CYBERSECURITY REGULATION: USING ANALOGIES TO DEVELOP FRAMEWORKS FOR REGULATION[173]

Julie J. C. H. Ryan[174], Daniel J. Ryan[175], Eneken Tikk[176]

Abstract

Cyberspace has been referred to as "wild, wild west" by a number of authors over past 20 years. The international cyber incidents witnessed by the international community in the past three years have awaked the international discussion on the regulation of the domain that is developing into a self-standing dimension of our daily life, national security and warfare. For the purposes of this article, cyberspace may be regarded as one of the great "commons". The purpose of taking this perspective is to evaluate the usefulness of the commons regulation analogy for resolving some of the issues nations and international community faces in regard to cyber security, and for guiding the development of a regulatory framework for cyberspace.

INTRODUCTION

A variety of analogies and metaphors have been proposed as aids for thinking about cyberspace and regulation of human behavior in cyberspace. For example, we talk about the information superhighway as a way of understanding traffic of

173 Opinions expressed in this paper are those of the authors and do not represent positions of George Washington University, or of the Information Resources Management College, the National Defense University, the Department of Defense, or the United States Government, or of the Cooperative Cyber Defence Centre of Excellence, the Government of Estonia, or NATO.
The following students performed research that informed our progress in writing this paper: James Allen, William Biggs, Joseph Bober, Earl Britt, Cynthia D. Brown, John Coller, Charles F. Hall, Daniel Jennings, Brenda Magente, Mark S. Mistal, Bruce W. Morris, Debora L. Nissenbaum, David B. Odom, Michael F. Pennock, Linda Snowden-Peninger, Timothy Potz, David W. Stickley, Linda Suppan, Stephen B. Sznajder, Uzill Weaver, and Howard G. W. Whyte.

174 Julie J. C. H. Ryan, Department of Engineering Management and System Engineering, School of Engineering and Applied Science, The George Washington University, Washington, D. C. 20052, USA, jjchryan@gwu.edu

175 Daniel J. Ryan, Department of Information Operations & Information Assurance, Information Resources Management College, National Defense University, Washington, D. C. 20319, USA, ryand@ndu.edu

176 Eneken Tikk, Legal Advisor / Head of Legal and Policy Branch, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, eneken.tikk@mil.ee

information across the World Wide Web. Even calling the Internet a "web" invokes a metaphor. Alternatively, cyberspace may be thought of as a *res communis*, a commons.[177] We know that men have been concerned with the regulation of the use of commonly owned resources since the dawn of history, and it is easy to imagine that such concerns predate historical records, since use of natural resources in prehistoric times must have required attention to who could use hunting and gathering territories, for example. Certainly the Greeks as early as the fifth century BCE were familiar with the problem. In 431 BCE, Thucydides wrote, "[T]hey devote a very small fraction of time to the consideration of any public object, most of it to the prosecution of their own objects. Meanwhile each fancies that no harm will come to his neglect, that it is the business of somebody else to look after this or that for him; and so, by the same notion being entertained by all separately, the common cause imperceptibly decays."[178] Eighty years later, Aristotle wrote, "That all persons call the same thing mine in the sense in which each does so may be a fine thing, but it is impracticable; or if the words are taken in the other sense, such a unity in no way conduces to harmony. And there is another objection to the proposal. For that which is common to the greatest number has the least care bestowed upon it. Each one thinks chiefly of his own, hardly at all of the common interest; and only when he is himself concerned as an individual. For besides other considerations, everybody is more inclined to neglect the duty to which he expects another to fulfill; as in families many attendants are often less useful than a few."[179] Two millennia later, in 1833, William Forster Lloyd, then Drummond Professor of political economy at Oxford, in attempting to refute Adam Smith's notion of a felicitous "invisible hand" that converted selfish behavior into common prosperity, coined the term "commons" to describe depletion of commonly owned resources through overuse due to maximization of short-term individual selfish interests.[180] In 1968, Garrett Hardin borrowed the term in his now-famous paper, "The Tragedy of the Commons."[181] Hardin's use of the term "tragedy" harkens back to the Greeks

177 See Peter Levine (Fall, 2001) Civic Renewal and the Commons of Cyberspace, *National Civic Review*, Vol. 90, No. 3. See also Dan Hunter (2003) Cyberspace as Place and the Tragedy of the Anticommons, 91 Cal. L. Rev. 439.

178 Thucydides, *History of the Peloponnesian War*, Book I, Sec. 141; translated by Richard Crawley (London: J. M. Dent & Sons; New York: E. P. Dutton & Co., 1910). Online at http://people.ucalgary.ca/~vandersp/Courses/texts/thucydi1.html#CH.V. Cited in Denmark and Mulvenon, p 44 n. 21. See also http://en.wikipedia.org/wiki/Tragedy_of_the_commons#References_to_the_Greek_classics.

179 Aristotle, *Politics*, Book II, Chapter III, 1261b; translated by Benjamin Jowett as The Politics of Aristotle: Translated into English with Introduction, Marginal Analysis, Essays, Notes and Indices (Oxford: Clarendon Press, 1885), Vol. 1 of 2. Online at http://classics.mit.edu/Aristotle/politics.2.two.html. Cited in Denmark and Mulvenon, p 44 n. 21. See also http://en.wikipedia.org/wiki/Tragedy_of_the_commons#References_to_the_Greek_classics.

180 *W. F. Lloyd on the Checks to Population. Population and Development Review*, Vol. 6, No. 3 (Sep., 1980), pp. 473-496. http://www.jstor.org/stable/1972412

181 "The Tragedy of the Commons," Garrett Hardin, Science, 162(1968):1243-1248.

notion of tragedy: "The essence of dramatic tragedy is not unhappiness. It resides in the solemnity of the remorseless working of things."[182]

Today there are many commons that may require regulatory attention. Grazing land may be publically owned, as in Lloyd's original exposition. Public facilities such as government buildings and land, parks, navigable waterways and the continental shelf may be considered commons. That body of knowledge residing in the public domain or the results of science and technology sponsored by the government may be thought of as commons. Oil, minerals, timber, and other resources found on or beneath public lands or under the surface of the sea comprise natural commons. The open seas, the atmosphere, outer space above the atmosphere, the Arctic icecap, the Antarctic continent, and the electromagnetic spectrum are resources owned in common by the citizens of the world.

States may try and control that portion of such commons over which they exercise jurisdiction, or may enter into international treaties for regulation of some commons or parts of commons. In other cases, individual entrepreneurs, private non-governmental organizations (NGOs) or corporations may seek to control and exploit parts of some commons for specific purposes or material gain.

Beginning with four nodes in 1969,[183] the wide area network-of-networks we call cyberspace[184] has grown and spread to become a commons, a critical infrastructure that is pervasive and upon which societies worldwide have become dependent for commerce, recreation, communication, delivery of government services, research, education and a host of other activities. United States President George W. Bush has said, "The way business is transacted, government operates, and national defense is conducted have changed. These activities now rely on an interdependent network of information technology infrastructures called cyberspace."[185] Cyberspace is our most recent commons,[186] but the problem of regulating human behavior in the use of commons is not, so we should be able to draw upon the lessons we have learned as we regulated behavior in other, earlier commons that can inform and facilitate the development of effective and efficient regulatory architectures for regulation of cyberspace.

182 Alfred North Whitehead, *Science and the Modern World* (Mentor, New York, 1948), p. 17. Cited in Hardin.
183 http://www.davesite.com/webstation/net-history.shtml
184 The term "cyberspace" was coined by the science fiction author William Gibson in his 1982 cyberpunk story "Burning Chrome."
185 http://georgewbush-whitehouse.archives.gov/pcipb/letter.pdf
186 Exactly when the cyberspace commons began depends upon the definition of cyberspace. The Internet arguably dates from December, 1969, but the use of technologies to facilitate communications and commerce arose much earlier. See Tom Standage (1998) *The Victorian Internet*. New York: Walker & Company. www.walkerbooks.com.

This is an ambitious undertaking. The best-known commons – the sea, the atmosphere, outer space, and Antarctica – have evolved comprehensive regulatory frameworks based on customary international law and treaties. Thus we have:

- The laws of the sea (maritime commons)
- Regulation of air traffic control (atmosphere commons)
- The Antarctic Treaties (Antarctic commons)
- Treaties controlling the use of outer space (extra-atmospheric commons)

Other regulatory frameworks may provide ways of better understanding how regulatory schema might evolve for cyberspace. These include, but are not limited to:

- The Laws of Armed Conflict (LOAC, or International Humanitarian Law)
- Environmental law
- Public health, epidemiological control and The World Health Organization (WHO)
- The World Intellectual Property Organization (WIPO) and control of intangible property
- Control of the electromagnetic spectrum
- Control of international commerce
- Water use regulation for non-tidal water
- Critical Infrastructure Protection (CIP) laws and regulations

We have the beginnings of a regulatory framework for cyberspace, including:

- Internet governance by NGOs[187]
- Cybercrime statutes at national levels[188]
- The European Cybercrime Convention[189]

But human occupation and use of cyberspace is relatively recent, and a comprehensive framework for regulation in cyberspace is still evolving. Each of the

187 See Milton Mueller (2004) *Ruling the Root: Internet Governance and the Taming of Cyberspace* . Cambridge, MA: MIT Press. See also http://www.ietf.org/ and http://www.icann.org/.
188 See, for example, http://www.law.cornell.edu/uscode/18/1030.html.
189 See http://conventions.coe.int/Treaty/EN/Treaties/HTML/185.htm . Also, http://epic.org/privacy/intl/ccc.html.

other commons and analogies may provide similes and metaphors that can inform and guide the evolution of rules for regulating human behavior in cyberspace.

Still, we must acknowledge at the outset that no analogy is perfect, and metaphors, while they can vividly illuminate areas of concern, can also mislead and confuse, even as they inform and guide. Therefore, as we explore these analogies and metaphors to glean guidance relevant to regulation of human behavior in cyberspace, we will maintain caution to avoid the fog of policy.

We will begin with the best known commons: the seas, the atmosphere, outer space and Antarctica.

THE LAW OF THE SEA

The seas constitute a commons that mankind has used for thousands of years for commerce, communication, and exploitation of the animals and plants it contains and of the minerals beneath the sea floors. Control of the use of the seas and its vast wealth is increasingly important as world population grows and per capita natural resources decline, both on- and off-shore.

Control of the seas has been contentious among European powers for well over five hundred years. Norway and Denmark claimed sovereignty over the Arctic Ocean (*Mare Septentrionale*) and Denmark and Sweden exercised control over the Baltic (*Dominium maris Baltici*).[190] Pope Alexander Borgia, to control access to the newly discovered Americas, arrogantly divided power over the ocean commons between Spain and Portugal in 1493, with a demarcation line 100 leagues west of the Azores.[191] All newly discovered lands west of the line were to be under Spanish control and all lands east of the line went to Portugal, and no other countries were allowed to sail to and trade with the new lands (*mare clausum*).[192] In the 17th century, Great Britain claimed control over a large area of the seas (*Oceanus Britannicus*). Needless to say, such claims led to much tension and outright conflict as the European powers tried to preserve the use of the sea to their country's military forces and commercial traders, while denying the use of sea lanes to their enemies.

In 1609, Hugo Grotius published his famous book *Mare Liberum*, promoting the principle of freedom of the seas. He argued that the seas were for the use of all, not subject to the control of a few strong nations. States that had coastlines were to

190 B. J. Theutenberg (1984) The Evolution of the Law of the Sea. Dublin: Tycooly International Publishing Limited, p. 1.
191 On June 7, 1494, the Treaty of Tordesillas moved the line to 370 leagues west of the Cape Verde islands, reserving Brazil to the Portugese and the rest of the New World to the Spanish. *Ibid.*
192 Theutenberg (1984).

be allowed control of a narrow strip of water along their coasts (territorial waters). Originally, territorial waters were conceived to be the part of the ocean that could be defended from shore – hence, one cannon shot in width. This distance was arbitrarily extended to 3 nautical miles (6 km) by several nations, including the United States, Great Britain and France. Iceland claimed two nautical miles, Norway four and Spain six. Late in the twentieth century, those claims were expanded by many nations to twelve nautical miles.[193]

The League of Nations made an attempt to develop a Law of the Sea Treaty in 1930, but the effort failed. In general, that part of the ocean that was not included in the territorial waters of some nation was available for use by anyone with a vessel (*usus publicus*), making international waters a commons. This principle was codified in the 1958 Geneva Convention on the High Seas.[194]

Claims to the right to control natural resources in and under the waters above the continental shelves adjacent to the land areas of nations were asserted by the United Kingdom and Venezuela, a claim espoused by the United States in 1945.[195] Control of the continental shelf was eventually codified in the Geneva Convention on the Continental Shelf in 1958.[196] The Third Conference on the Law of the Sea aimed to develop a comprehensive framework for regulating the utilization of the oceans and the seafloor. After fourteen years of work by 150 nations, the Conference adopted the United Nations Convention on the Law of the Sea Convention (UNCLOS) on December 10, 1982 at Montego Bay, Jamaica. UNCLOS codified the norms that had evolved over many years for controlling the use of the seas and the natural resources beneath the seabed. The Convention addressed for the first time environmental preservation and protection and deep ocean floor resources. UNCLOS was signed quickly by one hundred and nineteen states and finally came into force with ratification by 60 nations on November 16, 1994.[197] The UN says, "It is a complex and broad-ranging formulation of international law that seeks to regulate the world's oceans for the benefit of mankind.[198]"

193 While it is foreseeable that countries have different "cyber perimeter defense" capabilities, the principle of effective control could stress the responsibility of nation states to design information society so that it has the required level of security built in.
194 Theutenberg (1984).
195 *Department of State Bulletin*, September 30, 1945, p. 485.
196 Theutenberg, p. 2.
197 Conflicting interests, particularly regarding regulation of the use of deep seabeds, delayed the ratification of the Convention for many years after its signing in 1982. Eventually, in 1994, an agreement was reached on implementation of Part XI of the Convention, and the necessary 60 ratifications were attained. www.eoearth.org/article/United_Nations_Convention_on_Law_of_the_Sea_(UNCLOS),_1982.
198 United Nations Convention on the Law of the Sea of 10 December 1982- Overview and full text. (last updated January 8, 2010), Chapter 1 -3.

Today, the seas are divided into zones for purposes of regulation. The so-called "territorial waters" within twelve miles of the mean-low-water line of a coastal state are under the direct sovereign control of the state.[199] The air above these waters and the seabed below are also within the sovereign control of the state. Congruent with the territorial waters or perhaps as far as twenty-four miles beyond the mean-low-water line, a "contiguous zone" may allow a nation to exercise limited enforcements of customs, fiscal or immigration policies or sanitary laws. Finally, an exclusive economic zone is deemed to extend out to 200 nautical miles, and within that zone a costal nation can exercise control over all of the economic resources found there – living and mineral – and can regulate pollution of the waters within the zone. It may not, however, prohibit transiting of those waters by vessels in compliance with laws and regulations adopted by the costal nation in accordance with UN conventions.

The oceans outside of national jurisdiction are called variously "international waters", the "high seas", or *Mare Liberum*. Ships sailing on the high seas fall under the jurisdiction of their country of registry. The use of the high seas is subject to UNCLOS, especially Articles XII-XIV, and may also be subject to other global treaties and conventions, regional agreements such as those included in the Regional Seas Program of the United Nations Environment Programme,[200] or specific agreements for the use of certain bodies of water, e.g. the Helsinki Convertion on the Protection of the Marine Environment of the Baltic Sea.[201]

The seas and cyberspace share several important characteristics. Both are expansive domains in which humans can operate using specially designed and developed technologies. Neither is wholly contained within the sovereign territory of a single nation or small group of nations, and many nations profit from more or less simultaneous access to and free transit across these domains. Both require human investment of scarce resources to realize their potential, and both share analogous risks from property appropriation to criminal activity to warfare.

On the other hand, cyberspace, unlike the ocean, is mostly[202] manmade, and requires near-continuous human attention and support to remain functional. The seas have more-or-less well-defined boundaries related to topographically defined jurisdictions in physical space, while cyberspace has only weak connectivity to

199 If an overlap with another nation's territorial waters would occur, the boundary is taken to be the median points between the state's baseline mean-low-waters.
200 www.unep.org.
201 www.helcom.fi/Convention.
202 Certain portions of cyberspace use paths through the atmosphere and outer space for communications.

physical space.[203] And the technologies for using and exploiting cyberspace are evolving more rapidly today than those we use to take advantage of the oceans and the treasures beneath them.

AIR TRAFFIC CONTROL

One hundred years ago, airspace was mostly uncontrolled, as cyberspace is today. If you wanted to fly, you built or bought an airplane, studied (hopefully) how to take off and land and how to steer when airborne, and off you went. Neither flying nor airfields were subject to regulation. Today, flying, whether for recreation or for commercial purposes, is highly regulated, from licensing of pilots to safety of airplanes to use of airfields to transnational travel and commerce. How did this massive and pervasive regulatory structure evolve, and what lessons does it offer to us as we consider regulation of cyberspace?

Air traffic control rules are used to separate aircraft to prevent collisions and to organize and facilitate the flow of air traffic through the atmospheric commons. Some airspace is controlled (over national territories) and some is not (over international waters or Antarctica). Air traffic control activities may involve instructions to pilots that they are required to obey, or may merely provide information to pilots that does not involve mandatory instructions.

Heavier that air human flight began on December 17, 1903, when Orville and Wilber Wright made the first controlled, powered and sustained fixed-wing aircraft flight. In 1910, the first conference on regulation of the use of aircraft was held in Paris. By 1919, airplane use had grown to the point that international regulation was deemed necessary, and the International Commission for Air Navigation (ICAN) was created to develop rules for air traffic control. A Convention of forty-three articles, incorporating all of the principles discussed at the 1910 conference, was established to deal with technical, operational and organizational aspects of civil aviation.[204] The United States, still somewhat geographically isolated (at least in terms of air navigation), did not sign the ICAN Convention, developing its own rules somewhat later after the passage of the Air Commerce Act (ACA) of 1926. The ACA authorized the Department of Commerce to develop rules for air navigation, protection and identification of aircraft operating within the United States.

Early rules under the ACA in the United States focused on individual airport operations, but by 1935, the volume of air traffic had increased to a level that led

203 It is true that every computer, server, workstation and wire has some location in physical space, but these are largely transparent to transactions across cyberspace.
204 www.icao.int//cgi/goto_m.pl?icao/en/hist/history01.htm.

to coordination of traffic among airports. In December of 1935, the first air traffic control center opened at Newark, New Jersey. Additional centers at Chicago and Cleveland opened the next year. In July, 1936, en route air traffic control became a federal responsibility in the United States. In 1941, congress created the Civil Aeronautics Administration (CAA) to operate the air traffic control system. There were 155 air traffic control towers in the United States by 1944. By 1952, local radar was operational in the air traffic control system, and by 1956, and order for long-range radars for use in air traffic control was placed.

By the 1940's the volume of transnational air traffic to and from the United States made it clear that the United States and other nations could not continue to evolve independent and different air traffic control systems. On December 7, 1944, the International Civil Aviation Convention (commonly referred to as the Chicago Convention) was signed by 52 countries to create a common framework for control and regulation of air traffic. The 26th ratification occurred March 5, 1947, and the Convention became effective April 4, 1947. Since then, the Convention has been revised eight times to keep pace with the evolution of aircraft and aircraft control technologies and the increasing density of international air traffic. Today, air traffic control rules are managed by a United Nations Specialized Agency, the International Civil Aviation Organization (ICAO).[205] One hundred and ninety (190) states[206] worldwide follow ICAO rules in managing civil aviation within and between their national airspaces.

Like the seas, the atmosphere is divided into regions subject to different regulatory schemes. Some airspace is controlled – subject to Air Traffic Control regulations – and some is uncontrolled. The busy areas around airports are controlled to prevent collisions among planes. Specific rules apply to planes flying at cruising altitudes to expedite and maintain the orderly flow of air traffic, especially with regard to Instrument Flight Rules (IFR). Security is also important and certain areas are designated Air Defense Identification Zones (ADIZ). ADIZ are no fly zones with very strict rules. Altogether there are seven classes of airspace defined by the ICAO. They are designated A to G and ATC flight regulations take effect at E and progress in descending alphabetical order. Classes F and G are uncontrolled airspace. Not all countries use all seven classes of airspace in regulating air traffic above their territories.[207] Some airspace may be designated Special Use Airspace and is off limits for non-military aircraft. Special Use Airspace includes Prohibited Areas, Restricted Areas, Alert Areas, Warning Areas, and Military Operations Areas.[208]

205 www.icao.int.
206 www.icao.int/cgi/statesDB4.pl?en.
207 http://www.dicksmithflyer.com.au/airspace_categories.php.
208 http://quest.arc.nasa.gov/aero/virtual/demo/navigation/youDecide/airspace.html.

Both the atmosphere and cyberspace are extensive domains within which humans, using appropriate technology, can operate. Both are international in scope and use, with some areas within existing national jurisdictions and some areas outside of any national jurisdiction. Both have traffic flows that need to be controlled to facilitate transiting the domain.

While airspace is tightly connected to national jurisdictions and traffic is under the control of a specific jurisdiction when above a national jurisdiction, traffic in cyberspace is much less subject to such controls. Air traffic is tightly monitored and directed by the Air Traffic Control system; packets in cyberspace take unpredictable paths dictated by network routing protocols that can change dynamically in response to loading in ways that are not controlled or controllable by either the user or the nations the traffic paths traverse. Both planes and passengers are identified and tracked when they use airspace, but authentication and attribution of users of cyberspace is often impossible.

This analogy of cyberspace to the atmospheric commons leaves hope for those who argue that cyberspace has grown way over the head of the regulators. One could see the first wave of cyber domain regulation occur in early 90's. A revision of the original approaches has been undertaken in most countries during 2000-2005, but the occurrence of the Estonian case in 2007 clearly indicated that national homework regarding regulation of behavior in cyberspace is nowhere near to "done". Various entities and organizations are focusing on security standards for cyberspace – for example, IANA and ICANN deal with Internet assigned names and numbers or the domain name system, the European union has started a comprehensive information society development coordination effort, and the Council of Europe has contributed to the uniformity of criminal law in the field.

Thus, it would be unfair to conclude that from the regulatory perspective, the Internet is a sum zero. It is rather that some aspects of this traffic (such as national security emergency vehicles and "cyber tanks") have been left aside while others such "cargo flights" (business uses of the Internet) and some charter flights (e.g. personal data protection, consumer rights) have been heavily regulated. Furthermore, often regulation of the cyberspace domain has occurred on the national level and is thus subject to sovereignty ramifications. Private jets in the Internet are fairly easy to operate as the end users' rights have flourished under the regulation ruled by the human rights paradigm.

OUTER SPACE

Man began to explore and exploit the outer space commons just over a half

century ago: orbiting satellites, space stations and space laboratories, sending men to the moon and back, and launching deep-space exploration vehicles like Voyager 1 and 2.[209] Early efforts were undoubtedly driven by the competition between the United States and the, then, Soviet Union,[210] but with the first moon landing Neil Armstrong, saying "That's one small step for (a) man, one giant leap for mankind," made it clear that outer space is not the territory of one or a few countries, but the common territory of all.[211] "Outer space as a common territory beyond national jurisdiction is a "global commons" *par excellence*. Security must therefore be common, cooperative security, based on the rule of law and respect for international space law in the interest of all states and mankind as a whole."[212]

With the space race fully underway, the United Nations adopted its "Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space" in 1963.[213] The nine legal principles are:

1) The exploration and use of outer space shall be carried on for the benefit and in the interests of all mankind.

2) Outer space and celestial bodies are free for exploration and use by all States on a basis of equality and in accordance with international law.

3) Outer space and celestial bodies are not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means.

4) The activities of States in the exploration and use of outer space shall be carried on in accordance with international law, including the Charter of the United Nations, in the interest of maintaining international peace and security and promoting international co-operation and understanding.

5) States bear international responsibility for national activities in outer space, whether carried on by governmental agencies or by non-governmental entities, and for assuring that national activities are carried on in conformity with the principles set forth in the present Declaration. The activities of non-governmental entities in outer space shall require authorization and

209 National Aeronautics and Space Administration, Jet Propulsion Laboratory, Frequently Asked Questions, http://voyager.jpl.nasa.gov/faq.html.
210 On October 4, 1957, the then Soviet Union launched its Sputnik satellite, the first successful orbiting of a man-made satellite, and ushered in the Space Age.
211 Jones, Eric M. (1995) *One Small Step.* NASA's Apollo 11 Lunar Surface Journal. http://history.nasa.gov/alsj/a11/a11.step.html
212 Detlev Wolter (2003) *Common Security in Outer Space and International Law: A European Perspective,* p. 4.
213 http://www.oosa.unvienna.org/oosa/en/SpaceLaw/gares/html/gares_18_1962.html.

continuing supervision by the State concerned. When activities are carried on in outer space by an international organization, responsibility for compliance with the principles set forth in this Declaration shall be borne by the international organization and by the States participating in it.

6) In the exploration and use of outer space, States shall be guided by the principle of co-operation and mutual assistance and shall conduct all their activities in outer space with due regard for the corresponding interests of other States. If a State has reason to believe that an outer space activity or experiment planned by it or its nationals would cause potentially harmful interference with activities of other States in the peaceful exploration and use of outer space, it shall undertake appropriate international consultations before proceeding with any such activity or experiment. A State which has reason to believe that an outer space activity or experiment planned by another State would cause potentially harmful interference with activities in the peaceful exploration and use of outer space may request consultation concerning the activity or experiment.

7) The State on whose registry an object launched into outer space is carried shall retain jurisdiction and control over such object, and any personnel thereon, while in outer space. Ownership of objects launched into outer space, and of their component parts, is not affected by their passage through outer space or by their return to the earth. Such objects or component parts found beyond the limits of the State of registry shall be returned to that State, which shall furnish identifying data upon request prior to return.

8) Each State which launches or procures the launching of an object into outer space, and each State from whose territory or facility an object is launched, is internationally liable for damage to a foreign State or to its natural or juridical persons by such object or its component parts on the earth, in air space, or in outer space.

9) States shall regard astronauts as envoys of mankind in outer space, and shall render to them all possible assistance in the event of accident, distress, or emergency landing on the territory of a foreign State or on the high seas. Astronauts who make such a landing shall be safely and promptly returned to the State of registry of their space vehicle.[214]

The Declaration has since been supplemented by three resolutions laying down

214 *Ibid.*

the legal principles applicable to the exploration and exploitation of outer space,[215] the "Declaration on International Cooperation in the Exploration and Use of Outer Space for the Benefit and in the Interest of All States, Taking into Particular Account the Needs of Developing Countries,"[216] and five treaties and agreements governing the use of space and space-related activities.[217] These treaties, agreements and principles are collectively known as the "United Nations Treaties and Principles in Outer Space," which make access to and use of space available, limit the use of space to peaceful purposes (especially avoiding the weaponizing of space with nuclear[218] and other weapons of mass destruction, although not all weapons are banned from space, e.g. lasers or kinetic weapons), and fostering cooperation for the protection and recovery of astronauts. All of this was accomplished in spite of the fact that after more than twenty years of trying, there is still no accepted legal definition of "outer space."

In addition to United Nations Treaties and Principles in Outer Space efforts to regulate the use of outer space, other treaties and agreements offer additional regulations. Through the Convention of the International Telecommunications Union, the United Nations International Telecommunication Union "has coordinated the shared global use of the radio spectrum, promoted international

215 The Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting (resolution 37/92 of 10 December 1982), http://www.oosa.unvienna.org/oosa/en/SpaceLaw/gares/html/gares_37_0092.html; The Principles Relating to Remote Sensing of the Earth from Outer Space (resolution 41/65 of 3 December 1986), http://www.oosa.unvienna.org/oosa/en/SpaceLaw/gares/html/gares_41_0065.html; The Principles Relevant to the Use of Nuclear Power Sources in Outer Space (resolution 47/68 of 14 December 1992), http://www.oosa.unvienna.org/oosa/en/SpaceLaw/gares/html/gares_47_0068.html.

216 http://www.oosa.unvienna.org/oosa/en/SpaceLaw/gares/html/gares_51_0122.html.

217 The "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies" (the "Outer Space Treaty", adopted by the General Assembly in its resolution 2222 (XXI)), entered into force on 10 October 1967, http://www.oosa.unvienna.org/oosa/en/SpaceLaw/gares/html/gares_21_2222.html; the "Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space" (the "Rescue Agreement", adopted by the General Assembly in its resolution 2345 (XXII)), entered into force on 3 December 1968, http://www.oosa.unvienna.org/oosa/en/SpaceLaw/gares/html/gares_22_2345.html; the "Convention on International Liability for Damage Caused by Space Objects" (the "Liability Convention", adopted by the General Assembly in its resolution 2777 (XXVI)), entered into force on 1 September 1972, http://www.oosa.unvienna.org/oosa/en/SpaceLaw/gares/html/gares_26_2777.html; the "Convention on Registration of Objects Launched into Outer Space" (the "Registration Convention", adopted by the General Assembly in its resolution 3235 (XXIX)), opened for signature on 14 January 1975, entered into force on 15 September 1976, http://www.oosa.unvienna.org/oosa/en/SpaceLaw/gares/html/gares_29_3235.html; and the "Agreement Governing the Activities of States on the Moon and Other Celestial Bodies" (the "Moon Agreement", adopted by the General Assembly in its resolution 34/68), entered into force on 11 July 1984, http://www.oosa.unvienna.org/oosa/en/SpaceLaw/gares/html/gares_34_0068.html.

218 Although nuclear weapons are banned, it is recognized that some uses of nuclear power are needed in space, the Treaties and Principles provide for safety in its use, mitigation of risks, and liability for states that fail to control the nuclear power or its sources. http://www.unoosa.org/oosa/SpaceLaw/nps.html.

cooperation in assigning satellite orbits, worked to improve telecommunication infrastructure in the developing world, established the worldwide standards that foster seamless interconnection of a vast range of communications systems and addressed the global challenges of our times, such as mitigating climate change and strengthening cybersecurity."[219] The 1963 Partial Test Ban Treaty[220] prohibits the explosion of nuclear bombs in outer space. Multilateral and bilateral agreements and treaties, "such as the Convention of the European Space Agency in 1975, Arabsat in 1976, and EUMETSAT in 1983,"[221] may regulate the use of space among the parties to those agreements and treaties. Voluntary *schema* include the Missile Technology Control Regime (1987),[222] the Committee on the Peaceful Uses of Outer Space ("COPUOS"),[223] and the Global Exploration Strategy.[224] And, of course, Customary International Law applies.

Cyberspace and Outer Space share some interesting similarities. The use and exploitation of each is heavily technology-dependent. The inherent nature of each is only loosely related to traditional notions of territorial sovereignty. Although every computer, server and wire is located in some place subject to other regulatory frameworks, the paths by which packets travel across the Internet are largely beyond the control of the user and may pass through many different sovereign jurisdictions in route from sender to recipient. Spacecraft and satellites in orbit pass above many different sovereign jurisdictions and cannot avoid doing so, the laws of celestial mechanics being as they are. Thus, the notions of territorial control that apply well in the laws of the sea and the regulation of international air travel, do not apply well to outer space or cyberspace. If nations were allowed to exercise sovereign control over the use of outer space in the same way they exercise sovereign control of air traffic in the skies above their territories, it might be practically impossible to explore and use space at all. The same may apply to cyberspace.

Of course, despite their similarities, outer space and cyberspace are inherently different. One is real; the other virtual. Although cyberspace requires a physical medium, it exists within and among the components that comprise that medium, and as those components come and go, cyberspace expands and contracts. Cyberspace is polymorphic in ways that outer space is not. Disconnect the components and cyberspace evaporates; outer space is here to stay. These differences mean that, while a framework of principles, agreements and treaties

219 http://www.itu.int/net/about/index.aspx.
220 http://nuclearfiles.org/menu/library/treaties/partial-test-ban/trty_partial-test-ban_1963-10-10.htm.
221 Johnathan F. Galloway (2008) *Conference on Space and Telecommunications Law: Revolution and Evolution in the Law of Outer Space*, 87 Neb. L. Rev. 516.
222 http://www.mtcr.info/english/index.html. Cited in 87 Neb. L. Rev. 516.
223 http://www.oosa.unvienna.org/oosa/COPUOS/copuos.html. Cited in 87 Neb. L. Rev. 516.
224 http://www.nasa.gov/pdf/178109main_ges_framework.pdf. Cited in 87 Neb. L. Rev. 516.

may well serve to regulate behavior in cyberspace, they may not be the same principles, agreements and treaties that have evolved to control behavior in outer space. Professor Lessig[225] had it right when he told us that code *is* law, that the architecture of a place limits and enables the rules we can expect to work well in controlling behavior in those places. Differences in architectures require differences in rules of behavior. The trick is to use what is usable in common, without trying to use what is not.

MANAGING ANTARCTICA

We explore and use cyberspace from the comfort of our homes and offices. The seas, the air and outer space require that we create vessels that can sustain friendly environments around us as we traverse, use and exploit their resources. In some ways the most difficult of the great commons for humans to explore and use is the intensely cold and inhospitable Antarctic continent.

In 1773, James Cook circumnavigated Antarctica. Exploration of the Earth south of the Antarctic Circle began in earnest about 1820, when Russian, British, French and American teams began to visit the icebound region. February 7, 1821, saw the first landing on the continent by the American sealer Captain John Davis, the first of many visits by sealers and whalers. Later that year, ten British sailors and one officer were marooned and unwillingly spent the winter, the first winter-over by humans. By 1840, Antarctica was known to be a continent. In 1898, the first scientific expedition wintered over, also unwillingly. In 1902, Captain Robert Falcon Scott, with Ernest Shackleton and Edward Wilson, tried unsuccessfully to reach the South Pole. In 1907-9, Shackleton tried again and got within 156 km of the Pole. In 1909, Douglas Mawson reached the South magnetic pole, and, finally, in 1911, the Norwegian Roald Amundsen led a five-man team to the Pole itself.[226]

> Fortunately, scientific interests rather than political, economic, or military concerns dominated the expeditions sent to Antarctica after World War II. Fortunately, too, international scientific associations were able to work out arrangements for effective cooperation. In 1956 and 1957, for example, American meteorologists "wintered over" at the Soviet post Mirnyy, while Soviet meteorologists "wintered over" at Little America. These cooperative activities culminated in the International Geophysical Year of 1957-1958 (IGY), a joint scientific effort by 12 nations -- Argentina, Australia, Belgium, Chile, France, Japan, New Zealand, Norway, South Africa, the Soviet Union, the United Kingdom, and the United States -- to conduct studies of the Earth and its

225 Lawrence Lessig (1999) Commentary: The Law of the Horse: What Cyberlaw Might Teach. 113 Harv. L. Rev. 501. http://cyber.law.harvard.edu/works/lessig/LNC_Q_D2.PDF.

226 http://www.coolantarctica.com/Antarctica%20fact%20file/History/exploration%20and%20history.htm.

cosmic environment.[227]

Antarctica is a potentially rich source of natural resources. Platinum, copper, gold, iron ore, chromium and nickel, along with other minerals, have been discovered there. Hydrocarbons and coal appear only in small trace amounts. Most interesting, and perhaps ultimately most valuable, is that more than 70% of the world's fresh water supply is there. Of course, with all that valuable stuff about, as soon as it was possible to stay in Antarctica, countries began to claim territories there. Seven nations have made such claims, although the claims are not universally recognized as valid.[228] A legal framework was eventually constructed, entering into force in 1961, using a treaty – the Antarctic Treaty[229] – which neither recognizes nor disputes the territorial claims. The Treaty sets aside the continent as an area to be used only for peaceful purposes. Military activity is banned,[230] and freedom of scientific investigation and cooperation are required.

KEY LESSONS FROM REGULATION OF THE COMMONS

As noted *supra*, one must be careful in using analogies and metaphors for guidance. While they may inform and illuminate, no analogy or metaphor is a perfect fit. Surely there are ways in which the great commons are like cyberspace: each is a domain within which human activities transpire, for good or evil. Each relies upon and requires technology to enable the use and exploitation of the domain. Each offers benefits to those nations, organizations and individuals that can access them, and for each of the great natural commons, a regulatory framework has evolved that guides and controls human behavior within the commons. These likenesses offer the promise that analysis of their regulatory frameworks can guide and inform the development of a regulatory framework for cyberspace.

But we have also seen that there are significant differences among the commons and between each of the natural commons and cyberspace. The natural commons are all extensive in real space, while cyberspace (mostly) exists within a complex web of man-made wires, fiber optic cables, and electronic devices. Although these wires, cables and devices are each owned by someone and exist in real space with its developed legal jurisdictions, it is inherent in the design of the Internet that "location" in cyberspace is only loosely tied to real space in a detectable way, and so observed activities are difficult to attribute to specific individuals, organizations

227 http://www.state.gov/www/global/arms/treaties/arctic1.html.
228 https://www.cia.gov/library/publications/the-world-factbook/geos/ay.html.
229 http://www.state.gov/www/global/arms/treaties/arctic1.html.
230 Military personnel and equipment may be used for scientific research or any other peaceful purpose.

or nations. Distance in cyberspace seems unrelated to distance in real space, and the borders we so carefully defend in real space are effectively transparent in cyberspace. It follows inevitably that many of the schema and methodologies that serve us well in regulating the great natural commons are at least suspect, and may well be completely ineffectual, in cyberspace.

Nevertheless, we have seen that when nations perceive that it is in their common interest to develop internationally applicable regulatory frameworks, the means to do so exist. So, what might an effective international framework for regulation of behavior be like, given our experience with the frameworks guiding and regulating behavior in the great natural commons?

First, since every computer, system, server, wire and cable lies in or crosses existing jurisdictions in real space, the framework can and should, to the maximum extent possible, take advantage of those connections between cyberspace and real space. This follows the example of the laws of the sea and of the atmosphere, and implies that those portions of cyberspace that can be tied to nation-state jurisdictions will be subject to the laws of those jurisdictions, and that individuals and organizations who operate in cyberspace will be subject to the jurisdictions in which their operations take place. Making the laws of the various nations accessing, using and exploiting cyberspace coherent is a problem we will address in the next section of this paper. Even so, we recognize that even in real space some portions of the world are not subject to existing nation-state jurisdiction, and we must account for those portions of cyberspace that lie in international waters or in outer space, where international law applies, and develop appropriate rules for activities using those portions of cyberspace.

Second, we can develop a framework for regulating behavior in cyberspace that is as complex as it needs to be. As Albert Einstein famously said in another context, "Everything should be made as simple as possible, but no simpler."[231] The regulations for the law of the sea, for example, may be viewed as a transparency overlying real space: over land the laws of the relevant jurisdiction apply (except over Antarctica when jurisdiction is assigned by treaty), near to shore a slightly different set of rules apply, and beyond the near shore up to 200 miles from the coast still another set of rules applies, and then international law takes over for the high seas. Similarly, our framework need not consist only of hard-and-fast rules. In air traffic control, some communications relay binding instructions, while others are merely advisory. In cyberspace, we might want some hard requirements for implementation of policies, practices, procedures and technologies recognized to be effective in

231 http://rescomp.stanford.edu/~cheshire/EinsteinQuotes.html.

deterring, detecting and interdicting abuses and undesirable activities. In other cases, we may merely wish to inform users of steps and countermeasures they may wish to voluntarily take to enhance their own security and lessen their liability.

Third, we must recognize that the inherent nature of cyberspace and the media within which it exists limit our ability to regulate. As we saw in outer space, orbits necessarily cross borders and spaceflight would be impossible were concepts of sovereignty to permit nations to deny the users of space access to the portions of outer space above their territories like they can deny others the use of the atmosphere for airplane traffic above their territories. The routing of traffic through cyberspace is accomplished by algorithms largely beyond the control of those who access, use and exploit cyberspace. A framework in which Internet traffic could only pass through that portion of a nation's networks with the permission of that nation would render the Internet unusable.

The need for our framework to support free access and unhindered communications has especially interesting implications for cyberwar. All Internet communications must traverse various links and pass through various nodes as they travel from origin to destination. Since traffic is packetized, not all packets need pass through the same links or nodes. The user has little control over which links or nodes are used to complete the transmission. Civilian and military traffic share the same links and nodes, and military traffic – communications, espionage or information operations – may pass through links and nodes within the jurisdictions of belligerents, their allies, and neutral nations as well. The Internet protocols make no distinction among the users and their status with respect to cyberwar.[232] This makes cyberwar especially problematical with respect to the LOAC principle of distinction. The 1977 Additional Protocol I to the Geneva Convention[233] requires that parties to an armed conflict must distinguish between civilians and civilian property on the one hand, and combatants and military targets on the other, and that civilians and civilian property are forbidden targets. So called "dual-use" targets that serve both civilian and military purposes, now certainly including the Internet, may be attacked under certain circumstances:

> The answer depends on whether or not one applies Protocol I restrictions. If the [attacker is]is bound by Protocol I, a case can be made that such attacks are illegal, but the issue is very subject to interpretation. Let us consider the case of an attack upon an adversary's electrical system. Presuming that the justification of the attack is to destroy or degrade the adversary's military capability, then civilians are neither the "object of attack" nor is the primary purpose of the attack to "terrorize" them. Nevertheless, such an attack may violate Protocol I's provisions if it is indiscriminate

232 106 Mich. L. Rev. 1427, 1433.
233 http://www.icrc.org/ihl.nsf/COM/470-750073?OpenDocument.

> and/or if the incidental civilian effects are disproportionate to the concrete and direct military advantage of the attack. One can argue that such an attack is indiscriminate because it employs a method or means of combat (strategic attack of electrical generation facilities) the effects of which cannot be limited to the purely military objective. As a result, such an attack does not distinguish between military and civilian effects. Given this secondary, incidental effect upon civilians, one must apply the rule of proportionality, weighing the incidental effects on civilians with the concrete and direct military advantage the attack gives. Here there is divergence of view. [Cites Matthew C. Waxman, International Law and the Politics of Air Operations (Santa Monica, CA: Rand, 2000), 22.] The more restrictive view is that only direct civilian injuries, deaths, or destruction, namely those that occur immediately as a direct result of the attack (for example, from the explosion itself), should be considered. The second view is that all indirect civilian effects, namely those that occur over time as an indirect effect of the attack (for example, from loss of electricity) should also be considered. If one accepted the indirect view, then it might be very difficult to find a concrete and direct military advantage that outweighed the tens of thousands of civilian deaths that might be indirectly caused from loss of electricity. On the other hand, if one accepts only the direct view, such attacks would be very easy to justify provided one uses precision methods of attack. In sum, if one is bound by Protocol I, the legality of attacking dual-use targets is very much a matter of interpretation, as the disparity in views between the direct and indirect civilian effects creates a vast gray area in the law.
>
> If a state is bound by The Hague and Geneva Conventions but not Protocol I (like the US, for example), then the case against attack of dual-use targets is even weaker. Precision attack on an electrical facility doesn't rise to the level of "indiscriminate" or "wanton" destruction specified by The Hague and Geneva Conventions. Nor does it count as "willful killing" or "willfully causing great suffering or serious injury" to civilians because the harm to civilians is incidental to the military objective. Even if the incidental harm to civilians is significant, allowance for military necessity essentially neuters the civilian protections of the Conventions.[234]

So for an electrical facility, so for an Internet node.

As to the use of cyber versus kinetic weapons for the attack, international law does not turn on the nature of the weapon, but on the effect of the attack. If the attack takes place in cyberspace, should responses then be limited to cyber responses? After the Estonian incident, NATO took it as a rude awakening and started trying to figure out the implications of cyber incidents. They were thankful that Estonia did not exercise Article 5, but fully recognized that, had the Estonians done so, NATO would have been in a terrible position. If cyber incidents are sufficient to trigger Article 5, NATO could have ended up at war with Russia over the cyber attack on Estonia.

Following the Estonian and Georgian incidents, NATO has been working busily

234 http://www.airpower.au.af.mil/airchronicles/cc/Rizer.html

since trying to get new and improved doctrines in place so that future incidents are handled appropriately. They seem to be leaning toward a doctrine that asserts that cyber incidents are not "armed attacks" justifying kinetic responses and full application of the Laws of Armed Conflict. That position has interesting consequences. If a cyber incident is not an "attack" then, presumably, a cyber response isn't either. The LOAC applies in neither case. It's just kids on the playground; not WAR.

On the other hand, it seems that if a kinetic response is deemed appropriate after a cyber incident, then a cyber incident is, almost by definition, an "attack" triggering the LOAC. If the destruction caused by the incident is sufficiently widespread and destructive, it would be hard to argue that an attack had not occurred and that a kinetic response was not appropriate.

So, we are between the proverbial rock and hard place. If our ability to retaliate were sufficiently robust and the attacking state (or parties within a non-responsive attacking state) sufficiently unable to defend against our response, then we could just respond in kind (cyber only) – a kind of "mutually assured disruption" policy. But if either condition fails, a cyber incident could rapidly escalate into a full-scale shooting war, and that seems extreme. So the clear implication, it seems to us, is that we need to be sure a cyber incident can't lead to sufficiently widespread destruction as to justify a kinetic response. Defense precludes offense, so each nation must first have a strong focus on self-protection.

The nature of the Internet also makes more complex the notion of neutrality.[235] The Hague Conventions specify the rights and responsibilities of belligerent and neutral states with regard to neutrality. Under the Conventions, belligerents may not move troops, weapons, or other materials of war across neutral (land) territory,[236] and neutral states must enforce these rules.[237] Naval vessels may transit the waters of a neutral state provided they engage in no acts of hostility while in those waters.[238] But, with regard to telecommunications, Article 8 provides that," A neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals."[239] Arguably, this principle extends to modern

235 The following discussion is based on Jeffrey T. G. Kelsey (2008) Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare. 106 Mich. L. Rev. 1427.
236 1907 Hague Convention V, art. 2. http://avalon.law.yale.edu/20th_century/hague05.asp.
237 1907 Hague Convention V, art. 5. http://avalon.law.yale.edu/20th_century/hague05.asp.
238 1907 Hague Convention XIII, art. I and II. http://avalon.law.yale.edu/20th_century/hague13.asp.
239 http://avalon.law.yale.edu/20th_century/hague05.asp.

communications technologies, including the Internet.[240] But, to the extent that the information infrastructure of a neutral nation is used to move cyber weapons, or even information important to military operations like weather, imagery, or GPS navigation data, no exception applies and a neutral state that allowed a belligerent to move such information would open the neutral state to attack by the opposing belligerent parties to stop the flow.[241] To avoid the unintended consequences of the current LOAC framework, the, our new cyberspace framework may need take the position that what neutral parties need to do to maintain their neutrality merely is to avoid taking any action that would favor one belligerent or group of belligerents at the expense of others.[242]

Developing a regulatory framework for a great commons takes time, and significant efforts need to be expended at the national level in support of (and possibly prior to) efforts at the international level (the UNCLOS lesson). The development needs to follow real-life needs and balance the interests of multiple stake-holders (the ATC lesson). With careful attention to the inherent characteristics of cyberspace, and due care to recognize and avoid unintended consequences, it should be possible to create a regulatory framework that is realistic in application of rules that can actually work and which with due care can recognize and avoid unintended consequences.

LOOKING FORWARD

Creating a regulatory framework for cyberspace will only be possible if there is a shared recognition of the desirability – indeed, even the necessity – of doing so. Shared recognition of the necessity for international regulation of the use and exploitation of the seas and the natural resources within and under the seas led to international cooperation in developing a regulatory structure for the oceans, and eventually UNCLOS. Shared recognition of the need for coherent regulation of air traffic control led to the Chicago Convention. A mutual desire to keep nuclear weapons out of outer space led to the United Nations Treaties and Principles in Outer Space. And the shared recognition that Antarctica was best explored by scientists uninhibited by territorial aspirations or military utilization led to the Antarctic Treaty.

Several influential international organizations have promoted cyber security in

240 See Dept. of Defense Office of Gen. Counsel, An Assessment of International Legal Issues In Information Operations 11 (1999), http://www.maxwell.af.mil/ au/awc/awcgate/dod-io-legal/dod-io-legal.pdf at p. 10.
241 *Ibid.*
242 106 Mich. L. Rev. 1427, 1449.

their agenda. One of the most recent examples is the NATO 2020 report, whereby "NATO must accelerate efforts to respond to the danger of cyber attacks by protecting its own communications and command systems, helping Allies to improve their ability to prevent and recover from attacks, and developing an array of cyber defence capabilities aimed at effective detection and deterrence."[243] Similar conclusions have been reached by the EU, UN, OECD and others. In addition to mutual recognition that a regulatory framework was desirable for balance of powers in the great natural commons, there has also been a shared sense that the frameworks need to protect the rights to access and use the commons by nations that are not great powers as well as those that are.

It is not at all clear that such a consensus exists today or is even possible with respect to cyberspace. It is clear that cyberspace can be used not just for commercial or recreational purposes, but for the exercise of national power through espionage, diplomacy, and even military exploitation. Nations with access to and deep understanding of information technology are better positioned to use and exploit cyberspace for national power than nations that have fewer such resources, and may be unwilling to give up their advantages before it is clear that the downside to such use outweighs their advantage. That clarity may be some time in arriving. But regulatory frameworks for the great natural commons did not arrive overnight either. It took fourteen years and the contributions of 150 nations to produce UNCLOS. Years of effort led to the Chicago Convention for air traffic control. It is clear, however, that such comprehensive frameworks cannot develop if countries are not interested in pursuing them.

Lacking a consensus that a comprehensive framework for regulation of behavior in cyberspace is desirable, humankind will continue to develop regulations for cyberspace in a piecemeal fashion. Already we have the Council of Europe's Convention on Cybercrime[244] addressing criminal activity in cyberspace. Thirty-four countries participated in the signing ceremony in November of 2001, but few countries have ratified the Convention, relying on it more as a guide to development of internal legislation than as a binding treaty. "Common criticisms are that the treaty fails to provide meaningful privacy and civil liberties protections, and that its scope is too broad and covers much more than computer-related crimes. The treaty also lacks a "dual criminality" provision, under which an activity must be considered a crime in both countries before one state could demand cooperation from another." [245]

243 http://www.nato.int/cps/en/natolive/official_texts_63654.htm#p1.
244 Council of Europe's Convention on Cybercrime http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm.
245 http://epic.org/privacy/intl/ccc.html.

Property in cyberspace is the subject of much controversy. The United Nations created the World Intellectual Property Organization (WIPO), established by the WIPO Convention[246] in 1967 to create a regulatory framework for protection of intellectual property. Currently, 184 nations participate in determining the strategic direction and activities of the Organization.

Regulation of commerce in cyberspace, often called e-Commerce, has been evolving for many years. Of course, commerce used and depended upon electronic communications beginning as early as the advent of telegraphic communications. With the growth of the Internet, commerce began to exploit cyberspace for exchange of purchasing, delivery and financial information, and the legal system had to adapt rules that had evolved over centuries as contract law to allow legally cognizable contracts made by parties using cyberspace communications.[247] United Nations Commission on International Trade Law (UNCITRAL) was established by the General Assembly in 1966 to harmonize the laws governing international commerce and reduce obstacles to the flow of trade.[248] The United Nations Convention on Contracts for the International Sale of Goods was created to provide "uniform rules which govern contracts for the international sale of goods and take into account the different social, economic and legal systems would contribute to the removal of legal barriers in international trade and promote the development of international trade."[249]

Currently missing and badly needed are clear rules for information operations related to national power, especially military operations in cyberspace. International Humanitarian Law which serves is so well in real space needs to be adapted to the unique characteristics of cyberspace. Special attention is needed to the issues of attribution and accountability, as well as the forensic policies, practices, procedures and technologies needed to make attribution and accountability work.

Such a piecemeal approach to regulation of behavior in cyberspace undoubtedly has undesirable outcomes. Regulations may be inconsistent, or even contradictory when developed in isolation. Serious gaps may leave certain areas unregulated. Were a consensus to arise that a common regulatory framework for cyberspace is desirable, we have excellent models provided by the great natural commons for creation of regulatory frameworks that could be used. While the differences that make cyberspace unique among the great commons make it impossible to import existing regulatory frameworks without modifications that take into account the

246 The WIPO Convention http://www.wipo.int/treaties/en/convention/trtdocs_wo029.html.
247 http://www.sagepub.com/upm-data/9598_019964Ch1.pdf.
248 http://www.uncitral.org/uncitral/en/about/origin.html.
249 http://www.cisg.law.pace.edu/cisg/text/treaty.html

unique nature of cyberspace, the process for creating regulatory frameworks is well-understood. Using the process could eventually lead to a coherent, comprehensive regulatory framework for cyberspace that facilitates its access and exploitation, ensuring that the benefits of cyberspace are available to all and that the risks of its use for criminal purposes or national power abuses are minimized.