For Dr. Bill Martel

Here We Go Again: A Comparative Approach to Developing an International Cyberspace Governance Framework

Introduction

As humanity develops technologies that enable it to accomplish new feats and reach previously inaccessible places, new forms of conflict typically follow. New potentialities often lead to struggles over distributions of gains, competition for resources, and disputes about how to guide and restrain novel human activities. This chapter seeks to draw insights for cyberspace from the process of developing global governance frameworks for outer space.

Cyberspace is distinct from land, sea, air, and outer space because it requires human-made electronics, which can be constantly redesigned and reprogrammed, in order to exist. Although other domains can be altered by humans to some degree, cyberspace's greater capacity to morph, grow, and be shaped by different groups with varying agendas adds several layers of complexity.

Different domains and their associated threat landscapes differ significantly, but systemic human factors that lead to disputes, conflict, and war change little across space and time. Among them are the mutual fear and suspicion inherent in the security dilemma;[1] questions about who determines rules of behavior in the international system;[2] authority and control, particularly relating to jurisdiction, liability, and dispute resolution;[3] negative externalities;[4] desires to preserve one's identity, culture, and way of life as well as in-group, out-group frictions;[5] free rider and collective action dynamics;[6] and unrestrained ambition. However, the physics of different domains vary, which limit what is technically feasible and dictate how certain desired outcomes can and cannot be achieved. In other words, people fight with each other for many deeply ingrained reasons, but the specific ways they do so change over time, especially as technology changes.

Philosopher John Dewey observed in 1935, "We are always dependent upon the experience that has accumulated in the past and yet there are always new forces coming in, new needs arising, that demand, if the new forces are to operate and the new needs to be satisfied, a reconstruction of the patterns of old experience."[7] In this sense, the Internet, wireless and space-based communications, fiber optics, and increasingly powerful computers, sensors, transmitters,

[1] John Herz, "Idealist Internationalism and the Security Dilemma," *World Politics*, vol. 2, no. 2 (January 1950): 157-180; Robert Jervis, "Cooperation under the Security Dilemma," *World Politics*, vol. 30, no. 2 (January 1978):167-212; Charles Glaser, "The Security Dilemma Revisited," *World Politics*, vol. 50, no. 1 (October 1997): 171-201; and Adam Liff and G. John Ikenberry, "Racing Toward Tragedy? China's Rise, Military Competition in the Asia Pacific, and the Security Dilemma," *International Security*, vol. 39, no. 2 (Fall 2014): 52-91.

[2] Robert Gilpin, *War and Change in World Politics* (New York: Cambridge University Press, 1981): 34-35.

[3] Stephen Krasner, *Sovereignty: Organized Hypocrisy* (Princeton, New Jersey: Princeton University Press, 1999): 10-42.

[4] Ronald Coase, "The Problem of Social Cost," *Journal of Law and Economics*, vol. 3 (October 1960): 1-44.

[5] Richard Ned Lebow, "Identity and International Relations," *International Relations*, vol. 22, no. 4 (December 2008): 7-8.

[6] Mancur Olson, *The Logic of Collective Action: Public Goods and the Theory of Groups* (Cambridge, Massachusetts: Harvard University Press, 1965).

[7] John Dewey, *Liberalism and Social Action* (Amherst, NY: Prometheus Books, 2000, 1935), 55.

and algorithms that enable all sorts of previously unthinkable feats are new forces in society that require “a reconstruction of the patterns of old experience.”

Today, world society is experiencing disputes as well as forms of crime and conflict between states, between non-state actors and states, and among non-state actors that are playing out in cyberspace, with increasingly damaging and potentially escalatory effects. Due to their novelty and the diminished importance of geography and distance due to cyberspace, the structures of human government are having difficulty adapting. Analyzing outer space as a point of comparison for cyberspace is instructive due to the similar institutional frameworks that existed when they first generated broad concern. The challenges posed by outer space and modern cyberspace confronted humanity when the primary political bodies of human government were states, loosely woven together by regional organizations and the United Nations, which remains so today. Transnational networks, non-governmental organizations, and multi-national corporations have become increasingly influential in managing human affairs since World War II, but the monopoly on the legitimate use of force, the power to make and enforce laws and treaties, and the power to tax reside with states.

The term *cyberspace* generates confusion, and various understandings of it continue to circulate. However, it has recently been adopted by many state institutions and appears to be entering the broader lexicon. This chapter utilizes Daniel Kuehl’s definition in *Cyberpower and National Security*, with a slight modification. Kuehl defined cyberspace as “A global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to *capture or* [added by author] create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies.”[8] Adding the verb “capture” reflects the capacity of information-communication technologies to take photographs and videos, record sounds, sense smells, detect chemicals and heat levels, track heartbeats, measure wind speed and light intensity, etc. The information exists in the world independently of cyberspace, but once an electronic device has captured it, that information can be stored, transmitted, modified, exchanged, and exploited.

Outer space is conceptually easier to grasp than cyberspace, but it is not as simple as it may seem. This chapter defines it as the space beyond Earth’s atmosphere and in between other celestial bodies. However, drawing a precise line where outer space begins from Earth’s perspective can be difficult and has significant implications for space vehicles and satellites. Of course, satellites and space vehicles rely on cyberspace to receive communications from each other and Earth-based command centers, which are transmitted through radio waves to their electronic systems.

Most technologies have multiple uses. Some are designed for military purposes, whereas others are initially designed for commercial or social purposes, but how these technologies are ultimately used or perceived depend to a degree on political circumstances. Despite a proliferation of international institutions and efforts to strengthen international law since WWII, a mutual perception of threat and potential for escalation are often necessary for states to negotiate on contentious political issues with security implications. In order to comprehend new threats and opportunities such as those presented by cyberspace or outer space, one must

[8] Daniel Kuehl, “From Cyberspace to Cyberpower: Defining the Problem,” in Kramer, Starr, and Wentz (eds.), *Cyberpower and National Security* (Washington, DC and Dulles, VA: National Defense University Press and Potomac Books, Inc.), 28.

understand the relevant scientific aspects of the domain and the technologies that permit its use. In the case of outer space, these include physics, engineering, rocketry, and propulsion, among others. For cyberspace, they also include physics and engineering, but with a greater focus on the electromagnetic spectrum, computational sciences, microchip manufacturing, and software engineering. One must also contemplate how utilizing these domains alter interpersonal, societal, and international dynamics. This is necessary in order to develop mutually understood international behavioral norms and laws that enjoy broad legitimacy, and which allow for peaceful, coordinated, and productive use of the domain while also punishing transgressors.

This chapter argues that the process of developing such international governance frameworks is characterized by the interplay of strategic rivalry, technological advancement, economic ambitions, security concerns, and international dialogue. Competitive pressures drive development of technologies and tactics, which, in turn, open up new possibilities for various actors to engage in conflict. Moreover, desires to employ new technologies for economic and social benefits drive their development and adoption, which may unintentionally create vulnerabilities in societies. New capabilities and behavioral changes sometimes increase tensions and elicit responses from other actors, which can fuel security dilemma dynamics. Domestic political systems and economic considerations shape preference formation at the international level. International institutions, interaction, and strategic dialogue among allies, rivals, and neutral parties help develop mutually understood terminology, situation definitions, conceptual frameworks, and norms through both analogic and inductive reasoning. Importantly, the process is iterative and never complete.

The chapter concludes that work at the UN on cyberspace is less robust than it was for outer space, which slows preference formation and fragments dialogue. The remainder of the chapter is a comparative analysis of dynamic processes of creating international governance frameworks for outer space and cyberspace, with a focus on security concerns. It seeks to illustrate the broader context while drawing on examples and research to describe and explain patterns, trends, and trajectories. It is necessarily a simplified model of complex reality.[9]

Outer Space Geopolitical Context, Threats, and Opportunities

The 1950s through 1980s were characterized by intense military, economic, and political competition between the United States and Soviet Union, with proxy wars and near-confrontations but also periods of détente. This bipolar power structure divided the world into states that were either aligned with one of the superpowers or non-aligned. The North Atlantic Treaty Organization (NATO) linked the United States and its Western European allies, whereas the Soviet Union relied on the Warsaw Pact to bind Eastern European countries to it.

Nuclear weapons are inextricably linked to human activity in outer space because the possibility of their delivery through outer space was contemplated by political and military leaders from the beginning. In the early outer space years, geopolitical tensions combined with uncertainty about technical possibilities and related military doctrines to generate fears of worst-case scenarios.

[9] This analysis is inevitably U.S.-centric given that the author is an American citizen and has lived in Washington, DC since 2011. All efforts have been made to be a neutral observer, but human biases, both known and unknown, can never be completely eliminated.

The Soviet launch of Sputnik in October 1957, the first human-made satellite to reach orbit, marked a turning point when theoretical discussions about human activity in outer space became reality. Moreover, the same missile technology that delivered Sputnik to outer space could also be used to send missiles through outer space and hit cities and military installations from a previously unimaginable distance. Prior to the Soviet launch of the first inter-continental ballistic missile (ICBM) in August 1957, the most effective way to deliver a nuclear warhead was by airplane or cruise missile, both of which required greater proximity to the target than an ICBM. This limitation allowed for more advanced warning and the possibility of shooting down bombers or destroying nearby missile launchers, a feat easier than intercepting an ICBM launched from within enemy territory on a different continent. In 1960, the United States successfully launched the first submarine-launched ballistic missile (SLBM), adding a third effective delivery mechanism to the nuclear arsenal. The Soviet Union sent the first man into outer space in 1961, followed closely by the United States in 1962, which opened new theoretical possibilities for space-based warfare.

Though development of missile technologies was primarily driven by militarized superpower competition, satellites promised immense possibilities for global communications and remote sensing. Once the capacity to put them in orbit was developed, governments and telecommunications companies quickly sought to use them for scientific and commercial purposes, further stimulating development of missiles, satellites, and space vehicles. But there was no governance framework in place to manage the new domain. For example, "In 1960 AT&T filed with the Federal Communications Commission (FCC) for permission to launch an experimental communications satellite with a view to rapidly implementing an operational system. The U.S. government reacted with surprise – there was no policy in place to help execute the many decisions related to the AT&T proposal."[10] Moreover, distinguishing civilian technology development and testing from military research was nearly impossible because advances in one field were easily transferable to the other.

Even after the advent of satellites, ICBMs, and SLBMs, it took years of debate, experimentation, strategic analysis, and learning before states formed preferences regarding the outer space domain. As professor James Clay Moltz observed, the United States and Soviet Union tested nuclear weapons nine times in outer space between 1957 and 1962, which emitted damaging electromagnetic pulse radiation. "By the fall of 1962, however, the two sides had begun to recognize that nuclear testing and unfettered military competition in space had self-damaging consequences for both sides and increased the possibility of nuclear war. The Cuban Missile Crisis stimulated a process of mutual learning that had already begun with regard to space."[11]

Meanwhile, U.S. civilian strategists had been developing new strategic understandings of nuclear deterrence throughout the 1950s and 1960s that took into account new missile technologies, which influenced leadership and broader debates about outer space. Memorably dubbed the "Wizards of Armageddon" by journalist Fred Kaplan,[12] they engaged in dialogue with Soviet strategists and helped advance common understandings of strategic dynamics while

[10] David Whalen, "Communications Satellites: Making the Global Village Possible," NASA, last updated November 30, 2010, http://history.nasa.gov/satcomhistory.html.

[11] James Clay Moltz, "The Past, Present, and Future of Space Security," *Brown Journal of World Affairs*, vol. 16, no. 1 (Fall/Winter 2007): 188-9.

[12] Fred Kaplan, *The Wizards of Armageddon* (New York, NY: Simon and Schuster, 1983).

nuclear warheads were detonated around the world. Nuclear arms control treaties were also negotiated in an effort to reduce testing and proliferation, such as the 1963 Limited Test Ban Treaty and the 1970 Nuclear Non-Proliferation Treaty. The outer space governance framework was laid down in this tense, militarized context in which fears of mass destruction were quite real.

Outer Space Debates, Concepts, and Codification

The UN Committee on the Peaceful Uses of Outer Space (COPUOS) was formed as an ad hoc committee in 1958 and made permanent in 1959. It contains a scientific and technical subcommittee and a legal subcommittee. States haggled over the committee's balance between "East," "West," and non-aligned as well as mutually acceptable negotiating and voting procedures. Consisting of 24 member states in 1959, COPUOS prepared and presented numerous resolutions adopted by the UN General Assembly prior to completing the Outer Space Treaty (OST) in 1967. Years of debate and non-binding resolutions allowed governments to work toward consensus before committing to a binding treaty. The OST laid down core principles upon which outer space governance is built, including legal classification, liability, jurisdiction over objects and personnel, prohibition on placing weapons of mass destruction, and notification of activities. It is thin on details and was never intended to be the last step in the rule-making process. As historian Walter McDougall put it, "Space technology was moving very quickly; international legal committees move slowly. As specific uses and interests emerged, then nations could hammer out temporary conventions. But of the general charter for space, the spirit, not the letter, was the essence."[13]

Early on, the UN International Telecommunications Union (ITU) was empowered to regulate use of outer space radio waves and allocate orbital slots. Coordinated management of these rival resources is necessary to avoid overcrowding and collision as well as to control satellites and space vehicles.

As the process advanced at the UN and bilateral discussions, it was informed by debate among political and military elite, international lawyers, scientists, private telecommunications companies, and others about the potential implications of situation definitions and norms. Strategic thinking and ambitions were intertwined with rule-making. Classifying outer space, regulating satellites, and drawing a line between airspace and outer space were all informed by scientific realities, existing and potential capabilities, and the incentive structure that different definitions and rules would create. M.J. Peterson referred to this process as "The interplay of interest calculations and analogic reasoning."[14]

Early debates on outer space were speculative and dialectic due to novelty and uncertainty. A quote from a 1957 article by international lawyer Myres McDougal is illustrative:

> "With regard to outer space and customary international law, both Mr. Jenks, in a general way, and Professor Cooper, more specifically, have expressed the thought that the principle of the freedom of the seas appears to be the most relevant analogy… For a recoverable satellite it suffices to mention that there

[13] Walter McDougall, *The Heavens and the Earth: A Political History of the Space Age* (New York, NY: Basic Books, 1985), 419-420.

[14] Peterson, 68.

> is, of course, the possibility of unauthorized entry into traditional airspace of underlying states as well as of damage, and apprehension of damage, to structures on the earth."[15]

The urgency of building an outer space governance framework led to a decision to classify outer space by analogic rather than inductive reasoning. The threat of nuclear war made a slow, inductive process undesirable. Airspace analogies would have extended sovereign jurisdiction of states over their territory into outer space. Soviet leaders initially favored this approach because they were concerned about U.S. spy satellites over their territory, which could mean a loss of advantage in terms of intelligence-gathering because U.S. society was more open than Soviet society.[16] If airspace analogies were used, this would have established a right to shoot down U.S. satellites over their territory, even during peacetime.[17] Scientifically, extending airspace above territory did not make much sense because Earth's position is continuously shifting relative to specific portions of outer space.

High seas analogies implied defining outer space as a commons, including for spy satellites and in support of Earth-based military activities. These analogies by themselves also meant that the Moon and celestial bodies would be treated like islands, subject to appropriation into state domain by whoever established effective control, which could have led to intense competition. High seas analogies were eventually adopted for outer space, but were supplemented with analogies from the 1959 Antarctic Treaty when it came to the Moon and other celestial bodies, which prohibited "any measures of a military nature, such as the establishment of military bases and fortifications, the carrying out of military maneuvers, as well as the testing of any type of weapons."[18] This avoided creating a costly and destabilizing incentive structure and was also inspired by real-world similarities. As Peterson put it, "Both Antarctic explorers and astronauts needed a level of supply requiring large support teams and budgets. The relatively long distance from other continents and the difficulty of the climate meant that military and other installations would be hard to defend from attack."[19]

Delimiting the boundary between airspace and outer space was also debated. In scientific terms, there is no clear line dictated by nature where airspace ends and outer space begins. Concentrations of gases in Earth's atmosphere gradually thin out to the end of the exosphere at roughly 10,000 km distance from Earth, at which point the airless void of outer space begins. However, delimitation in legal terms aids in questions of jurisdiction and establishing rules for distinct types of spaces.

Some suggested the Kármán line of 100 km above sea level. This line is used by NASA and the World Air Sports Federation to determine "spaceflight" and is a rough estimate of the point below which significant lateral thrust is needed to maintain aerodynamic lift. But "such 'lines' were a function of velocity and therefore of technology, and were in no way innate."[20] If the line were set too high, satellites with an orbit dipping below the line could be shot down. If it

[15] Myres McDougal, "Artificial Satellites: A Modest Proposal," *The American Journal of International Law*, vol. 51 (1957): 75-76.
[16] William Burrows, *This New Ocean: The Story of the First Space Age* (New York, NY: The Modern Library, 1999), 338-339.
[17] Peterson, 50.
[18] Antarctic Treaty, Art. I (1).
[19] M.J. Peterson, *International Regimes for the Final Frontier* (Albany, NY: State University of New York Press, 2005), 56.
[20] Walter McDougall, 186.

were set too low, states would lose sovereign control over part of their airspace, which could lead to intrusive actions. Since few wanted to constrain future operations as capabilities advanced, the question was ultimately left undecided and remains so today, which is considered a weakness in the outer space governance framework.

Other issues included questions of liability, jurisdiction, coordination, and control. These were resolved in principle by assigning international responsibility and liability over objects and people to the states to which they were registered. For non-governmental entities, states retained jurisdiction over their activities depending on their nationality, whereas responsibility for activities of international organizations were jointly borne by the organizations and the states comprising them.[21] Subsequent treaties on the return of astronauts and space objects, liability, registration, and the Moon entered into force between 1968 and 1984, which further fleshed out principles adopted in the OST.[22]

Though the OST and subsequent outer space treaties lacked enforcement mechanisms, they codified principles that had emerged through years of debate and state practice. Political scientists Koremenos, Lipson, and Snidal argue that "Uncertainty is a frequent obstacle to cooperation, as is 'noise,' the difficulty of observing others' actions clearly. States are naturally reluctant to disclose vital information that could make them more vulnerable. Reducing uncertainty among participants is a major function of institutions."[23] Thus, among the most important initial functions of the OST was to reduce uncertainty in a volatile international environment by providing agreed-upon definitions and general behavioral guidelines. Moreover, negotiating processes entailed interaction and strategic dialogue, giving states a window into each other's minds.

In short, all actors were unsure how to treat the outer space domain and its associated set of threats and opportunities, nor did they know how others were thinking about it. Uncertainty about the goals, intentions, and strategic thinking of an adversary is typically destabilizing, but especially so when new technologies have recently altered the strategic landscape and rendered existing mental frameworks outdated. When the ramifications of agreeing to be bound by certain rules are unknown, there is an incentive to avoid making commitments while continuing to experiment with newfound capabilities. Thus, aside from the benefits of reaching agreed-upon rules and mutually understood concepts that helped guide policy, the process of creating an outer space governance framework helped mitigate security threats by reducing uncertainty and accelerating state preference formation through dialogue. Of course, international governance frameworks must be continuously refined.

Refining the Outer Space Governance Framework

[21] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, Arts. VI–VIII.

[22] The four other UN treaties include the Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space (1968); Convention on International Liability for Damage Caused by Space Objects (1972); Convention on Registration of Objects Launched into Outer Space (1976); and Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (1984).

[23] Barbara Koremonos, Charles Kipson, and Duncan Snidal, "The Rational Design of International Institutions," *International Organization*, vol. 55, no. 4 (Autumn 2001): 766.

As trends and incidents in outer space have generated new concerns, additional agreements, guidelines, and state practices have sought to reduce security risks and strengthen outer space governance. Efforts have focused on the threats of anti-satellite weapons (ASATs), proliferation of missile technology, and space debris.

The Anti-Ballistic Missile (ABM) Treaty was signed in 1972 between the Soviet Union and United States as the recent development of multiple independent targetable reentry vehicles (MIRVs) threatened to create a costly and destabilizing situation. With MIRVs, several nuclear warheads could be mounted on one ICBM, which could split off and hit multiple targets as the missile descended from outer space, making it harder for missile defense systems to shoot them down. Even absent MIRVs, advancing technology increased the possibility of shooting down incoming ICBMs with missile interceptors and created an incentive to make more ICBMs and warheads in order to ensure that some would reach their targets. MIRVs meant that missile defense systems would have to be even more robust. Thus, by allowing only two missile defense sites per country and obligating both sides not to interfere with national technical means of verification, the treaty helped generate greater trust and assurance of nuclear deterrence. It also prohibited sea-, air-, and space-based ABM systems, further limiting strategic competition.

As technological change and proliferation continued, concerns about spreading missile technology led the G-7 countries[24] to create the Missile Technology Control Regime (MTCR) in 1987, a voluntary effort to limit export of missiles and components. It eventually expanded to 34 members. MTCR's track record is mixed, but it has served as a forum for dialogue and norm development, such as defining "a nuclear-capable ballistic missile as one that could carry a 500-kilogram payload to a range of 300 kilometers."[25]

In 2002, with growing concerns about regimes such as Iran and North Korea, MTCR members established the International Code of Conduct against Ballistic Missile Proliferation (ICOC). The voluntary ICOC is open to all states and currently has 137 members. In addition to establishing controls on technology related to WMD-capable ballistic missiles, it includes transparency and confidence-building measures such as annual declarations and the imperative to "exchange pre-launch notifications on their Ballistic Missile and Space Launch Vehicle launches and test flights."[26] The ICOC also calls on members to ratify the Outer Space Treaty, Registration Convention, and Liability Convention, seeking to reinforce existing principles.

Significant concerns about the outer space framework emerged when China conducted a kinetic ASAT test against its own defunct weather satellite in 2007, hitting it with a missile, which created significant space debris. Though the Soviets conducted numerous ASAT tests between 1968 and 1982, no one had done so since the United States in 1985. The Chinese test "galvanized long-held U.S. military fears about the vulnerability of the satellites it relies on for global power projection."[27] This was followed by a U.S. ASAT demonstration, which shot down an unresponsive de-orbiting intelligence satellite in 2008, citing a safety risk if the satellite's hydrazine tank leaked or exploded over a populated area. It occurred low enough in the atmosphere for debris to quickly de-orbit and burn up. This could have been designed to

[24] Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States.

[25] Waheguru Pal Singh Sidhu, "Looking Back: The Missile Technology Control Regime," *Arms Control Today*, April 2, 2007.

[26] International Code of Conduct against Ballistic Missile Proliferation, Art. IV.i.3 (2002).

[27] Theresa Hitchens, "Debris, Traffic Management, and Weaponization: Opportunities for and Challenges to Cooperation in Space," *Brown Journal of World Affairs*, vol. 16, no. 1 (Fall/Winter 2007): 179.

strengthen norms about notification and consultation, to signal to Chinese leaders about U.S. capabilities, or both. As Moltz notes, "Whatever the true reason, Washington conducted the world's first advance consultation under Article IX of the Outer Space Treaty."[28]

Aside from risks posed by intentional satellite destruction, degradation, or incapacitation through ASATs, accumulation of space debris from decades of human activity in outer space is a growing concern. Spent rockets, defunct satellites, and even paint flecks threaten operational satellites through collision. The Inter-Agency Space Debris Coordination Committee was formed in 1993 by major world space agencies, which created debris-mitigation guidelines eventually adopted by the UN in 2008. These guidelines outline best practices for collision avoidance, reducing debris creation during operations, end-of-life procedures to remove satellites from optimal orbits, etc. In 2009, an accidental collision between the operational Iridium 33 communications satellite and the defunct Kosmos 2251 Russian spy satellite added more space debris and confirmed growing fears.

Other initiatives include a Prevention of an Arms Race in Outer Space (PAROS) process which has sought since 1981 to advance discussions at the UN Conference on Disarmament, and through transparency and confidence-building measures. PAROS includes a 2008 Sino-Russian proposal for a Treaty on the Prevention of the Placement of Weapons in Outer Space and the Threat or Use of Force Against Outer Space Objects. It grew out of Chinese and Russian fears after U.S. withdrawal from the ABM Treaty in 2002, which undermined the strategic logic of nuclear deterrence. Their fears were compounded by a 2006 National Space Policy that stressed U.S. freedom of unilateral action. This action-reaction feedback loop is putting outer space back in the realm of strategic, militarized competition, especially as geopolitical tensions have increased in recent years.

In 2008, the European Union proposed a Code of Conduct for Outer Space Activities, which provides detailed rules for specific situations. It has gone through numerous drafts and was endorsed in principle by the United States in 2012, pending modifications. Though imperfect, as Lucia Marta notes, "a Code today can facilitate the adopting of a Treaty tomorrow, or even the creation of customary international law."[29] Indeed, international lawyers Lyall and Larsen argue that certain elements of the OST have become customary international law, noting that numerous agreements "relating to space activities all proceed on the basis of the general principles of space law."[30] Such international norms are starting to emerge for cyberspace, but clear general principles of cyberspace law remain elusive.

Cyberspace Geopolitical Context, Threats, and Opportunities

Cyberspace lacks a clear pivotal moment like Sputnik, although revelations beginning in 2013 of widespread surveillance and other activities by the U.S. National Security Agency is a significant milestone. Cyberspace has existed for over a century and has played a supporting role in warfare in the form of radar jamming, communications interception, monitoring troop

[28] James Clay Moltz, *Crowded Orbits: Conflict and Cooperation in Space* (New York: Columbia University Press, 2014), 148.

[29] Lucia Marta, "The Hague Code of Conduct against Ballistic Missile Proliferation: 'Lessons Learned' for the European Union Draft Code of Conduct for Outer Space Activities," *European Space Policy Institute Perspectives*, no. 34 (June 2010): 2.

[30] Francis Lyall and Paul Larsen, *Space Law: A Treatise* (Farnham, United Kingdom: Ashgate Publishing, 2009), 79.

movements, remotely piloting aircraft, precision-guided munitions, etc. As Kuehl notes,[31] cyberspace came into being with the invention of the telegraph in 1837. This could be conceptualized as the Big Bang moment for cyberspace, meaning that it came into being and has been expanding in size and complexity ever since.[32]

For simplicity, this chapter considers the invention of the World Wide Web in 1989 as the beginning of the modern cyberspace era because it enabled the commercialization and growth of the Internet in society. The Internet is the most integral piece of cyberspace because it enables one global, interoperable network of computers and other electronics to exist through its shared protocols, root servers, unique names and numbers, and coordinated management. Separate computer networks exist, but distinct public networks for different states have not been created, although levels of content filtering and activity monitoring vary in different states.

The modern cyberspace era was initially characterized by the end of the Cold War and a period of triumphalist sentiment in the "West." The Warsaw Pact crumbled, but NATO expanded eastward as did the European Union. In recent years, however, geopolitical tensions have grown. The 2014 Russian invasion and annexation of Crimea, followed by support for separatists in Eastern Ukraine, brought NATO-Russia relations to their most tense since the Cold War.

Chinese military strategy and modernization of forces focused on anti-access/area denial capabilities in response to a sense of encirclement led U.S. strategists to develop the Air/Sea Battle Concept, arguably stoking a security dilemma as both sides boost capabilities and put war plans on paper.[33] Though it is the job of militaries to prepare for all contingencies, perceptions of threat often grow when potential adversaries become aware of an opposing party's new plans and capabilities. The United States has been refocusing economic and military attention toward the Asia-Pacific since 2011, known as the "Pivot to Asia."[34] Tensions in the East and South China Seas between China and neighboring states over islands and maritime borders have fueled an arms race as well as increased U.S. support for countries such as Japan, the Philippines, and Vietnam. Of particular concern is China's construction of islands with military-capable installations in the South China Sea.[35]

The 2011 Arab Spring revolts against dictatorships in the Middle East and North Africa and subsequent government crackdowns ushered in greater instability, violence, and ungoverned spaces in that region. They also generated fears of similar uprisings among Russian and Chinese leadership, especially given the efficient coordination among citizens within and across Arab societies enabled by modern cyberspace through social media and mobile devices.[36] The Syrian

[31] Kuehl, 30.

[32] The author thanks Matt Herbert for this metaphor.

[33] Ayush Midha, "Lessons in Avoiding a U.S.-China War: Rethinking the Air/Sea Battle," *Harvard Political Review*, December 17, 2015, http://harvardpolitics.com/united-states/lessons-avoiding-u-s-china-war-rethinking-airsea-battle/.

[34] "We're Back: America Reaches a Pivot Point in Asia," *The Economist*, November 19, 2011, http://www.economist.com/node/21538803.

[35] Helene Cooper and Jane Perlez, "White House Moves to Reassure Allies With South China Sea Patrol, but Quietly," *New York Times*, October 27, 2015, http://www.nytimes.com/2015/10/28/world/asia/south-china-sea-uss-lassen-spratly-islands.html.

[36] Jonathan Pollack, "Unease from Afar," in *The Arab Awakening* (Washington, DC: Brookings Institution, November 2011), http://www.brookings.edu/~/media/research/files/articles/2011/11/18-arab-awakening-china-pollack/18-arab-awakening-china-pollack.pdf; Bruce Etling, "The Russian Media Ecosystem and the Arab Spring,"

civil war that began in 2011 became a broader proxy conflict between regional Middle East powers, while providing enabling conditions for the rise of the terrorist group Daesh, which conquered parts of Iraq in 2014.

These and other conflicts present an array of existing and potential threats apart from the death and destruction that has already occurred. Nuclear, biological, and chemical weapons remain significant concerns. Like with outer space, human activity in cyberspace is shaped by the broader political and technological environment. Geopolitical rivalry, threats posed by non-state actors, domestic politics, and desires to stay one step ahead of potential adversaries drive development of increasingly sophisticated computer network attack and surveillance capabilities. However, rather than a "Sputnik moment" that marked a clear *before* and *after* space flight, whose security implications were immediately clear because of the kinetic and nuclear implications of rockets and space vehicles, the security implications of cyberspace gradually sunk into public consciousness. Whereas early strategic thinking about outer space was primarily driven by fears of potential worst-case scenarios involving nuclear weapons, modern cyberspace has been shaped by numerous instances of actual harm in addition to fears of potential worst-case scenarios.

In terms of actual harm, examples include the "I Love You" virus, unleashed by a 24-year-old Filipino man in 2000, which infected roughly 50 million computers and caused an estimated $10 billion in damage.[37] Increasingly frequent corporate data breaches and identity theft throughout the 2000s raised awareness of dangers. Chinese hackers, some with links to the People's Liberation Army, have for years been stealing personnel records, intellectual property, weapons designs, and other data from U.S. computer networks. The 2007 distributed denial of service (DDoS) attacks on Estonia, which temporarily disabled financial, media, and government websites in the country, demonstrated a new type of threat. The attacks are widely assumed to have been at least partially directed by the Russian state, and they ushered in what political scientist Lucas Kello called "a wholly new type of social and economic disturbance."[38] Operation Olympic Games, the assumed U.S.-Israeli cyberattacks that caused physical destruction in Iran's nuclear facility at Natanz and other locations, began to leak out in 2010 as the Stuxnet virus spread to computers around the world. The 2012 Shamoon cyberattacks believed to have been conducted by Iran destroyed roughly 30,000 computers at Saudi Aramco. The 2014 cyberattack on Sony Pictures Entertainment in the United States stole and published proprietary information and internal communications in addition to destroying computers and servers, which the United States publicly accused North Korea of and imposed economic sanctions in retaliation.[39]

With regards to potential worst-case scenarios, U.S. President Barack Obama explained in February 2015, "We're hugely vulnerable. We've started with critical infrastructure. That's an area where heavy involvement with those industries — whether it's Wall Street and the financial

Internet & Democracy Blog at Harvard University's Berkman Center, May 18, 2011, http://blogs.law.harvard.edu/idblog/2011/05/18/russian-media-ecosystem-arab-spring/; and Chrystia Freeland, "Arab Spring, Russian Winter," *Reuters*, December 16, 2011, http://blogs.reuters.com/chrystia-freeland/2011/12/16/arab-spring-russian-winter/.

[37] Mark Landler, "A Filipino Linked to 'Love Bug' Talks About His License to Hack," *New York Times*, October 21, 2000.

[38] Lucas Kello, "The Meaning of the Cyber Revolution," *International Security*, vol. 38, no. 2 (Fall 2013), 24.

[39] Carol Lee and Jay Solomon, "U.S. Targets North Korea in Retaliation for Sony Hacks," *Wall Street Journal*, January 3, 2015, http://www.wsj.com/articles/u-s-penalizes-north-korea-in-retaliation-for-sony-hack-1420225942.

sector, utilities, our air-traffic control system — all of that, increasingly, is dependent on the digital base that they're working off of."[40] In a 2015 book, *Lights Out*, journalist Ted Koppel highlighted a long-held fear that cyberspace could be used to knock out the U.S. electric grid for weeks or months, resulting in mass death and destruction. He also pointed to concern among U.S. military planners that an electromagnetic pulse (EMP) attack, perhaps through high-altitude detonation of a nuclear weapon over U.S. territory, could result in "destruction of electronic equipment over an extremely wide area."[41] Of course, U.S. offensive cyberspace capabilities are assumed to be the best in the world, meaning that U.S. political and military leaders are acutely aware of what may be achievable. Moreover, other states are equally if not more vulnerable than the United States, depending on the degree to which their economies and societies rely on modern cyberspace in order to function.

As in the early outer space years, demonstrations of capabilities and provocative actions have led to reactions, mutual learning, and dialogue regarding cyberspace. The U.S. electric grid's vulnerability has been known for over a decade, but public awareness and policy responses have grown as hackers linked to Iran, Russia, China, and non-state actors such as Daesh are discovered penetrating computer systems that operate the grid and lay the groundwork for a potential cyberattack (known in military circles as "preparing the battlefield"). The 2007 DDoS attacks on Estonia sped the creation of the NATO Cooperative Cyber Defence Center of Excellence (CCDCoE) in 2009.[42] The speed of protestor mobilization demonstrated by the Arab Spring led Russia, China, and other less open states to tighten control of information flowing through their portions of cyberspace and also proposed in September 2011 a draft International Code of Conduct for Information Security at the UN,[43] which was updated in 2015.

Iran and North Korea have likely learned from U.S. cyberattacks, including ones believed to have been conducted under Olympic Games such as Stuxnet, Flame, Wiper, and Duqu. The 2012 Shamoon and 2014 Sony Pictures cyberattacks appear to have been inspired by the Wiper cyberattack on Iran's oil industry. As journalist Kim Zetter explained, "Regardless of whether Iran is behind the Shamoon attack, there's no question that it and other nations learn from cyberattacks launched by the US and its allies. Common cybercriminals also study Stuxnet and the like to learn new techniques for evading detection and stealing data."[44]

Soon after the 2013 NSA leaks began, many governments pushed for data localization in an effort to protect their citizens and sovereignty. This would have required major tech companies to store data for their nationals within their territory. But European calls for "technological sovereignty," Brazil's temporary flirtation with data localization in the context of Marco Civil legislation,[45] and similar initiatives around the world often betrayed a lack of technical understanding of cyberspace akin to the early outer space years because *where* data is

[40] Barack Obama, "The Re/Code Interview," interview with Kara Swisher, February 13, 2015, http://recode.net/2015/02/15/white-house-red-chair-obama-meets-swisher/.

[41] Ted Koppel, *Lights Out* (New York, NY: Crown Publishers, 2015), 21.

[42] Robert McMillan, "NATO to Set Up Cyber Warfare Center," *Network World*, May 15, 2008, http://www.networkworld.com/article/2279535/lan-wan/nato-to-set-up-cyber-warfare-center.html.

[43] See, for example, Timothy Farnsworth, "China and Russia Submit Cyber Proposal," *Arms Control Today*, November 2, 2011, https://www.armscontrol.org/act/2011_11/China_and_Russia_Submit_Cyber_Proposal.

[44] Kim Zetter, "The NSA Acknowledges What We All Feared: Iran Learns from US Cyberattacks," *Wired*, February 10, 2015.

[45] Tim Ridout, "Marco Civil: Brazil's Push to Govern the Internet," *Huffington Post*, October 22, 2013, http://www.huffingtonpost.com/t-a-ridout/brazils-push-to-govern-the-internet_b_4133811.html.

stored matters less for data security and privacy than *how* it is stored and transmitted. Other reactions included the Global Commission on Internet Governance (GCIG) chaired by former Swedish Foreign Minister Carl Bildt, established in January 2014.[46] In December 2013, U.S.-based tech companies announced the formation of the Reform Government Surveillance coalition, seeking to pressure the U.S. government and other governments to update laws and practices.[47]

Demonstrated capabilities help drive a cyber arms race that includes more than five dozen countries seeking military-cyber operations.[48] Unlike outer space, lower barriers to entry mean that weaker states and non-state actors can have significant impact in cyberspace. The complexity of modern cyberspace and the vast spectrum of conflict it enables make it a more difficult domain to understand than outer space. When cyberspace was primarily a means to communicate information quickly across distances through networked electronics, disruption to those systems did not present a significant security threat. However, cyberspace security concerns have grown as it has become clear that a range of actors can hack directly into modern systems through an ever-expanding global, interoperable computer network and remotely issue commands to computer-operated machinery and infrastructure on different continents that can cause physical destruction. Moreover, growing dependence on cyberspace opens new vectors for attack and theft while also increasing the potential magnitude of harm to society that can be inflicted through cyberspace.

Even as dangers grow in cyberspace, desires to utilize it for commercial, scientific, and social purposes continue to drive technological advancement and adoption, as with satellites and missile technology. For example, MIT scientist Alex Pentland has helped develop a discipline he calls "social physics," which utilizes cyberspace to map billions of human interactions in organizations and societies in order to track the flow of ideas and identify patterns. With the knowledge garnered, he hopes to "begin to build a society that is better at avoiding market crashes, ethnic and religious violence, political stalemates, widespread corruption, and dangerous concentrations of power."[49] Manufacturing could increasingly be customized through 3-D printing, placing a higher proportion of value-added in digital design and distributed services relying on cyberspace.[50] Significant potential also exists for the Internet of Things, smart grids, cloud computing services, and smart cities. By computerizing and adding sensors to nearly everything and connecting them to the global network that is the Internet, it would be technically possible to significantly reduce inefficiencies in energy usage, traffic patterns, and financial markets while also opening new social and commercial possibilities.

As with outer space, these and other possible future scenarios affect behavior today, both in terms of ambition to innovate and commercialize as well as protect against emerging threats and prepare for worst-case scenarios, but the difficulty of distinguishing between potentially

[46] Michelle Dobrovolny, "Commission Seeks New Ways to Govern the Internet," *SciDev.Net*, July 29, 2014, http://www.scidev.net/global/icts/news/commission-seeks-new-ways-to-govern-the-internet.html.

[47] Jon Swartz, "Tech Giants Team Up to in Anti-Snooping Effort," *USA Today*, December 10, 2013, http://www.usatoday.com/story/tech/2013/12/09/google-microsoft-facebook-others-form-reform-government-surveillance-coalition/3914697/.

[48] Shane Harris, "China Reveals Its Cyberwar Secrets," March 18, 2015, http://www.thedailybeast.com/articles/2015/03/18/china-reveals-its-cyber-war-secrets.html.

[49] Alex Pentland, *Social Physics* (New York, NY: Penguin Books, 2014), 17.

[50] Alfredo Valladão, *Masters of the Algorithms: The Geopolitics of the New Digital Economy from Ford to Google* (Washington and Rabat: The German Marshall Fund of the United States and OCP Policy Center, May 2014).

destructive activities and more benign ones fuels security dilemma dynamics. Though the cyberspace governance framework is more advanced today than the outer space framework was in 1960, it is a patchwork of specific conventions and agreements that have been adopted as opportunities and threats have arisen. It has not kept pace with the increasing size and complexity of modern cyberspace.

Cyberspace Debates and Concepts

Much like the early outer space years, many governments do not have a good understanding of modern cyberspace's scientific and technical properties or clear preferences regarding aspects of its use. Potential threats and opportunities are poorly understood, as are the ways modern cyberspace has altered social and strategic dynamics. There is no well-established lexicon. Cyberspace classification and situation definitions are poorly formed and there is no clear set of agreed principles governing its use that enjoys international political legitimacy.

Whereas the ITU was empowered to manage outer space radio frequencies and orbital slots, the Internet Corporation for Assigned Names and Numbers (ICANN) is the primary technical body for the Internet. Created in 1998, ICANN manages the domain name system and is responsible for *Internet governance*, a term often confused with debates about norms and laws regarding cyberspace. ICANN operates through a multi-stakeholder governance system that includes "owners and operators of servers and networks around the world, domain name registries, regional IP address allocation organizations, standards organizations, Internet service providers, local and national governments, noncommercial stakeholders, business users, intellectual property interests, and others." [51] ICANN still has a link to the U.S. government by virtue of the Internet Assigned Numbers Authority (IANA) functions contract with the U.S. National Telecommunications and Information Administration (NTIA), which is transitioning the contract to the global Internet multi-stakeholder community.

Given the Internet's central role in modern society, questions about its engineering are inherently political. As Internet-enabled cyberspace continues to supplant previous means of carrying out basic social functions in areas such as banking, commerce, healthcare, and government services, cyberspace is increasingly required to participate in society; thus, age-old questions of legitimacy, representation, and preference-aggregation are becoming more prevalent. Unlike the multi-stakeholder model, the United Nations is based on multilateral engagement between states, although states are free to appoint experts of any background as their representatives on UN committees. Lu Wei, Chinese minister of the Cyberspace Administration, has offered the predominant Chinese view on the competing models: "These two alternatives are not intrinsically contradictory. Without 'multilateral,' there would be no 'multi-stakeholders.' Exaggerating our disagreements due to difference in concepts is neither helpful to the China-U.S. Internet relations nor beneficial to global governance and development of the Internet."[52]

U.S. preference for the multi-stakeholder model could be explained by the logic of a "two-level game" described by political scientist Robert Putnam: "At the national level, domestic groups pursue their interests by pressuring the government to adopt favorable policies, and

[51] Lennard Kruger, *The Future of Internet Governance: Should the U.S. Relinquish Its Authority Over ICANN?* (Washington, DC, Congressional Research Service, May 5, 2015), 1.

[52] Lu Wei, "Cyber Sovereignty Must Rule Global Internet," *The Huffington Post*, December 15, 2014, http://www.huffingtonpost.com/lu-wei/china-cyber-sovereignty_b_6324060.html.

politicians seek power by constructing coalitions among those groups. At the international level, national governments seek to maximize their own ability to satisfy domestic pressures, while minimizing the adverse consequences of foreign developments."[53] The U.S. position is undoubtedly influenced by the libertarian ethos of people that built the Internet and spread it commercially, which is mistrustful of government and values freedom to innovate over order and security.

Aside from disagreement over how to manage the Internet, ambiguity regarding situation definitions, lexicon, and strategic dynamics in cyberspace inhibits efforts to lay down principles. General Michael Hayden, former director of the NSA and the CIA, argued in 2011, "Our most pressing need is clear policy, formed by shared consensus, shaped by informed discussion, and created by a *common* body of knowledge. With no common knowledge, no meaningful discussion, and no consensus… the policy vacuum continues."[54] A similar sentiment was echoed by current NSA Director and Commander of Cyber Command Admiral Mike Rogers in February 2015: "The concepts of deterrence in the cyber domain are still relatively immature. We clearly are not, I think, where we need to be."[55]

The *Tallinn Manual on the International Law Applicable to Cyber Warfare*, published by CCDCoE in 2013, is an effort to create situation definitions and apply the Law of Armed Conflict and International Humanitarian Law to cyberspace. Though criticized as insufficient to address the novel challenges of cyber conflict and for its lack of input from Russia and China,[56] the *Tallinn Manual* has informed cyberspace debates regarding international conflict. A second edition, *Tallinn 2.0*, is due out in 2016. International lawyer Michael Schmitt, editor of the manuals, argued in a 2015 article with Sean Watts that states have largely ceded debates to non-state entities on how International Humanitarian Law applies in cyberspace, indicating inchoate preferences and a desire not to constrain operations prematurely.[57]

A shared lexicon is lacking within countries as well as internationally. In common parlance in the United States and elsewhere, different people and professional communities use terms such as *online*, *the Internet*, *the virtual world*, *digital technologies*, *the web*, *information and communications technologies (ICTs)*, *cyberspace*, *information security*, *cybersecurity*, *network security*, and so on. Many of these terms refer to similar concepts, but consensus on appropriate verbiage and definitions are lacking. However, different concepts exist within cyberspace debates.

One source of confusion and disagreement is over *cyberspace/cybersecurity* and *information space/information security*. In Russian and Chinese conceptions, information space includes the cognitive effects of information on the population and the resultant social effects. "The Chinese view 'information space' as a domain, or landscape, for communicating with all of the world's population. This chimes with the Russian view of this space including human

[53] Robert Putnam, "Diplomacy and Domestic Politics: The Logic of Two-Level Games," *International Organization*, vol. 42, no. 3 (summer 1988): 434.
[54] Michael Hayden, "The Future of Things 'Cyber,'" *Strategic Studies Quarterly*, vol. 5, no. 1 (Spring 2011): 5.
[55] Michael Rogers, remarks at "Cybersecurity for a New America" conference, Washington, DC, February 23, 2015.
[56] See, for example, Ashley Deeks, "Tallinn 2.0 and a Chinese View on the Tallinn Process," *Lawfare*, May 31, 2015, https://www.lawfareblog.com/tallinn-20-and-chinese-view-tallinn-process.
[57] Michael Schmitt and Sean Watts, "The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare," *Texas International Law Journal*, vol. 50, symposium issue no. 2 (2015): 223-224.

information processing, in effect cognitive space."[58] Thus, *information security* in this conception refers not only to computer, network, and data security; it also encompasses information intended for human consumption – i.e., content. Therefore, questions of public morals, coordinating action between citizens, and government criticism are included, whereas the concept of *cybersecurity* leaves these aside. Ironically, U.S.-based tech companies frequently invoke *information security*, but their conception focuses on protecting information from theft, alteration, or destruction. Once that information is intentionally sent by its owner into public cyberspace, they would be loath to see it controlled by anyone, especially a government.

Within the *information space* debate, professors Andrey Krutskikh and Anatoly Streltsov have stressed the need for clarifying definitions internationally. They refer to "information war" as defined in the 2009 Agreement between the Governments of the Member States of the Shanghai Cooperation Organization in the Field of Ensuring International Information Security, which includes "mass psychologic brainwashing to destabilize society and state, as well as to force the state to taking decisions in the interest of an opposing party."[59] Krutskikh and Streltsov discussed disruption of air control systems, missile defense, and critical infrastructure, which are included in *cybersecurity* debates. But they also referred to the unlawful use of ICTs in which "physical damage is difficult to assess since losses are often intangible," noting the damage caused by mass theft and publication of information.[60]

Despite different terminology and concepts, democratic societies control certain types of information sent through cyberspace such as those involving defamation of character, incitement to violence, providing material support to criminal or terrorist groups, and Holocaust denial. They are more permissive about free expression, but they monitor and control their information space. Indeed, uses of cyberspace by Daesh to raise money and engage directly with Americans has led the FBI to increasingly monitor Twitter, prompting questions such as: when do "retweets" become criminal acts?[61] Given that modern cyberspace emerged in the United States, the Internet and business models that have built computer operating systems, software, and social media platforms reflect U.S. democratic ideology and culture, a source of friction in managing global cyberspace. Thus, more authoritarian societies tend to slow or block U.S.-inspired models. As Timothy Thomas argued in 2001, "Russia lost an ideology and is working hard to ensure that Russian culture, identity, and spirit do not also disappear along with it."[62]

Given differing views on information space, more authoritarian societies perceived Secretary of State Hillary Clinton's January 2010 "Internet Freedom" speech as provocative. An

[58] Keir Giles and William Hagestad II, "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English," in Podins, Stinissen, and Maybaum (eds.), *2013 5th International Conference on Cyber Conflict* (Tallinn, Estonia: NATO CCD COE Publications, 2013), 7.

[59] Shanghai Cooperation Organization, *Agreement between the Governments of the Member States of the Shanghai Cooperation Organization in the Field of Ensuring International Information Security [unofficial translation]*, Yekaterinburg, June 16, 2009, Annex 1, https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf.

[60] Andrey Krutskikh and Anatoly Streltsov, "International Law and the Problem of International Information Security," *International Affairs: A Russian Journal of World Politics, Diplomacy and International Relations*, no. 6 (2014): 67-68.

[61] See, for example, Ryan Reilly, "FBI: When It Comes to @ISIS Terror, Retweets = Endorsements," *The Huffington Post*, August 7, 2015, http://www.huffingtonpost.com/entry/twitter-terrorism-fbi_55b7e25de4b0224d8834466e.

[62] Timothy Thomas, "Information Security Thinking: A Comparison of U.S., Russian, and Chinese Concepts," *Foreign Military Studies Office Publications* (July 2001): 4.

agenda that includes "supporting the development of new tools that enable citizens to exercise their rights of free expression by circumventing politically motivated censorship"[63] can be seen as fomenting revolution within more closed societies that have a less permissive culture towards freedom of expression and assembly.[64]

With regards to classification, a 2014 GCIG paper by political scientist Joseph Nye used inductive and analogic reasoning to conceptualize cyberspace. It exhibited the same speculative, dialectic style characterizing articles such as the one by Myres McDougal in 1957:

> "The cyberspace domain is often described as a public good or a global commons, but these terms are an imperfect fit. A public good is one from which all can benefit and none should be excluded, and while this may describe some of the information protocols of the Internet, it does not describe the physical infrastructure, which is a scarce proprietary resource located within the boundaries of sovereign states and more like a 'club good' available to some, but not all. And cyberspace is not a commons like the high seas, because parts of it are under sovereign control. At best, it is an 'imperfect commons' or a condominium of joint ownership without well-developed rules."[65]

Whereas Nye's discussion sought to understand social dynamics within the domain (classification questions), Lu Wei has sought to establish clear jurisdiction over portions of the domain that correspond to territorial boundaries (delimitation questions). Conveying the official position of the Chinese government, he has argued that "cyber sovereignty" must dictate management of the global Internet.[66] Michael Chertoff and Paul Rosenzweig, also writing for GCIG, offered another perspective in 2015 on jurisdiction based on the assumption of an open, borderless Internet. They proposed a "choice-of-law rule based on either: the citizenship of the data creator; the citizenship of the data subject; one based on the location where the harm being investigated has taken place; or one based on the citizenship of the data holder or custodian."[67] These debates are similar to haggling over classification and delimitation of outer space in the 1950s and 1960s, but the complexity of cyberspace dynamics appear to make a slower, inductive process more likely than an analogic one.

The primary UN body charged with developing a framework for cyberspace is the Group of Governmental Experts on the Developments in the Field of Information and Telecommunications in the Context of International Security (commonly referred to as the GGE). GGE is roughly equivalent to COPUOS in its early years but, unlike COPUOS, the GGE has not been charged with laying the groundwork for a formal treaty and is not permanent.

The GGE first met in 2004-2005. At the conclusion of its third iteration in 2012-2013 it issued a report determining that international law, particularly the UN Charter, is applicable in

[63] Hillary Clinton, "Remarks on Internet Freedom," The Newseum, Washington, DC, *U.S. Department of State transcript*, January 21, 2010, http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

[64] Richard Andres, "Inverted Militarized Diplomacy: How States Bargain with Cyber Weapons," *Georgetown Journal of International Affairs: International Engagement on Cyber IV* (October 2014): 124.

[65] Joseph Nye, "The Regime Complex for Managing Global Cyber Activities," *Global Commission on Internet Governance Paper Series: No. 1* (Waterloo, Canada and London, UK: Centre for International Governance Innovation and Chatham House, May 2014), 6.

[66] Wei.

[67] Michael Chertoff and Paul Rosenzweig, "A Primer on Globally Harmonizing Internet Jurisdiction and Regulations," *Global Commission on Internet Governance Paper Series: No. 10* (Waterloo, Canada and London, UK: Centre for International Governance Innovation and Chatham House, March 2015), 2.

the "ICT environment."[68] The GGE's 2015 report used the term *cyberspace* for the first time and elaborated on how international law applies to cyberspace and the ICT environment. Though the GGE's work is not binding, it constitutes an effort to build an international governance framework for cyberspace, elements of which could be codified in a treaty at some point.

One emerging international cyberspace norm is that the same rights that people enjoy offline must also be protected online.[69] It can be found in the UN resolution put forth by Brazil and Germany in 2013 on The Right to Privacy in the Digital Age, in the 2015 draft of the International Code of Conduct for Information Security, the 2014 EU Human Rights Guidelines on Freedom of Expression Online and Offline, and elsewhere. Another emerging norm involves state responsibility for activities originating within their territory. As the 2015 GGE report put it, states "should not knowingly allow their territory to be used for internationally wrongful acts using ICTs."[70] Of course, verifying whether states are aware of and have the capacity to halt these acts is difficult. Regardless of difficulties of implementation, the existence of these norms would help guide policy and facilitate dispute resolution by providing principles upon which to base specific actions.

Conclusion and Recommendations: Toward a UN Cyberspace Treaty

Although cyberspace still suffers from inchoate state preferences, lack of a shared lexicon, and significant uncertainty, the process of developing a cyberspace governance framework built on mutually understood international behavioral norms and laws is slowly advancing through an interdependence of strategic rivalry, technological advancement, economic ambitions, security concerns, and international dialogue.

It seems necessary to begin negotiations on an international cyberspace treaty at the United Nations that lays down core principles to guide action in this domain. As with the Outer Space Treaty, a cyberspace treaty would not be a panacea, nor would it be the end of the rule-making process. Concluding one would inevitably take years or decades, but putting in place core principles that outline a cyberspace governance framework from which future cyberspace law can derive would be valuable.

The process of negotiating a cyberspace treaty at the UN would facilitate purposeful interaction and idea exchange among states. Given geopolitical tensions partially fueled by conflict in cyberspace, working together on a common project would be a constructive exercise, providing a focal point in the world's primary global political body to slowly arrive at common understandings. It could stimulate work in other fora with cyberspace components, encouraging all stakeholders to transmit preferences to state leaders while accelerating debate and updates to legal frameworks within states. Negotiations could also facilitate strategic learning and discipline the cyberspace lexicon such that concepts of deterrence and awareness of potentially escalatory dynamics could more quickly mature. The GGE serves this purpose to a degree, but its ad hoc

[68] UN Res A/68/98, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," June 24, 2013,

[69] See, for example, Henry Rõigas, "An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New?" *InCyder News* (CCDCoE), February 10, 2015.

[70] United Nations, "Report of the Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/RES/70/174: Art. III.13.c, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

nature and ambiguity about its future signals a lack of importance from which COPUOS did not suffer, making it easier for states to engage in "forum shopping,"[71] which fragments dialogue and leads to confusion. A distinction should also be made between concepts of *Internet governance* (focused on technical management of one piece of cyberspace) and *cyberspace governance* (focused on the totality of the space created by networked electronics and the electromagnetic spectrum).

The legitimacy of a UN cyberspace treaty would generate greater "buy-in" around the world, and it would codify core principles that emerge from state practices and normative debate. Moreover, if and when a cyberspace treaty is concluded, it would create a shared reference of higher law that could be drawn upon to guide future action, resolve disputes, and address new challenges. Negotiating it could also reduce current uncertainty and resulting anxiety among leaders and populations about how to manage potential threats and worst-case scenarios, mitigating security dilemma dynamics.

A cyberspace treaty would have to consider the implications that might arise from uses of networked artificial intelligence, greater computerization of human bodies through mechanical limbs and organ-regulating devices such as heart monitors, direct brain-to-brain communication via the Internet,[72] and so on. It would have to address questions of jurisdiction, liability, and control, including how to manage threats posed by non-state actors. It would need to be simple enough so average citizens could comprehend the basic principles and broad enough to allow for future interpretation and evolution as technologies and norms change.

As we struggle with the challenges of modern cyberspace, wisdom from the early outer space years is worth revisiting: "Particular subjects may be dealt with by formal agreement… The remainder of what a future historian will—only in that future—be entitled to call 'The Law of Space,' when law is conceived as the community's expectations about the ways in which authority will and should be prescribed and applied, will undoubtedly grow by the slow building of expectations, the continued accretion of repeated instances of tolerated acts, the gradual development of assurances that certain things may be done under promise of reciprocity and that other things must not be done on the pain of retaliation."[73]

Cyberspace governance frameworks will inevitably evolve over time and will be guided by myriad actors and institutions, but without core principles and mental frameworks to help governments and other organizations understand where to focus energies and invest resources, it will be hard for anyone to adjust to the challenges of modern cyberspace.

[71] See, for example, Frank Baumgartner and Bryan Jones, *Agendas and Instability in American Politics* (Chicago: University of Chicago Press, 1993); and Alastair Johnston, "The Social Effects of International Institutions on Domestic (Foreign Policy) Actors," in Daniel Drezner (ed.), *Locating the Proper Authorities* (Ann Arbor, Michigan: University of Michigan Press, 2003), 145-196.

[72] See, for example, Andrea Stocco et al., "Playing 20 Questions with the Mind: Collaborative Problem Solving by Humans Using a Brain-to-Brain Interface," *PLOS ONE*, September 23, 2015, http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0137303.

[73] Myres McDougal and Leon Lipson, "Perspectives for a Law of Outer Space," *The American Journal of International Law*, vol. 52 (1958): 420.