analogy between the brain and ant colonies, highlighting the similarities in how individual units work together to produce sophisticated system-wide behaviors.[66]

---

[59] *Ibid.*

[60] *Ibid.*

[61] Melanie Mitchell, *Complexity: A Guided Tour*, 1st ed (New York; Oxford University Press, 2011).

[62] *Ibid.*

[63] *Ibid* at 14.

[64] *Ibid* at 13.

[65] *Ibid* at 4.

[66] *Ibid* at 5-6.

To date, scientists still do not fully understand how actions of individual agents or dense networks combine to generate cognitive patterns.[67] The immune system's behavior emerges from the independent actions of simple players — B cells, T cells, macrophages — forming a kind of chemical signal-processing network.[68] When one cell recognizes an invader, it triggers a cascade of signals among other cells, setting into motion an intricate, coordinated response.

Lastly, economies are complex systems.[69] Adam Smith famously called the market's self-organizing behavior the "invisible hand."[70] The "simple, microscopic" components consist of actors providing and consuming goods and services, and the collective behavior is the hard-to-predict behavior of markets.[71] Some study biological evolution as an emergent phenomenon, with efforts investigating whether genetic changes sifted by natural selection are not entirely random but emerge via an array of mutational mechanisms.[72] In fact, complex systems science has long been intertwined with space studies, offering insights into the relationship between general relativity and quantum field theory.[73]

---

[67] *Ibid* at 6.

[68] *Ibid* at 9.

[69] *Ibid* at 9.

[70] *Ibid* at 10.

[71] *Ibid.*

[72] Nate Barksdale, "What Is Emergence?", (15 February 2023), online: <www.templeton.org/news/what-is-emergence>.

[73] George Musser, "Emergence: A Review of Research on Condensed Matter and Quantum Gravity and Resonances Between These Fields" (December 2021) John Templeton Foundation, online(pdf): <www.templeton.org/wp-content/uploads/2021/12/Research-on-Emergence-Musser-1.pdf>.

Drawing from the international relations literature,[74] we argue that space-based infrastructure within the Earth-Moon System can be conceptualized as a complex system, given its emergence and self-organizing behavior. First, emergence is usually referred to as "systemic unexpected outcomes, where the sum is not only greater but most of all different—unexpected patterns arise from interactions among the elements of the system."[75] Space-based infrastructure exhibits nontrivial emergence, the result of many separate actions by multiple and diverse stakeholders, including space agencies, private space companies, and regulatory bodies, and the collaboration and interaction among the various stakeholders, which lead to unanticipated outcomes. Joint efforts in space exploration and satellite deployment often result in new technologies, protocols, and governance frameworks that no single entity could have predicted or controlled. These interactions create a dynamic network where individual actions, decisions, and innovations shape the overall system in unpredictable ways. This can lead to technological advancements and improved international cooperation as well as regulatory conflicts or space debris accumulation.

The complexity is further heightened by the diverse goals and interests involved, such as scientific research, commercial ventures, national security, and environmental protection. We generally cannot predict which big new threat or opportunity will eventuate, or even what those threats and opportunities might be.[76] We cannot always tell which relationship is going to be the most important, or which kind of power will be effective.[77]

---

[74] Carla Winston, "International Norms as Emergent Properties of Complex Adaptive Systems" (2023) 67:3 International Studies Quarterly sqad063; Rakhyun E Kim, "Is Global Governance Fragmented, Polycentric, or Complex? The State of the Art of the Network Approach" (2020) 22:4 International Studies Review 903; Amandine Orsini et al, "Forum: Complex Systems and International Governance" (2020) 22:4 International Studies Review 1008; Seva Gunitsky, "Complexity and theories of change in international politics" (2013) 5:1 International Theory 35; Youn-soo Sim, "International Relations & Complex Systems Theory" (2007) Proceedings of the 51st Annual Meeting of the ISSS — 2007, Tokyo, Japan, online: <journals.isss.org/index.php/proceedings51st/article/view/607>; Emilian Kavalski, "The Fifth Debate and the Emergence of Complex International Relations Theory: notes on the application of complexity theory to the study of international life" (2007) 20(3) Cambridge Review of International Affairs 435; Ion Cîndea, "Complex Systems – New Conceptual Tools for International Relations" (2006) 26 Perspectives : Review of International Affairs 46.

[75] Orsini et al, *supra* note 74 at 1010–1011; Kavalski, *supra* note 74.

[76] Winston, *supra* note 74.

[77] *Ibid.*

The second property of a complex system is self-organization, meaning that "order does not rely on a clear authority but on the system itself and on its multiple interactions."[78] In other words, new forms are generated from internal guidelines rather than being imposed from the outside.[79] In the context of space-based infrastructure, self-organization is evident in how the various stakeholders interact and cooperate. This organization happens without a single governing body dictating every action. Instead, individual entities independently pursue their goals while adapting to the actions and innovations of others. For instance, the development of the UN space law treaties, international cooperation on space missions, and the establishment of protocols for satellite communications are outcomes of these self-organizing processes.[80] This self-organizing behaviour is especially evident here because most international agreements on space-based infrastructure are non-binding.

Overall, framing the space-based infrastructure within the Earth-Moon System as a complex system aligns with the evolution of space governance, which has exhibited the concept of emergence and self-governance. As explained by Eytan Tepper, the initial hierarchic structure of space governance, in which UN Committee on the Peaceful Uses of Outer Space (UNCOPUOS) is mandated with creating and expanding the *corpus juris spatialis*, reached an impasse culminating in a decades-long gridlock, and has been experiencing a slow-motion "big bang."[81] While the early building blocks remain, the subsequent evolution of space governance is continued through the work of various governance centers, with participants introducing various outputs.[82] We can expect the continuation of the emergence of issue-specific governance centers and new regimes, as a result of the self-governed and voluntary activities of individual actors with no single guiding hand.[83] With the cessation of the rule making capability of UNCOPUOS, the twenty-first century has seen a gradual, yet steady emergence of smaller, issue-specific forums, often led by experts and stakeholders, that introduce various types of instruments: 'guidelines,' 'building blocks,' 'manual,' etc.[84] For example, the Space Debris Mitigation Guidelines.

---

[78] Orsini et al, *supra* note 74 at 1010-1011.

[79] Kavalski, *supra* note 74 at 439.

[80] Winston, *supra* note 74 at 5.

[81] Eytan Tepper, "The Big Bang of Space Governance: Towards Polycentric Governance of Space Activities" (2022) 54 NYUJ Intl L & Pol 485 at 516.

[82] *Ibid.*

[83] *Ibid* at 510.

[84] *Ibid.*

B. POLYCENTRIC GOVERNANCE OF COMPLEX SYSTEMS AND RESILIENCE

The characteristics of complex systems constrain our ability to predict their behavior, calling for a shift in expectations regarding what policy tools can feasibly achieve.[85] Consequently, policy analysis must move away from a traditional focus on outcome optimization toward an evolutionary model that prioritizes adaptability.[86] Sustainable policy development, in turn, requires evaluating and potentially redesigning policymaking processes to ensure they are resilient and capable of adapting to dynamic conditions.[87]

To manage complex change effectively, the governance system must mirror the complexity of the external environment—an idea some label as the "diversity hypothesis."[88] The assumption is that institutional and organizational diversity is the most effective way to cope with complexity.[89] This can be traced back to the work of W. Ross Ashby and the now classic ''Law of Requisite Variety,'' which notes that only ''variety can destroy variety.''[90] While earlier waves of complexity theory applications on social science were criticized for being too closely aligned with their natural science origins, a new application of complex systems thinking has emerged within the social sciences over the past two decades.[91] The wave of applications more sensitive to the characteristics endogenous to the social realm includes Elinor Ostrom's shift from studying the local governance of natural resources to an increased emphasis on social-ecological systems.[92] Ostrom's scholarship has demonstrated the power of local-level collective action, particularly in the governance of Common-Pool Resources (CPR), a type of resource characterized by high subtractive ability and low excludability.[93]

---

[85] Barbara A Cherry & Johannes M Bauer, "Adaptive Regulation: Contours of a Policy Model for the Internet" (2004), at 13.

[86] *Ibid.*

[87] *Ibid.*

[88] Andreas Duit et al, "Governance, complexity, and resilience" (2010) 20:3 Global Environmental Change (Governance, Complexity and Resilience) 363 at 365.

[89] *Ibid.*

[90] William Ross Ashby, *An introduction to cybernetics* (New York; J Wiley, 1956).

[91] Duit et al *supra* note 88 at 363.

[92] *Ibid* at 364.

[93] Elinor Ostrom, "Beyond Markets and States: Polycentric Governance of Complex Economic Systems" (2010) 100:3 American Economic Review 641.

Under Ostrom's leadership, extensive empirical research was conducted at the Workshop in Political Theory and Policy Analysis, also known as the Ostrom Workshop.[94] Her work at the Ostrom Workshop led to the development of the "Bloomington School of Political Economy,"[95] which introduced the Institutional Analysis and Development (IAD) Framework. This framework provides social scientists with the building blocks to analyze human interactions and outcomes across diverse settings.[96] The IAD Framework laid the groundwork for a coding manual that enabled researchers to record key variables for CPR studies.[97] This approach led to the identification of eight design principles essential for managing CPRs, ultimately contributing to Ostrom's Nobel Prize.[98]

The eight design principles embedded the notion of ''polycentricity,'' described by the Bloomington School as the existence of "multiple centers of decision-making, or multiple authorities, no one [of] which has ultimate authority for making all collective decisions."[99] Ostrom's study of polycentricity started with the research on federalism.[100] The insight was that the presence of overlapping jurisdictions—such as the interdependence of governed issues and the interconnectedness of physical territories—is essential to the dynamism of polycentric governance.[101] Without this overlap, fewer decision centers would feel compelled to consider one another's actions, which is crucial for fostering both competition and cooperation among authorities.[102]

---

[94] Indiana University, "The Ostroms & Our History", online: <ostromworkshop.indiana.edu/about/ostroms-history/index.html>.

[95] Paul D Aligica & Vlad Tarko, "Polycentricity: From Polanyi to Ostrom, and Beyond" (2012) 25:2 Governance 237.

[96] Ostrom, *supra* note 93 at 646.

[97] *Ibid* at 649.

[98] *Ibid* at 653.

[99] Mark Stephan, Graham Marshall & Michael McGinnis, "An Introduction to Polycentricity and Governance" in Andreas Thiel, William A Blomquist & Dustin E Garrick, eds, *Governing Complexity*, 1st ed (Cambridge; Cambridge University Press, 2019) 21 at 31.

[100] *Ibid* at 22.

[101] *Ibid* at 33.

[102] *Ibid*.

The advantages of polycentric governance are not limited to only small-sized decision centers, but rather serve as a solution for adaptive management, resilience and robustness also in large systems.[103] When discussing climate change, for instance, Ostrom states that polycentric governance tends to enhance innovation, learning adaptation, trustworthiness, levels of cooperation of participation and the achievement of more effective, equitable, and sustainable outcomes at multiple scales.[104] In essence, polycentric governance responds to a broad range of challenges and disturbances with greater agility, allowing for a more nuanced and locally adapted response to issues, as decisions are made closer to the affected areas and by those with better contextual understanding.[105] This approach enables various decision-making bodies to innovate and experiment with different solutions, leading to a diversity of strategies that can be tailored to specific needs and conditions. In fact, the redundancy inherent in polycentric systems enhances resilience. If one part of the system fails, others can compensate, reducing the risk of total system collapse. This overlapping of functions and jurisdictions means that the system as a whole can continue to function and adapt even when individual components are under stress.

Polycentric systems themselves can be CAS without one central authority dominating all the others.[106] On a variety of occasions, polycentric governance has been equated with CAS.[107] In a polycentric system, some units are general-purpose governments while others may be highly specialized. Direct attempts at system-level coordination will prompt cascading adjustments by other decision centers, each adapting to one another's shifts. As a result, the outcome becomes emergent.[108]

---

[103] *Ibid* at 38.

[104] Ostrom, *supra* note 93 at 665.

[105] Ludomir R Lozny, "Polycentric Governance as a Practical Strategy for Balanced Policing: A Cross-Cultural Analysis" (2023) 22:2 SEH 249.

[106] "Polycentricity, Complexity, and the Commons", online: <centerforneweconomics.org/publications/polycentricity-complexity-and-the-commons/>.

[107] Andreas Thiel, Raul Pacheco-Vega & Elizabeth Baldwin, "Evolutionary Institutional Change and Performance in Polycentric Governance" in Andreas Thiel, William A Blomquist & Dustin E Garrick, eds, *Governing Complexity*, 1st ed (Cambridge; Cambridge University Press, 2019) 91, 101.

[108] Stephan, Marshall & McGinnis *supra* note 99 at 38.

Effective coordination within complex systems may emerge from explicit efforts by higher levels within the system or from the bottom up as a side-effect of other efforts.[109] The result is the facilitation of the emergence of "stronger, better performing polycentric governance" that is nimble and adaptive, both characteristics of a complex adaptive system.[110]

Polycentric governance insights have been applied to global affairs.[111] The substantively similar nature of local and global problems justifies this expansion. The underlying logical configuration is fundamentally alike, and any global regime that undermines the requisites for successful cooperation at the local level is unlikely to be sustainable.[112] Keohane and Ostrom observe that "many of the 'design principles' underlying successful self-organized solutions to CPR problems appear relevant to the design of institutions to resolve problems of international cooperation."[113]

Polycentric governance aligns with what international law scholars call, often with concern, as "fragmentation," referring to the proliferation of treaties, rules, institutions, and tribunals.[114] It resonates with what international relations literature refers to as "regime complexes," where a single issue area lacks an integrated, comprehensive governing regime.[115] Tepper explains that "there is convergence of the underlying causes, characteristics and, significantly, insights, of the three theories of decentralized governance."[116] In fact, space governance is on track to become polycentric, as "stakeholders and experts establish various forums ('governance centers'), that suggest, adopt or push for rules and standards of varying types and membership, bringing decentralized, incremental evolution of space governance."[117]

---

[109] *Ibid.*

[110] Thiel, Pacheco-Vega & Baldwin, *supra* note 107 at 109.

[111] Eytan Tepper, "The Laws of Space Warfare: A Tale of Non-Binding International Agreements" (2024) 83:2 Maryland Law Review 458 at 504; Scott J Shackelford, *Governing New Frontiers in the Information Age: Toward Cyber Peace* (New York; Cambridge University Press, 2020).

[112] Michael McGinnis & Elinor Ostrom, *Design Principles for Local and Global Commons* (2 Harvard Ctr Int'l Affs, Working Paper No D92-6, 1992), online(pdf): <dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/5460/design%20principles%20for%20loca l%20and%20global%20commons.pdf>.

[113] Robert Keohane & Elinor Ostrom, *Local Commons and Global Interdependence: Heterogeneity and Cooperation in Two Domains* (London: SAGE Publications Ltd, 1995).

[114] *Ibid* at 520.

[115] *Ibid.*

[116] *Ibid* at 536-537.

[117] Tepper, *supra* note 81.

This trend can be seen in the Outer Space Treaty. Under Article VI, besides governmental entities, the participation of non-governmental entities is included.[118] The Outer Space Treaty serves as a constitutional-type document, establishing foundational rules and principles broadly accepted by all actors. It remains intentionally vague, encompassing only the most basic guidelines. Moreover, the once monocentric governance system with the UNCOPUOS at the core is transforming. As mentioned above, UNCOPUOS was instrumental in the introduction of the existing five space law treaties adopted between 1967 and 1979. But the changing geopolitical environment curtailed its ability to further develop international space law, and indeed, no space law treaty was adopted since 1979, and none is expected in the foreseeable future.

But while international rulemaking is in decades-long gridlock, new technologies, products and business models transform space activities, straining the ability of the space law treaties to provide adequate governance. Stakeholders respond and try to update the governance system in various ways, including off-UN forums and the adoption of non-legally binding instruments. As a result, Tepper suggests that this bottom-up development of space governance would lead to a more comprehensive, flexible, and updated governance system than a top-down system could yield.[119]

IV. DIGITAL RESILIENCE VIA POLYCENTRICITY

Framing the Space-Based Infrastructure within the Earth-Moon System as a complex system opens up the discussion about polycentric governance, emphasizing the need for multiple, interconnected governance structures to enhance resilience. These structures operate at various levels—ranging from international agreements to local jurisdictional frameworks—while fostering cooperation and reducing the potential for conflict. At the national level, polycentricity means there should be multiple government agencies involved, notably the national space agency, the defense establishment, and the agencies regulating communication, air traffic, and more. None of them has overriding power, and together with the commercial space industry, these stakeholders create a complex and polycentric governance system. In this context, we will examine scenarios where space-based infrastructure might be targeted and explore how to foster polycentric governance in Taiwan.

---

[118] *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, 27 January 1967, 610 UNTS 205, art VI.
[119] *Ibid.*

A. INTRODUCTION: THE SPACE-CYBER NEXUS

Space-based infrastructure, as critical security and economic infrastructure, is a prime target for malicious attack. This has been described by Tepper as the "Space-Cyber Nexus."[120] Considering its connectivity, threats stemming from the internet can potentially turn into attacks, conflicts, or warfare in outer space, compounded by the race for outer space commercialization and the lack of an oversight agency responsible for securing space assets.[121] Noting, for example, that the US Space Force warns from multiple attack vectors of space systems including "hacking on-orbit satellites; infiltrating the ground-system computers that control and receive data from satellites; compromising drones; or affecting other computer systems, which in-turn can compromise everything from satellites to power grids and other infrastructure."[122] The various threats include data breach, denial of service, malware, spyware, terrorism and ransomware. Combining limited energy resources, weaker processors, and outdated hardware and software in space systems can create vulnerabilities.[123] In addition, space-based services are vulnerable to electronic interference, including the jamming and spoofing of GPS signals.[124] Arguably, cyberattacks are likely to become the preferred method for targeting space-based infrastructure, rather than anti-satellite weapons.[125] After all, only a few countries possess the capability to physically destroy satellites—primarily India, China, Russia, and the U.S.—making accountability more straightforward.[126] Moreover, the resulting space debris would also pose a direct risk to each actor's own satellites. In comparison, cyberattacks require fewer resources in terms of funding, technology, and engineering.[127] Furthermore, cyber attackers can attempt to disguise their identity, leaving the targeted nation uncertain about attribution and its appropriate response.[128]

---

[120] Tepper, *supra* note 53 at 1.

[121] Yasir Gökce, "Satellites Under Attack: An Evaluation of a Mock Cyber Operation in Space Under International Law" in Unal Tata et al *Space Infrastructures: From Risk to Resilience Governance* (IOS Press, 2020) 100.

[122] "Focused on the Threat: Cyber Attacks (Part 1 of 6)", (12 September 2024), online: <www.ssc.spaceforce.mil/Newsroom/Article-Display/Article/3904505/https%3A%2F%2Fwww.ssc.spaceforce.mil%2FNewsroom%2FArticle-Display%2FArticle%2F3904505%2Ffocused-on-the-threat-cyber-attacks-part-1-of-6>.

[123] Eytan Tepper et al, "The Sixth Warfighting Domain? Governing The Space-Cyber Nexus", (forthcoming 2024) 59 Georgia L Rev *1.

[124] *Ibid* at 23.

[125] *Ibid* at 1.

[126] *Ibid.*

[127] *Ibid.*

[128] *Ibid.*

Overall, the endeavor toward developing space-based infrastructure is closely linked to the war in Ukraine. Since the Russian invasion, Starlink has been utilized by Ukrainian civilians, government, and military forces.[129] Furthermore, on the day Russia invaded Ukraine, Viasat, a high-speed satellite broadband service provider, suffered an outage that disrupted internet services for the Ukrainian armed forces, intelligence agencies, and police.[130] It is alleged that Russia jammed GPS signals in Ukraine, hindering the Ukrainians' ability to pinpoint their location, navigate, and direct weapons to their targets.[131] Additionally, Dmitry Rogozin, the head of the Russian space agency Roscosmos, warned that any hacking of Russian satellites would be considered a *casus belli*—a justification for war.[132] Clémence Poirier mapped 124 cyber operations against the space sector in the context of the war in Ukraine, including at least 57 different space targets that ended up in hacker groups' crosshairs.[133] The current war in Ukraine might be remembered as the first space-cyber war,[134] where space has become the "sixth" space cyber warfare domain.[135]

China has noticed Starlink's national security implications. Chinese researchers advise that the government must be prepared to disable Starlink through a combination of hard-kill and soft-kill anti-satellite capabilities if it threatens China's national security.[136] China's concern centers on Starlink's US military utility if China launches a campaign to annex Taiwan or takes action against an ally.[137] China is aware that Starlink could potentially provide command and control capabilities to Taiwanese forces.[138] Consequently, China appears to be taking preemptive measures against Starlink via an Article V action filed with the UN.[139]

---

[129] *Ibid* at 3.

[130] *Ibid.*

[131] *Ibid.*

[132] *Ibid.*

[133] "Hacking the Cosmos: Cyber operations against the space sector. A case study from the war in Ukraine", (4 October 2024), online: <css.ethz.ch/ueber-uns/CSS-news/2024/10/hacking-the-cosmos-cyber-operations-against-the-space-sector-a-case-study-from-the-war-in-ukraine.html>.

[134] *Ibid* at 2.

[135] Tepper et al, *supra* note 123.

[136] Ren Yuanzhen et al, "The current development status of the Star Chain project and counter-thinking" (2022) 50(2) Modern defence technology [title translated by author].

[137] Michael J Listner, "The Space Review: China, Article V, Starlink, and hybrid warfare: An assessment of a lawfare operation", (11 September 2023), online: <www.thespacereview.com/article/4650/1>.

[138] *Ibid.*

[139] *Ibid.*

The shift toward space-based infrastructure for internet connectivity is reflected in new NATO initiatives. A NATO-funded initiative, launched on 31 July 2024, aims to make the internet resilient by rerouting the flow of information into space in the event that undersea cables are attacked or accidentally severed.[140] The new consortium called "Hybrid Space/Submarine Architecture Ensuring Infosec of Telecommunications," also known as HEIST, includes researchers from Johns Hopkins University, Bifröst University in Iceland, ETH Zürich in Switzerland and the Swedish Defence University (Försvarshögskolan).[141] Taiwan should engage in similar initiatives by embracing a polycentric model to better safeguard its critical communications infrastructure against various threats, reinforcing its position as a leader in network resilience and innovation in the Asia-Pacific region.

The Space-Cyber Nexus has emerged as a significant risk for security, economic infrastructure, and numerous commercial companies.[142] Introducing a fundamentally different internet connectivity—from satellite-based internet to submarine cables—established and operated by multiple public and private entities, creates a decentralized, polycentric infrastructure, resilient to single-point failures. This approach enhances the security of Taiwan's digital landscape and also ensures that the nation remains connected even in the face of disruptions. It recognizes the diverse stakeholders involved, including governments, the private sector, and international organizations, each of which may have competing interests, but all of which must collaborate to ensure sustainable, secure, and equitable access to space infrastructure.

Besides the infrastructural development, more institutional work needs to be done to embrace polycentricity. For this reason, this article advocates for polycentric governance of Taiwan's space-cyber infrastructure, where multiple agencies, stakeholders, and forums—including government ministries, the domestic commercial sector, foreign companies, and allies—collaborate to ensure a resilient framework. We believe that three institutional actions need to be done by the Taiwanese government to embrace polycentricity. In the following section, we will explore key recommendations for Taiwan's institutional arrangements that embrace polycentricity on various levels.

---

[140] North Atlantic Treaty Organization, "NATO-funded project to reroute internet to space in case of disruption to critical infrastructure", online: <www.nato.int/cps/en/natohq/news_228257.htm>.

[141] David Nutt, "Hybrid system would create new 'backbone' for internet in space", online: <news.cornell.edu/stories/2024/08/hybrid-system-would-create-new-backbone-internet-space>.

[142] Tepper, *supra* note 53 at 1.

B. TAIWAN AS AN INSTITUTIONAL ENTREPRENEUR

Taiwan must take the lead as an institutional entrepreneur by forging a regional alliance. Taiwan can establish itself as a decision-making center within this framing, creating a network of partnerships that enhances regional cooperation and influence in global space policy discussions. To effectively address collective-action problems, fostering entrepreneurship and innovation across local, regional, national, and international domains becomes critical. As explained by Elinor Ostrom, entrepreneurship is a particular form of leadership focused primarily on problem solving and putting heterogeneous processes together in complementary and effective ways. These can be understood as "acts performed by actors who seek to punch above their weight."[143] Indeed, there is a critical difference between actors who merely do their job and do what is appropriate.[144]

Taiwan should actively engage in conversation with regional alliances within the East Asian region, Southeast Asian region, as well as the Pacific Island region. The Quadrilateral Security Dialogue, known as the Quad, for instance, is a strategic security dialogue between Australia, India, Japan, and the United States.[145] Taiwan should initiate activities within the Quad, considering its geographical proximity to the key stakeholders and its strategic importance in the Indo-Pacific region. Taiwan should also actively engage within the Pacific region, participating in platforms such as the Asia-Pacific Regional Space Agency Forum (APRSAF)[146] while strengthening ties with Pacific Island nations, including the Marshall Islands, the Republic of Palau, and Tuvalu.[147]

---

[143] Elinor Ostrom, "Polycentric Systems: Multilevel Governance Involving a Diversity of Organizations" in Eric Brousseau et al, eds, *Global Environmental Commons: Analytical and Political Challenges in Building Governance Mechanisms,* 1st ed (Oxford; Oxford University Press, 2012) 105.

[144] Elin Boasson, "Entrepreneurship" in Andrew Jordan et al, eds, *Governing climate change: Polycentricity in action?* (Cambridge; Cambridge University Press, 2018) 117.

[145] Derek Grossman, "America's Indo-Pacific Alliances Are Astonishingly Strong", (1 November 2024), online: <foreignpolicy.com/2023/12/05/us-china-alliances-allies-geopolitics-balance-power-asia-india-taiwan-japan-south-korea-quad-aukus/>.

[146] "Asia-Pacific Regional Space Agency Forum", online: <www.aprsaf.org/>.

[147] Alayna Parlevliet, "Support Threefold: Taiwan's Pacific Island Allies", (17 July 2024), online: <www.csis.org/blogs/new-perspectives-asia/support-threefold-taiwans-pacific-island-allies>.

Another step Taiwan could take is to initiate the formation of a regional alliance, similar to NATO. Established after World War II, NATO serves as an intergovernmental military alliance of 32 member states—30 European and two North American. It is a collective security system, where independent States agree to defend each other against attacks by third parties. In fact, since the conflict between Russia and Ukraine, NATO is set to deepen relations with its four Indo-Pacific partners, in response to the closer ties between Russia and China.[148] The goal is for Taiwan to call for policy changes in regard to maintaining the security of space-based infrastructure.

Overall, this approach contributes to a more resilient and adaptable governance structure in the region. Through regional collaboration, Taiwan can help shape a cohesive and effective governance model that reflects the shared interests of its allies while positioning itself as a central node in the polycentric governance of space. Taiwan can facilitate the exchange of knowledge, resources, and expertise among its partners, creating a more integrated and responsive governance network, by leading the formation of a regional alliance.

C. INFORMATION SHARING TO BUILD TRUST

One important notion to foster polycentricity is information sharing, a measure for interorganizational, intersectoral, and intergovernmental exchange of data that is deemed by sharers to be relevant to the resolution of a collective action problem.[149] It should be an ongoing exercise in trust building among shares.[150] In a literature review of public good and CPR experiments, Ostrom explains that "building trust ... to be a key link in the communication-cooperation connection" and "the efficacy of communication is related to the capacity to talk on a face-to-face basis."[151] A polycentric approach maximizes the potential for remedying informational asymmetries among a diversity of shares, bringing a variety of perspectives and capabilities and explicitly acknowledges the complex inter-dependencies of different actors.[152]

---

[148] Didi Tang, "NATO and its Asian partners forge deeper relations to counter China", (10 July 2024), online: <apnews.com/article/nato-japan-south-korea-australia-new-zealand-6c3d9aa6fccc1253ca99ee140073f95c>.

[149] Deborah Housen-Couriel, "Information Sharing as a Critical Best Practice for the Sustainability of Cyber Peace" in (2022) 39.

[150] *Ibid* at 42.

[151] Elinor Ostrom, "Toward a behavioral theory linking trust, reciprocity, and reputation" in Elinor Ostrom & James Walker, eds, *Trust and reciprocity: Interdisciplinary lessons from experimental research* (New York; Russell Sage Foundation, 2003) 19.

[152] Housen-Couriel, *supra* note 149 at 42.

Currently, the Taiwanese Administration has built a comprehensive information sharing mechanism, with institutions such as a national-level Information Sharing and Analysis Center, Computer Emergency Response Team, and Information Security Control Center in eight critical infrastructure domains, linking governmental agencies and critical infrastructure providers.[153] According to the "Cyber Security Management Act," agencies should implement cyber security threat detection and defense mechanisms.[154] The Taiwanese Administration has also established a national monitoring center, to detect and analyze abnormal network activities, and strengthen the governmental agencies' security. Other regulations include the "Notification and Response of Cyber Security Incident"[155] and the "Cyber Security Incident Reporting and Response Procedures." Additionally, for the private enterprises that fall outside the scope of the "Cybersecurity Management Act," it is covered by Taiwan Computer Emergency Response Team / Coordination Center for incident response and information sharing.

A critical next step is to establish a local chapter of the Space Information Sharing and Analysis Center (Space ISAC), the equivalent of the US Cybersecurity and Infrastructure Security Agency. The Space ISAC serves to:

> facilitate collaboration across the global space industry to enhance our ability to prepare for and respond to vulnerabilities, incidents, and threats; to disseminate timely and actionable information among member entities; and to serve as the primary communications channel for the sector with respect to this information.[156]

A chapter in Taiwan means fostering a collaborative environment where local space industry stakeholders can share critical information, enhance cybersecurity measures, and build a resilient infrastructure. This local chapter would act as a coordination hub, ensuring that Taiwan is well-prepared to address the unique challenges of space governance.

---

[153] Administration for Cyber Security, MODA, "Cyber Security Incident Reporting and Response", online: <moda.gov.tw/en/ACS/operations/notification-and-response/656>.

[154] *Cybersecurity Management Act,* (2018), Laws and Regulations Database of the Republic of China (Taiwan), online: <law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=A0030297>.

[155] *Regulations on the notification and response of Cyber Security Incident*, (2021), Laws and Regulations Database of the Republic of China (Taiwan), online: <law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=A0030305#:~:text=every%20six%20months.-,2.,required%20under%20the%20preceding%20paragraph.>.

[156] "Space Information Sharing and Analysis Center", online: <spaceisac.org/>.

For policy analysis, one research mechanism to coordinate the different sharing practices is through Governance Knowledge Commons (GKC) research. Ostrom explored knowledge commons later in her career, collaborating with Charlotte Hess. Together, they explore the differences between artifacts, facilities, and ideas.[157] Further, a group of scholars — Brett Frischmann, Michael J. Madison, Madelyn Sanfilippo, and Kathy Strandburg — contributed to the development of a broader research program called the GKC Research Coordination Network, where they define knowledge commons as "the institutional approach (commons) to governing the management or production of a particular type of resource (knowledge)."[158] As explained by Madison, GKC-based research looks for instances of "shared knowledge, information, and data that prompt the need for, even the demand for, governance mechanisms for people to get along in creating, using, and storing it."[159]

Taiwan's policy on information sharing can be examined through the knowledge commons framework by breaking down a question into clusters of related questions that can be asked and answered in a systematic way.[160] Questions include how we define a community or collective that produces or manages that data, and how is that community structured and organized? What are the various rules and social norms that define the resource, shape the community, and determine how the resource is produced and managed, presumably in response to governance challenges? What are the expected and unexpected outcomes associated with the practice of the rules and norms of space governance?

D. TAIWAN'S CYBERSECURITY CULTURE

Taiwan should advance cybersecurity culture as part of its process of building digital resilience. Cybersecurity culture are the norms from industries to individuals to governments on best cybersecurity practices. In the context of polycentric governance, cybersecurity culture can be understood as a set of rules manifested as either formal regulations or informal social norms and values through industry.

---

[157] Charlotte Hess & Elinor Ostrom, eds, *Understanding knowledge as a commons: from theory to practice* (Cambridge; MIT Press, 2007); Charlotte Hess & Elinor Ostrom, "Ideas, Artifacts, and Facilities: Information as a Common-Pool Resource" 66:11 Law and Contemporary Problems 111.

[158] Brett M Frischmann, Michael J Madison & and Katherine J Strandburg, eds, *Governing Knowledge Commons* (Oxford; Oxford University Press, 2014); "The Knowledge Commons Research Framework", online: <knowledge-commons.net/research-framework/>.

[159] Michael J Madison, "Knowledge Commons Past, Present, and Future" (2024) 28 Lewis & Clark L Rev 303.

[160] *Ibid*.

Companies, acting as decision making centers, naturally possess a rich blend of valuable skills and native knowledge to tackle various challenges. It is essential to address issues close to these communities, acknowledging the potential for solutions rooted in local expertise. One mechanism to foster a cybersecurity culture is for local industries to develop a voluntary cybersecurity framework specifically tailored to space-based infrastructure. This approach emphasizes a bottom-up, rather than a top-down approach. One example is the cybersecurity framework published by the National Institute of Standards and Technology (NIST) in the US.[161]

In Taiwan, the National Institute of Cyber Security (NICS) is a newly created entity under the Ministry of Digital Affairs, established in 2023.[162] The goal of the Institute is to work with local businesses to "[b]uild a World-class Scientific Research Team in Cyber Security Resilience and a Secure, Assured, and Stable Digital Environment." What is unique about NICS is that it is structured as a non-departmental public body, a semi-official institution within the government system of Taiwan.[163] This new arrangement gives the institution both the characteristics of a legal entity, under a corporate structure, with the goal of achieving specific public administrative objectives. NICS should create voluntary cybersecurity frameworks for space-based infrastructure, analogous to the cybersecurity framework created by NIST. Other examples include Japan's "Guidelines on Cybersecurity Measures for Commercial Space Systems," advising important risk scenarios and outline necessary attack mitigation measures, with the purpose of encouraging businesses to take voluntary cybersecurity measures.[164] A voluntary cybersecurity framework should be established through an inclusive and transparent process, bringing together stakeholders from the private sector, civil society, and government. Industry groups, with their deep understanding of best practices, can lead the way in crafting local rules, which can then be refined and enforced to ensure broad compliance and effectiveness.

Taiwan could produce its own manual on how cybersecurity and international law intersect, without including new rules. Some call this the "manual approach," which manifests the unique development of

---

[161] "National Institute of Standard and Technology", online: <www.nist.gov/>.

[162] National Institute of Cyber Security, "About Us", online: <www.nics.nat.gov.tw/en/about/introduction/>.

[163] *Act for the Establishment of the National Institute of Cyber Security,* (2022), Ministry of Digital Affairs: Laws and Regulations Retrieving System, online: <law.moda.gov.tw/EngLawContent.aspx?lan=E&id=4>.

[164] Tepper et al, *supra* note 123 at *30.

international law[165] - notable examples include the San Remo Manual on International Law Applicable to Armed Conflict at Sea,[166] the Harvard Manual on International Law Applicable to Air and Missile Warfare,[167] the Tallinn Manual on International Law Applicable to Cyber Warfare[168] and the McGill Manual on International Law Applicable to Military Uses of Outer Space (MILAMOS).[169] By initiating its own manual within the region, Taiwan can contribute to the global discourse on space-based infrastructure and cybersecurity while safeguarding its own interests in the increasingly contested domain of space. A manual on space-based infrastructure and cybersecurity could be developed within a university setting, serving as a bridge between academia and local industry. Universities, with their capacity to organize workshops, conferences, and collaborative policy analysis sessions, can play a crucial role in enhancing regional dialogue. This collaboration between academia and industry would not only support the creation of a manual but also position Taiwan as a key player in the global conversation on space and cybersecurity governance. Leading this initiative would allow Taiwan to ensure its viewpoints and priorities are reflected in the international legal framework, while also cultivating a well-informed community of experts equipped to address the complex challenges in these fields.

V. CONCLUSION

Taiwan needs to adopt a polycentric approach to build resiliency to its space-cyber infrastructure governance. We must ensure our space governance institutions are capable of quick and effective responses. Recognizing the nature of space-based infrastructure as a complex system, and drawing on Elinor Ostrom's theory on polycentric governance, may offer guidance. Taiwan, standing at a critical moment, has the potential to explore innovative, adaptive governance structures. While we cannot know the full impact of current policy decisions on future space governance, we can create specific institutional adaptations to address the unique challenges of outer space.

---

[165] *Ibid* at 39.

[166] International Humanitarian Law Databases, "San Remo Manual on International Law Applicable to Armed Conflicts at Sea, 12 June 1994", online: <ihl-databases.icrc.org/en/ihl-treaties/san-remo-manual-1994>.

[167] *HPCR Manual on International Law Applicable to Air and Missile Warfare* (Cambridge; Cambridge University Press, 2013).

[168] Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2d ed (Cambridge; Cambridge University Press, 2017).

[169] "Manual on International Law Applicable to Military Uses of Outer Space", online: <www.mcgill.ca/milamos/>.