HEINONLINE

Citation: 64 A.F. L. Rev. 1 2009

Content downloaded/printed from
HeinOnline (http://heinonline.org)
Fri Jun 20 14:00:37 2014

-- Your use of this HeinOnline PDF indicates your acceptance of HeinOnline's Terms and Conditions of the license agreement available at http://heinonline.org/HOL/License

-- The search text of this PDF is generated from uncorrected OCR text.

-- To obtain permission to use this article beyond the scope of your HeinOnline license, please use:

https://www.copyright.com/ccc/basicSearch.do?
&operation=go&searchType=0
&lastSearch=simple&all=on&titleOrStdNo=0094-8381

SOVEREIGNTY IN CYBERSPACE: CAN IT EXIST?

LIEUTENANT COLONEL PATRICK W. FRANZESE

I. INTRODUCTION 2
A. On-Going Cyberwar? 2
B. International Law and Cyberspace 5
C. Why Is Sovereignty Important? 7
D. What Is Sovereignty? 8
E. Definition 9
II. STATE SOVEREIGNTY IN CYBERSPACE AND THE GLOBAL COMMONS 10
A. Cyberspace Development 10
B. State Sovereignty in Cyberspace 11
C. Global Commons 14
III. DEVELOPMENT OF SOVEREIGNTY IN OTHER DOMAINS 18
A. Sea Sovereignty 18
B. Air Sovereignty 22
C. Outer Space Sovereignty 24
D. Insights for Sovereignty in Cyberspace 27
Table. International Regime Breakdown 28
IV. ISSUES CONFRONTING STATE SOVEREIGNTY IN CYBERSPACE 33
A. Recognizing Cyberspace as a Sovereign Domain 33
B. Wanting Sovereignty in Cyberspace 34
C. Civilian Expectations 38
D. Technical Issues Regarding Sovereignty 39
V. CONCLUSION 40

Lieutenant Colonel Patrick W. Franzese (B.S., Washington University (1993); J.D., University of Minnesota (1996); M.A., Air Command and Staff College (2008); M.A., School of Advanced Air and Space Studies (SAAS) (2009)) is currently assigned to United States Strategic Command. He is a member of the Minnesota Bar. *This article is based on the author's SAAS thesis. The author thanks Dr. John Sheldon, Lt Col (Dr.) John Davis, Ms. Susan Turley, Capt Scott Hodges, and Capt Mark Rosenow for their valuable assistance and insights in creating this article. The author also wishes to thank his wife Christina and his children for their continuing love and support.*

I. INTRODUCTION

Imagine if 15 years ago a foreign analyst stated he could accomplish the following: (a) gain access to, and possibly alter, U.S. military plans; (b) monitor U.S. military operations and communications; (c) disable vital U.S. military command and control systems either immediately or at any chosen future moment; (d) target specific U.S. military personnel via their financial, medical, or family information; (e) seriously degrade, if not render wholly inoperable, some computer-dependent conventional weapons, thereby significantly negating the United States' conventional advantage; (f) strike at the United States' critical infrastructure such as financial markets, power plants and grids, communication nodes, and transportation systems; and (g) achieve this all non-kinetically, without being physically present in the United States, leaving the United States unable to trace these activities back to the potential adversary's country generally, or its military specifically. Fifteen years ago, his superiors would probably have summarily dismissed this plan as too far-fetched. Yet today, due to the rapid maturity and expansion of cyberspace and the extent to which it increasingly permeates every aspect of society, potential enemies of the United States could possibly accomplish every one of the scenarios listed above.

A. On-Going Cyberwar?

Every day, countries, organizations, and individuals are exploiting, or attempting to exploit, the opportunities and advantages that cyberspace offers, and the United States serves as a rich target for these endeavors. For example, on a single day in 2008, the Pentagon was "attacked" electronically six million times by people seeking access.[1] Although the Pentagon has not publicly provided specifics as to the number of successful intrusions, these attacks reportedly disrupted an internal e-mail system for two days.[2] Moreover, "[m]ultiple Congressional computers have been hacked from multiple Chinese locations."[3] This cyberwar, however, is not limited to government networks, computers, and computer systems. For example, an executive with one New York-based financial house said his company had been attacked one million times in a 24-hour period.[4] This staggering

---

[1] Ardaud de Borchgrave, *Silent Cyberwar*, WASH. TIMES, Feb. 19, 2009, *available at* http://www.washingtontimes.com/news/2009/feb/19/silent-cyberwar/.
[2] *Id.*
[3] *Id.*
[4] *Id.*

number of incidents underscores the threat the United States faces in cyberspace.

The United States, though, is not the world's lone cyberattack victim. In Britain, for example, e-mail across most, if not all, of the military was shut down in January 2009, after the discovery that a hybrid virus or worm infected their systems and sent e-mails to "IP addresses traced back to Russia."[5] In the summer of 2008, Canadian researchers discovered a large electronic spying operation that had infiltrated at least 1,295 computers in 103 countries—including many belonging to embassies, foreign ministries and other government offices—and stolen documents from hundreds of government and private offices.[6] Not only was the operation searching for particular important targets, but the software used had the capability to turn on the camera and audio recording functions of an infected computer, allowing individuals to see and hear what was going on in a room.[7] "Although the Canadian researchers said that most of the computers behind the spying were in China, they cautioned against concluding that China's government was involved. The spying could be a nonstate, for-profit operation, for example, or one run by private citizens in China known as 'patriotic hackers.'"[8]

In addition to infiltrating computer systems and gathering information, nations, organizations, and individuals have used cyberattacks to affect state behavior. Most notably Estonia, Georgia, and Kyrgyzstan were subjected to cyberattacks that significantly affected Internet service—and the corresponding government, banking and communication services, and operations—throughout those countries. These three cyberattacks demonstrate how outsiders can exploit cyberspace to influence state actions across a wide range of situations.

In 2007, the government of Estonia removed the Bronze Soldier, a statue of a Soviet soldier created as a memorial to the fallen soldiers of World War II, in their capital city Tallinn, prompting protests and riots by ethnic Russians living in Estonia. Coinciding with these public demonstrations was a cyberattack against Estonia, primarily in the form of a "DDoS, or Distributed Denial of Service, attack, where websites are suddenly swamped by tens of thousands of visits, jamming and disabling them by overcrowding the bandwidths for the servers

---

[5] Kevin Coleman, *UK Cyber Attack Reported*, DEFENSETECH.ORG, Jan. 20, 2009, http://www.defensetech.org/archives/004644.html (last visited Sept. 12, 2009).

[6] John Markoff, *Vast Spy System Loots Computers in 103 Countries*, N.Y. TIMES.COM, Mar. 29, 2009, http://www.nytimes.com/2009/03/29/technology/29spy.html (last visited Sept. 12, 2009).

[7] *Id.*

[8] *Id.*

running the sites."[9] "The main targets inside of Estonia were: the Estonian presidency and its parliament; almost all of the country's government ministries; political parties; three of the country's six big news organisations; two of the biggest banks; and firms specializing in communications."[10] While the cyberattack was largely traced back to Russia, questions still surround whether, and to what extent, the Russian government was involved.[11]

In 2008, Russia invaded Georgia over disputes in the Georgian provinces of South Ossetia and Abkhazia. Before the invasion by Russian forces, Georgia was subject to a cyberattack, once again primarily in the form of DDoS attacks. This attack spread after the physical fighting began, and the targets included government websites as well as media, communications, and transportation companies.[12] Overall, "Georgia, with a population of just 4.6 million and a relative latecomer to the Internet, saw little effect beyond inaccessibility to many of its government Web sites, which limited the government's ability to spread its message online and to connect with sympathizers around the world during the fighting with Russia."[13] Like Estonia's attack, the attack on Georgia largely originated from Russia, although again debate continues concerning whether, and to what extent, the Russian government was involved.[14] However, unlike Estonia, Georgia engaged in its own cyberattacks by initiating DDoS attacks against pro-Russian websites.[15]

Finally, in 2009, DDoS attacks resulted in two of Kyrgyzstan's four Internet service providers (ISPs) being shut down, taking as much as 80% of the Internet traffic to the West offline.[16] Again, while analysts agree that this cyberattack involved Russian computers, questions remain as to whether the Russian government was involved

---

[9] Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, THE GUARDIAN, May 17, 2007, *available at* http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.

[10] *Id.*

[11] Borchgrave, *supra* note 1; *see also* Charles Clover, *Kremlin-Backed Group Behind Estonia Cyber Blitz*, FIN. TIMES, Mar. 11, 2009, *available at* http://www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html.

[12] John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES.COM, Aug. 12, 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html (last visited Sept. 12, 2009).

[13] *Id.*

[14] Markoff, *supra* note 12; *see also* Borchgrave, *supra* note 1.

[15] Timothy L. Thomas, *The Bear Went Through the Mountain: Russia Appraises Its Five-Day War in South Ossetia*, 22 J. SLAVIC MIL. STUD. 31, 56 (2009).

[16] Danny Bradbury, *The Fog of Cyberwar*, THE GUARDIAN, Feb. 5, 2009, *available at* http://www.guardian.co.uk/technology/2009/feb/05/kyrgyzstan-cyberattack-internet-access.

and, if so, the extent of its involvement.[17] Moreover, experts disagree as to the purpose of the cyberattack. Many have speculated that Russia initiated the cyberattack as a means of coercing the Kyrgyz Government to close Manas Air Force Base, thus removing the United States military from Kyrgyzstan.[18] However, others believe that Kyrgyzstan's government actually initiated the cyberattack, using organizations within Russia to execute this attack, as a means of silencing government opposition.[19]

In sum, states, organizations, and individuals continually act in cyberspace to both probe networks and gather information on other actors. Actors are also continually realizing, developing, and exploiting the potential power of cyberspace to influence, and respond to, the actions of other states. States must thus focus on developing an appropriate framework that will address the multitude of issues raised by cyberspace.

B. International Law and Cyberspace

Currently, commentators analyzing cyberattacks emphasize questions such as the following: When does a cyberattack constitute "use of force" under Article 2(4) of the United Nations (UN) Charter?[20] When does a cyberattack constitute an "armed attack" under Article 51 of the UN Charter?[21] When can a state respond in self-defense with a cyberattack of its own? When can a state respond in self-defense with physical force to a cyberattack? And what is the appropriate, proportional response to a cyberattack?[22] The answers to these

---

[17] Robert Mackey, *Are 'Cyber-Militias' Attacking Kyrgyzstan?*, N.Y. TIMES NEWS BLOG, THE LEDE, Feb. 5, 2009, http://thelede.blogs.nytimes.com/2009/02/05/are-cyber-militias-attacking-kyrgyzstan/?ref=asia (last visited Sept. 12, 2009).

[18] *Id.*; *see also* Christopher Rhoads, *Kyrgyzstan Knocked Offline*, WALL ST. J.COM, Jan. 28, 2009, http://online.wsj.com/article/SB123310906904622741.html (last visited Sept. 12, 2009) (discussing cyberattack against Kyrgyzstan).

[19] Rhoads, *supra* note 18; *see also* Posting of Jeffrey Carr to IntelFusion, *Why I Believe That the Kyrgyzstan Government Hired Russian Hackers to Launch a DDOS Attack Against Itself*, Jan. 30, 2009, http://intelfusion.net/wordpress/?p=520 (last visited Aug. 25, 2009) (discussing cyberattack against Kyrgyzstan).

[20] U.N. Charter art. 2, para. 4 ("All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.").

[21] U.N. Charter art. 51 ("Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security . . . . ").

[22] *See, e.g.*, WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE (Aegis Res. Corp. 1999); THOMAS C. WINGFIELD, THE LAW OF INFORMATION CONFLICT: NATIONAL

questions are important for guiding both how a state will respond to a cyberattack and, equally important, how a state will conduct its own cyber operations. Applying these questions to the cyberattacks discussed above demonstrates both the complexity of these issues and the need for resolution. Specifically, did Russia use force in gaining access to the UK military's e-mail? Was Estonia subject to an armed attack from Russia? Did Russia's actions before the actual invasion of Georgia provide Georgia the right to use force in self-defense? What is the appropriate response for governments victimized by China's spying operation? What responsibility do Russia and China have for monitoring and preventing cyberattacks originating from their respective countries? Finally, could Russia and China be held responsible for not preventing cyberattacks originating from their territory and, if so, how?

Unfortunately, no consensus has developed in answering these questions. More troubling, various commentators still hold widely divergent views on basic, fundamental questions. For example, they cannot even agree on a framework when addressing the question of when a cyberattack constitutes an act of war, armed attack or use of force. Some believe that for a cyberattack to constitute an act of war, it must "accompany a military offensive in the real world."[23] Others argue that cyberattacks cause "widespread harm."[24] Even these interpretations are somewhat ambiguous because people could hold varying opinions as to what exactly the terms "a military offensive in the real world" and "widespread harm" mean. Applying these ideas to the cyberattacks discussed above, some could argue that only Russia's attack on Georgia constituted an act of war because it accompanied a military offensive in the real world; however, others could argue that each cyberattack was an act of war because each attack caused "widespread harm," depending on how that term is defined.

While many scholars have provided insightful analysis of how cyberspace might fit under current international law, the current international legal paradigm predates cyberspace and cannot adequately address the various issues raised by cyberspace. Moreover, the rapid growth of cyberspace has outpaced the ability of nations individually, and the international community as a whole, to understand and control it. These facts, however, are not remarkable. With any new technology, either existing international law addresses the new issues or the law evolves with the new technology. Thus, the question becomes how to

---

SECURITY LAW IN CYBERSPACE (Aegis Res. Corp. 2000). Both books discuss in detail these types of questions and their interpretation of how international law applies.

[23] *Marching Off to Cyberwar*, ECONOMIST, Dec. 4, 2008, *available at* http://www.economist.com/sciencetechnology/tq/displaystory.cfm?story_id=12673385.

[24] *Id.*

determine the appropriate basis or framework from which the international community can begin to address the issues raised by cyberspace. The answer, this article proposes, is recognizing and establishing state sovereignty in cyberspace.

C. Why Is Sovereignty Important?

The sovereignty of the state forms the fundamental basis of the current international order, something that most scholars trace back to the Peace of Westphalia in 1648.[25] Under the current international order, the state is the traditionally recognized actor that engages in war, fashions alliances, enters into treaties, and both creates and populates international organizations such as the United Nations. In fact, a key principle of the United Nations, and its Members, is that the United Nations "is based on the principle of the sovereign equality of all its Members."[26] Preserving state sovereignty is a vital goal of both state-based international organizations and individual countries. For example, when Iraq invaded Kuwait in 1990, the UN Security Council authorized the use of force to, in part, "restore the sovereignty, independence, and territorial integrity of Kuwait."[27] In 1960, the Soviet Union shot down an American U-2 airplane flying over Soviet airspace because the Soviet Union claimed the U-2 had violated its sovereignty.[28] While not every violation of sovereignty will necessarily result in the use of force, state practice evidences that a state can use force to defend its sovereignty.[29]

Moreover, the United Nations often uses "sovereignty" in conjunction with the traditional phrasing of Article 2(4) of the UN Charter, which reads, "[a]ll members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any manner inconsistent with the Purposes of the United Nations."[30] Numerous UN Security Council and General Assembly resolutions concerning state conflict use the

---

[25] *See* DANIEL PHILPOTT, REVOLUTIONS IN SOVEREIGNTY: HOW IDEAS SHAPED MODERN INTERNATIONAL RELATIONS, ch. 5 (Princeton Univ. Press 2001) (asserting the Peace of Westphalia as the origin of modern international relations).

[26] U.N. Charter art. 2, para. 1.

[27] S.C. Res. 661, U.N. Doc. S/RES/0661 (Aug. 6, 1990); *see also* S.C. Res. 674, U.N. Doc. S/RES/0674 (Oct. 29, 1990), *and* S.C. Res. 678, U.N. Doc. S/RES/0661 (Nov. 29, 1990).

[28] *See* Oliver J. Lissitzyn, *Some Legal Implications of the U-2 and RB-47 Incidents*, 56 AM. J. INT'L L. 135 (1962) (which discusses the legal issues and implications of the U-2 incident).

[29] *See infra* notes 154-156 and accompanying text.

[30] U.N. Charter art. 2, § 4.

phrase "sovereignty, territorial integrity and political independence."[31] This underscores the fundamental role sovereignty plays in the current international order.

D. What Is Sovereignty?

While understanding the fundamental role of sovereignty is important, the more difficult task is defining exactly what constitutes sovereignty. Black's Law Dictionary states that sovereignty is "1. Supreme dominion, authority or rule. 2. The supreme political authority of an independent state. 3. The state itself".[32] While informative, the definition is too general for the purposes of this article. Stephen Krasner, a renowned international relations professor, however, provides a more practical and useful explanation of sovereignty. He posits that sovereignty is usually conceptualized in four different ways:

> Domestic sovereignty, referring to the organization of public authority within a state and to the level of effective control exercised by those holding authority; interdependence sovereignty, referring to the ability of public authorities to control transborder movements; international legal sovereignty, referring to the mutual recognition of states; and Westphalian sovereignty, referring to the exclusion of external actors from domestic authority configurations.[33]

Krasner also states that there are a "bundle of properties associated with sovereignty-territory, recognition, autonomy, and control" that characterize states in the international system.[34]

Both constructs are useful when thinking about how cyberspace impacts sovereignty and whether sovereignty can exist in cyberspace. For example, cyberspace tests a state's interdependence sovereignty because it challenges a state's ability to control transborder movements. With the interconnectivity of cyberspace, a person sitting in Africa can "enter" the United States and conduct numerous innocuous activities such as shopping, correspondence, and electronic records retrieval

---

[31] *See, e.g.*, S.C. Res. 1680, U.N. Doc. S/RES/1680 (May 17, 2006); G.A. Res. 47/121, U.N. DOC. A/RES/47/121 (Dec. 18, 1992); S.C. Res. 1234, U.N. Doc. S/RES/1234 (Apr. 9, 1999).

[32] BLACK'S LAW DICTIONARY 1430 (8th ed. 2004).

[33] STEPHEN D. KRASNER, PROBLEMATIC SOVEREIGNTY: CONTESTED RULES AND POLITICAL POSSIBILITIES 6-7 (Colum. Univ. Press 2001).

[34] STEPHEN D. KRASNER, SOVEREIGNTY: ORGANIZED HYPOCRISY 220 (Princeton Univ. Press 1999).

"inside" the United States, which result in transferring information outside the United States. That same person can "enter" the United States and engage in harmful activities such as hacking into government computer systems, altering computer code, or disabling computer run systems, such as power grids, inside the United States. However, because cyberspace presents a challenge to sovereignty does not mean that a state is powerless to exert sovereignty in cyberspace. To the contrary, state sovereignty in cyberspace will not only require that a state receive recognition of its sovereignty in cyberspace from other states but also that it is able to exert some measure of control over its cyberspace. Chapter Three explores this last idea more fully.

It is important to understand that Krasner argues that his four concepts of sovereignty are often in tension and not all four concepts have to be present together for sovereignty to exist.[35] Additionally, he states that all political entities have never concurrently possessed all four types of sovereignty. [36] Thus, while Krasner's proffered concepts and properties give shape to what constitutes sovereignty and provide a useful method for discussion, they are not a strict checklist of prerequisites.

E. Definition

In discussing cyberspace, a common point of contention is the question of its definition. For the purposes of this paper, the definition set forth in Joint Publication 1-02, "DOD Dictionary of Military and Associated Terms," will suffice. It defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[37] While the Internet is a subset of cyberspace, and the terms are not interchangeable, this article focuses heavily on the Internet. That said, the principles developed here apply not only to the Internet, but to cyberspace as a whole.

With an understanding of the threats and issues raised by cyberspace, as well as the important role that sovereignty plays in our international order, the next step is analyzing the role of sovereignty and cyberspace. The remainder of this article focuses on whether states can assert their sovereignty in cyberspace, how states might achieve it, and the obstacles that stand in their way. Section II of this article explores

---

[35] *See generally* KRASNER, *supra* note 33; KRASNER, *supra* note 34 (providing further discussion of these concepts).

[36] KRASNER, *supra* note 34, at 238.

[37] U.S. DEP'T OF DEF. JOINT PUB. 1-02, DICTIONARY OF MILITARY AND ASSOCIATED TERMS, 12 Apr. 2001 (Mar. 17, 2009).

two concepts commonly discussed when examining the issue of sovereignty and cyberspace. Specifically, it explores the idea that cyberspace is immune from state sovereignty and the idea that cyberspace is a global commons. While both these notions initially appear promising, they both break down when analyzing the requirements and implications each respective notion entails. Section III examines how sovereignty has developed, and continues to develop, in the other recognized domains of sea, air, and space. While sovereignty in each domain developed independently and is unique, the establishment of sovereignty in each domain shares many characteristics. Lessons from how sovereignty developed in these domains give insight as to how sovereignty in cyberspace might develop. Section IV considers four key obstacles to states asserting sovereignty in cyberspace. Specifically, states must recognize cyberspace is a sovereign domain, decide that exerting state sovereignty in cyberspace is in their strategic interests, manage civilian expectations of state sovereignty in cyberspace, and develop the technical capability to exert their sovereignty in cyberspace.

II. STATE SOVEREIGNTY IN CYBERSPACE AND THE GLOBAL COMMONS

The organizations, purpose, and people behind the creation of cyberspace heavily influenced what it is today. Specifically, the academics and scientists looked at cyberspace in romanticized terms, seeing the promise it held for all of humankind. This belief naturally affected how people considered the issue of sovereignty and cyberspace, which resulted in essentially two competing theories in lieu of the idea of state sovereignty. The first theory is that cyberspace is immune from state sovereignty. However, this theory ignores the fact that cyberspace needs the stability and regulation that state sovereignty provides, and states have a valid interest in exercising their control in cyberspace. The second theory is that cyberspace is a global commons. This theory, however, distorts the essence of a global commons and discounts the role states play in creating them.

A. Cyberspace Development

The military and scientists played large roles in the early, foundational development of cyberspace, and both groups brought their own divergent ideas on how it should develop. The military brought its values "such as survivability, flexibility, and high performance, over commercial goals such as low cost, simplicity, or consumer appeal."[38]

[38] JANET ABBATE, INVENTING THE INTERNET 5 (MIT Press 1999).

Conversely, academic scientists "incorporated their own values of collegiality, decentralization of authority, and open exchange of information."[39] Thus, cyberspace in many ways combined what the military wanted from it and what academics wanted it to be.

In the mid-twentieth century, academics such as educator Herbert McLuhan viewed technology and the interconnectedness that was possible via electronic media as a means of creating a "global village."[40] More significantly, some academics believed technology would actually spur an evolution in human consciousness. Because they equated consciousness with information, through interconnectedness, they reasoned that "human beings [would] become units of information, each contributing to this new world sentience."[41] Additionally, these academics thought that technology would help replace the industrial age that valued and promoted competitiveness with an information age that valued and promoted cooperation between humans. [42] In their minds, "the more information is shared, the freer society is, the greater the potential is for cooperation. Perfect cooperation reaps the same results as perfect competition, and without losers."[43]

To reach this nirvana, academics and scientists believed that governments and corporations should not control the emerging information technology. This notion encompassed the belief that whoever controlled the communication or information systems also controlled the message. As Abbie Hoffman, a prominent political activist during the 1960s and 1970s, stated, "Freedom of the press belongs to those that own the distribution system."[44] Therefore, the key to ensuring that individuals could truly share information was to have communication/information systems that were free from government and corporate interference.

B. State Sovereignty in Cyberspace

The belief that cyberspace should be free from government interference, or sovereignty, led to the idea that cyberspace is, in fact, immune from state sovereignty. Perhaps the one statement that embodies this concept more than any other was made by John Perry Barlow, a lyricist for the Grateful Dead and founding member of the Electronic Frontier Foundation, an organization dedicated to defending

---

[39] *Id.*

[40] ADAM BRATE, TECHNOMANIFESTOS: VISIONS FROM THE INFORMATION REVOLUTIONARIES 197-203 (Texere 2002).

[41] *Id.* at 199.

[42] *Id.* at 207-08.

[43] *Id.* at 208.

[44] *Id.* at 209.

civil liberties on the Internet. Back in 1996, in response to the Communications Decency Act, Barlow wrote "A Declaration of the Independence of Cyberspace," which began, "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."[45]

Despite the rhetorical flair of Barlow's declaration, there are five key reasons why cyberspace is not immune from state sovereignty. The first is that some entity must control cyberspace for it to exist and function. Cyberspace requires a physical structure, because without it, users have no access. That physical structure, however, is terrestrially based and thus naturally falls under the purview of the state where those physical assets sit. Additionally, cyberspace itself requires regulation and oversight.[46] For example, the Internet Corporation of Assigned Names and Numbers (ICANN) is an organization responsible for such vital matters as assigning domain names and IP addresses.[47] This needed oversight will only increase, moreover, as the number of users continues to rapidly expand.[48]

The second reason cyberspace is not immune from state sovereignty is that financial relationships in cyberspace need laws to govern those relationships and transactions. [49] If cyberspace was immune from state sovereignty, any financial relationship established in cyberspace would be tenuous at best and fraught with peril for either side. The fact that business decisions are heavily influenced by the laws

---

[45] John Perry Barlow, A Cyberspace Independence Declaration, http://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration (Feb. 9, 1996) (last visited Aug. 25, 2009).

[46] *See* Internet Assigned Numbers Authority, Introducing IANA, http://www.iana.org/about/ (last visited Aug. 24, 2009) ("[w]hilst the Internet is renowned for being a worldwide network free from central coordination, there is a technical need for some key parts of the Internet to be globally coordinated").

[47] Internet Corporation for Assigned Names and Numbers, ICANN Factsheet, http://www.icann.org/en/factsheets/fact-sheet.html (last visited Aug. 24, 2009). While this body is under contract with the United States, the intent is that ICANN will ultimately turn into a fully independent organization.

[48] As early as December 1995, 16 million people or .4 percent of the world population used the Internet. By June 2009, almost 1.7 billion people or 24.7 percent of the World population, used the Internet. Internet Word Stats: Usage and Population Statistics, Internet Growth Statistics, http://www.internetworldstats.com/emarketing.htm (last visited Sep. 9, 2009).

[49] *See generally* JACK L. GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 29-46 (Oxford Univ. Press 2006) (discussing how companies such as eBay needed laws to help operate their business and how the laws of states influence their business practices).

of a respective state, evidences that cyberspace is not immune from state sovereignty.[50]

The third reason cyberspace is not immune from state sovereignty is that content sent through cyberspace holds significance in the "real" world. While cyberspace ideally allows for the free flow of information, no "cyberspace exemption" shields information from the valid interests of the state where information is sent, received, or stored. For example, the United States, along with many other countries, has a stated interest in preventing the possession and spread of child pornography, France has a stated interest in stopping the spread of Nazi memorabilia, and Australia has a stated interest in protecting its citizens from defamatory statements.[51] In each of the examples above, court systems ruled that information accessible to the individual located in those respective states via cyberspace is subject to the laws within that respective state.[52] Accordingly, a website located outside of France, which sells Nazi memorabilia, that people can access from France, is subject to the laws of France.[53] While this area of the law is still developing, it demonstrates that states have valid interests in and legitimate control over what occurs in cyberspace.

The fourth reason cyberspace is not immune from state sovereignty is that states are increasingly required to assert their presence in cyberspace as a matter of national security. Whether by design or neglect, many states connect to and operate some of their critical infrastructure in or through cyberspace.[54] This has left those states, including the United States, increasingly vulnerable. As the *National Strategy to Secure Cyberspace* succinctly states:

> In peacetime America's enemies may conduct espionage on our Government, university research centers, and private companies. They may also seek to prepare for cyber strikes during a confrontation by mapping U.S. information systems, identifying key targets, and lacing our infrastructure with back doors and other means of access. In wartime or crisis, adversaries may seek to intimidate the Nation's political

---

[50] *Id.*
[51] *Id.* at 147-61.
[52] *Id.*
[53] *Id.*
[54] For example, *The National Strategy to Secure Cyberspace* lists a number of critical infrastructures that are dependent upon cyberspace. These include: Banking and Finance; Chemical; Oil and Gas; Electric; Law Enforcement; and Transportation (Rail); and Water. U.S. DEP'T OF HOMELAND SEC., THE NATIONAL STRATEGY TO SECURE CYBERSPACE xiii (2003).

> leaders by attacking critical infrastructures and key economic functions or eroding public confidence in information systems.[55]

Because the potential to cause harm in cyberspace is real and continues to grow, states cannot leave cyberspace ungoverned but must find a way to exert their control and authority to reduce their vulnerability.

As discussed above, a driving force behind the early development of the Internet were scientists who viewed the Internet as a means of cooperation for the betterment of humankind and "were assumed to be uninterested in abusing the network."[56] However, not everyone who uses the Internet today shares that same vision and many of those users see the Internet as a means to exploit other individuals, create chaos, gain an advantage over a competitor, or disseminate a specific message of hate or violence. Consequently, much like the "real" world which requires state sovereignty to regulate, protect, and punish various actors, cyberspace needs this sovereign influence as well. Furthermore, since states currently exploit cyberspace as a means of gaining a strategic and military advantage over another state,[57] states must exert their control as a matter of national security. The end result is that cyberspace is not immune from state sovereignty.

C. Global Commons

A second theory often put forth is that cyberspace is part of the global commons. Even some U.S. government publications promote this idea. Specifically, the 2005 *Strategy for Homeland Defense and Civil Support* states that "the global commons consist of international waters and airspace, space, and cyberspace."[58] Additionally, while the 2008 National Defense Strategy does not specifically define global commons, it references "information transmitted under the ocean or through space," when discussing global commons.[59] Even the National Strategy to Secure Cyberspace uses the word "global" 20 times when discussing the nature of cyberspace, while at the same time it fails to mention the word "sovereignty" even once.[60]

---

[55] *Id.* at viii.
[56] *Id.*
[57] *See supra* notes 1-19 and accompanying text for a discussion of these types of activities.
[58] U.S. DEP'T OF DEF., THE STRATEGY FOR HOMELAND DEFENSE AND CIVIL SUPPORT 12 (2005), *available at* http://www.defenselink.mil/news/Jun2005.
[59] U.S. DEP'T OF DEF., NATIONAL DEFENSE STRATEGY 16 (2008), *available at* http://www.defenselink.mil/news/2008%20national%20defense%20strategy.pdf.
[60] U.S. DEP'T OF HOMELAND SEC., *supra* note 54.

The preliminary question is how to define the "global commons." No universally accepted definition exists, and depending upon which dictionary or non-governmental organization one consults, a slightly different or nuanced definition appears. Most definitions, however, focus on natural resources that are not under the control of a specific nation.[61] Fortunately, within international governmental organizations, there is a bit more uniformity. Specifically, bodies within both the United Nations and the Organization for Economic Cooperation and Development (OECD) define global commons as "natural assets outside national jurisdiction such as the oceans, outer space and the Antarctic."[62] However, in analyzing this definition, it becomes clear that the oceans, outer space, and the Antarctic are not global commons simply because they are "natural assets outside natural jurisdiction." Rather, five similarities exist among them that evidence what it means to be a global commons.

First, international treaties govern each of these natural assets. The UN Convention on the Law of the Sea (Law of the Sea) entered into force in 1994, and, as of 19 December 2008, 157 countries have signed the treaty.[63] The Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (Outer Space Treaty) entered into force in 1967, and, as of 1 January 2008, 98 states have ratified the treaty and 27 additional states have signed onto it.[64] Finally, in 1959, 12 countries

---

[61] *See, e.g.,* World Resources Institute, The Global Commons, Overview, http://www.wri.org/publication/content/8393 (last visited Sept. 12, 2009) ("the global commons – those natural systems and cycles that underpin the functioning of ecosystems everywhere"); THE OXFORD POCKET DICTIONARY OF CURRENT ENGLISH, Encyclopedia.com, *Global Common*, http://www.encyclopedia.com/doc/1O999-globalcommon.html (last visited Sept. 12, 2009) ("any of the earth's ubiquitous and unowned natural resources, such as the oceans, the atmosphere, and space").

[62] Organization for Economic Co-operation and Development, Glossary of Statistical Terms, *Global Commons*, http://stats.oecd.org/glossary/detail.asp?ID=1120 (last visited Sept. 12, 2009); United Nations Statistics Division, Global Commons Definition, http://unstats.un.org/unsd/environmentgl/gesform.asp?getitem=573 (last visited Aug. 24, 2009).

[63] United Nations Division for Ocean Affairs and Law of the Sea, Chronological Lists of Ratifications of, Accessions and Successions to the Convention and the Related Agreements as of 20 July 2009, http://www.un.org/Depts/los/reference_files/chronological_lists_of_ratifications.htm#The United Nations Convention on the Law of the Sea (last visited Aug. 24, 2009). Note, the Law of the Sea built upon earlier conventions such as the Convention on the High Seas that entered into force on 30 September 1962.

[64] *See* Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, Jan. 27, 1967, 18 U.S.T. 2410, *available at* http://www.oosa.unvienna.org/oosa/SpaceLaw/outerspt.html [hereinafter Outer Space Treaty].

signed the Antarctic Treaty, and 47 countries are currently party to the treaty.[65]

Second, each of these treaties addresses specific permissible uses and prohibitions for the natural asset. The Antarctic Treaty states, in part, that nations can only use the Antarctic for peaceful purposes, including scientific research, and specifically prohibits nations from testing nuclear weapons or disposing nuclear waste in the Antarctic.[66] Similarly, the Outer Space Treaty states, in part, that nations can only use the moon and other celestial bodies for peaceful purposes, including scientific research, and prohibits nations from launching any nuclear weapon or other weapon of mass destruction into orbit.[67] Finally, the Law of the Sea covers a broad range of issues ranging from a nation's transit rights, to a nation's ability to lay submarine cables and pipeline, to a nation's fishing rights on the high seas.[68]

Third, each of the treaties specifically addresses the issue of sovereignty. The Antarctic Treaty states, "No new claim, or enlargement of an existing claim, to territorial sovereignty in Antarctica shall be asserted while the treaty is in force."[69] The Outer Space Treaty states, "Outer space, including the Moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means."[70] Finally, the Law of the Sea states, "no State may validly purport to subject any part of the high seas to its sovereignty" and "no State shall claim or exercise sovereignty or sovereign rights over any part" of the seabed and ocean floor and subsoil thereof, beyond the limits of national jurisdiction "or its resources."[71]

Fourth, each treaty bounds, or defines, areas of sovereignty and thus areas that constitute the global commons. Under the Antarctic Treaty, the global commons is defined as "south of 60 [degrees] South Latitude, including all ice shelves."[72] The Law of the Sea has a myriad of provisions precisely defining areas that constitute territorial waters where a state has sovereignty as well as other areas of state interest such

---

[65] Secretariat of the Antarctic Treaty, The Antarctic Treaty, http://www.ats.aq/e/ats_treaty.htm (last visited Sept. 12, 2009).

[66] *See* The Antarctic Treaty, Dec. 1, 1959, 12 U.S.T. 794, 402 U.N.T.S. 72, *available at* http://www.ats.aq/documents/ats/treaty_original.pdf.

[67] Outer Space Treaty, *supra* note 64.

[68] *See* United Nations Convention on the Law of the Sea, Dec. 10, 1982, 1833 U.N.T.S. 397 [hereinafter UNCLOS]. Not surprisingly, since nuclear powered ships and ships carrying nuclear weapons existed when nations created the Law of the Sea, there is no prohibition, or other restrictions, placed on nuclear weapons on the high seas.

[69] The Antarctic Treaty, *supra* note 66, at 74.

[70] Outer Space Treaty, *supra* note 64, at 208.

[71] *See* UNCLOS, *supra* note 68, arts. 89, 139.

[72] The Antarctic Treaty, *supra* note 66, at 76.

as an exclusive economic zone, thereby generally leaving the remaining oceans as a global commons.[73] Finally, under the Outer Space Treaty, the global commons essentially constitutes all of "outer space, including the Moon and other natural celestial bodies," although there is no specific definition of outer space provided in the Outer Space Treaty and thus no clear line between airspace and outer space.[74]

Finally, states could not realistically expect to exercise sovereignty over these areas when they established these treaties. Even if a nation wanted to assert sovereignty over the entirety of the oceans, outer space, or the Antarctic, no nation realistically could exert control or enforce its sovereignty over the entirety of these natural assets. As Section III will discuss, the areas where a state could reasonably exert sovereignty were not likely to end up as part of the global commons. As states gain the ability to exert sovereignty over portions of the global commons, and have a commensurate desire to do so, sovereignty over these areas will likely become an issue again.

Thus, the prerequisite to becoming a global commons is not that the area is a "natural asset outside natural jurisdiction." Rather, a global commons is something that has five unique characteristics. First, a global commons has a governing international treaty. Second, this treaty provides specific permissible uses and prohibitions of that global commons. Third, the global commons has boundaries and is definable. Fourth, nations have agreed to forgo, or at least leave unasserted in the case of the Antarctic, claims of exclusive sovereignty over any portion of the global commons. Finally, no single state is capable of controlling the global commons. In other words, a global commons is not the absence of sovereignty but rather the presence of a shared global sovereignty. With this understanding, categorizing cyberspace as a global commons is problematic because all five of these unique characteristics are not present with regard to cyberspace.

Many of the designers and creators of cyberspace viewed it as an intellectual nirvana free from the constraints of the "real" world. However, in reality, cyberspace is part of the "real" world and thus subject to its constraints and order—in other words, subject to state sovereignty. The idea that cyberspace is immune from state sovereignty is impractical. Cyberspace is based upon a physical architecture and needs regulation, thus allowing states to exert their control. In fact, as discussed above, states are beginning to exert control. Similarly, the idea that cyberspace is part of the global commons is flawed. Putting aside that cyberspace is not a natural asset, cyberspace currently lacks the defining characteristics of a global commons. Significantly, states

---

[73] *See generally* UNCLOS, *supra* note 68.
[74] *See generally* Outer Space Treaty, supra note 64.

would need to agree on shared sovereignty over cyberspace if they want it to be a global commons. While cyberspace is not immune from state sovereignty and is not a global commons, the question remains as to whether cyberspace could ever be free from state sovereignty or become a global commons. Although both options seem theoretically possible, the existence of an international order fundamentally based upon the concept of state sovereignty renders both options impractical. While Section III develops this answer, the basic reason is that states' competing interests, namely security, will ultimately cause them to want to assert control in cyberspace.

III. DEVELOPMENT OF SOVEREIGNTY IN OTHER DOMAINS

Cyberspace is subject to the constraints of the "real" world, which lacks shared global sovereignty over cyberspace, thus this article turns now to how individual states might achieve sovereignty in cyberspace. Because sovereignty in cyberspace will be an extension of territorial sovereignty, analyzing the development of sovereignty within the domains of air, sea, and space—domains that all sprang forth from territorial sovereignty as well—can provide insight into how sovereignty in cyberspace might develop. Due to the historical breadth of this subject, this examination remains within certain parameters. Specifically, the analysis focuses on broad chronological developments, the major notions of state sovereignty in the various domains, and the significant issues within each domain relevant to this article. From this examination, this chapter draws some insights into how states might achieve sovereignty in cyberspace.

A. Sea Sovereignty

By at least the second century BC, Roman law considered the seas to be *communes omnium naturali jure*, or common to all humankind.[75] Roman Emperor Justinian I (483-565 AD) wrote the earliest recorded statement on the law of the sea and in it "declared that the sea and its fish were available to all and no state could extend its jurisdiction beyond the shore, which was defined as the high-water mark."[76] Of course, this concept of the seas being common to all humankind was easy to follow since the Mediterranean Sea was essentially a "Roman lake" due to the empire's territorial borders.[77] With the collapse of the Roman Empire, other actors asserted their

---

[75] SUSAN J. BUCK, THE GLOBAL COMMONS: AN INTRODUCTION 76 (Island Press 1998).
[76] *Id.*
[77] GEORGE GALDORISI & KEVIN R. VIENNA, BEYOND THE LAW OF THE SEA: NEW DIRECTIONS FOR U.S. OCEANS POLICY 8 (Praeger 1997).

sovereignty over the oceans at varying lengths from their shores "based on some mix of the commercial aspect of the claims, national security, protection of fisheries, and collection of tariffs."[78] Anarchy, in which the strongest navy prevailed, essentially ruled the oceans until the late sixteenth century and early seventeenth century.[79]

Starting in the late sixteenth century and early seventeenth century, the debate over control of the seas was refined between those who championed *mare liberum*, or "open seas," and those who championed *mare clausum*, or "closed seas." Although many writers contributed to the development and promotion of these theories, Hugo Grotius remains the dominant figure, and open seas became the dominant theory. In his work *Mare Liberum*, Grotius "defended the freedom of the seas by arguing that the seas cannot be owned, that 'the sea is one of those things which is not an article of merchandise, and which cannot become private property. Hence it follows, to speak strictly, that no part of the sea can be considered as territory of any people whatsoever.'"[80] However, most jurists adopted the position that states "enjoy some rights to regulate in their own interests activities in the seas adjoining their coasts," something that even Grotius acknowledged.[81] By the end of the seventeenth century, the idea of a distinction between "high seas, free and open to all, and coastal waters susceptible to appropriation by the adjacent State" was well established, and by the beginning of the nineteenth century it was a respected principle of international law.[82] Some trace the "shrinkage of maritime sovereignty . . . to changed concepts of the value of the sea to the world community. Originally regarded as an avenue of plunder and as a buffer area separating national territories, by the comparatively peaceful nineteenth century the sea had come primarily to signify a medium of trade" and states financially benefited from the increased trade made possible by free seas and open trade routes.[83]

Although the idea of limited maritime sovereignty was established, "two matters remained unresolved: first, the question of the width of those waters . . . , and secondly, the question of the precise

---

[78] BUCK, *supra* note 75, at 76-77.

[79] GALDORISI & VIENNA, *supra* note 77, at 8; *see also* Note, *National Sovereignty of Outer Space*, 74 HARV. L. REV. 1160 (1961). The only brief respite during this period was the Treaty of Tordesillas in 1494 between Portugal and Spain that audaciously split the world between the two countries. Not surprisingly, as other countries' maritime capabilities grew, Portugal and Spain could not enforce the treaty. BUCK, *supra* note 75, at 77-78.

[80] GALDORISI & VIENNA, *supra* note 77, at 10.

[81] R. R. CHURCHILL & A. V. LOWE, THE LAW OF THE SEA 59 (rev. ed., St. Martin's Press 1988) (1983).

[82] *Id.* at 59-60.

[83] Note, *supra* note 79, at 1161.

juridical nature of coastal States' rights over the territorial sea."[84] With regard to the width of territorial waters, the most notable historic position was that of three miles, which, according to the generally accepted rationale, was the distance a cannon shot would carry,[85] and was approximately the line of sight from the shoreline.[86]

For approximately two centuries, countries disputed the width of territorial waters. Some states wanted to minimize territorial waters to maximize freedom of navigation for their merchant fleets and warships, while other states wanted to maximize territorial waters to control such activities as fishing and smuggling near their coasts.[87] By 1960, most states claimed the width of territorial waters was less than twelve miles, however, by the 1980s, "the great majority of States claimed territorial seas of twelve miles or more . . . . The steady shift towards wider territorial seas . . . is a reflection of the desire to bring coastal waters—and the fishing, pollution and so on conducted, often by foreign vessels, within them—under national control."[88] Moreover, the discovery of mineral resources, notably oil, under the seabed also led states to extend their claims of sovereignty.[89] Eventually, the Law of the Sea established the width of territorial waters at twelve nautical miles.[90] However, a handful of countries still claim different distances or have unique circumstances that affect the twelve nautical mile width.[91]

With regard to the second unresolved issue concerning the precise juridical nature of coastal states' rights, two broad approaches initially developed. The first "claimed that coastal States either had proprietorial rights in their territorial seas, or at least enjoyed sovereignty or plenary jurisdiction over them."[92] This approach emphasized the notion of sovereignty over territorial waters. The second approach argued for a slightly different rule:

---

[84] CHURCHILL & LOWE, *supra* note 81, at 60.
[85] GALDORISI & VIENNA, *supra* note 77, at 10.
[86] *Id.* at 31; *see also* INGRID DETTER DELUPIS, INTERNATIONAL LAW AND THE INDEPENDENT STATE (Crane Russak 1974). Not all states subscribed to the three-mile rule. For example, Scandinavian states claimed dominion over a fixed distance, which had narrowed to four miles by the mid-eighteenth century. CHURCHILL & LOWE, *supra* note 81, at 65; DETTER DELUPIS, *supra* note 86, at 31.
[87] CHURCHILL & LOWE, *supra* note 81, at 65-66; *see also* DETTER DELUPIS, *supra* note 86, at 31-36.
[88] CHURCHILL & LOWE, *supra* note 81, at 67.
[89] Note, *supra* note 79, at 1162.
[90] UNCLOS, *supra* note 68, at pt. II, § 2.
[91] CHURCHILL & LOWE, *supra* note 81, at 65-68.
[92] *Id.* at 60.

> States enjoyed only a 'bundle of servitudes' (*faisceau de servitudes*) over coastal waters, permitting them to exercise jurisdiction in the measure necessary for the protection of their interests, and accepted the corollary that if the existence of a right of jurisdiction were to be questioned the burden lay upon the coastal State to prove that it did exist.[93]

This approach emphasized that states had rights in adjoining waters, short of sovereignty, that varied depending upon the specific interest and purpose.

Despite the two competing positions, more and more states moved to assert sovereignty, although some states continued to claim separate jurisdictional zones for various purposes even into the twentieth century.[94] Eventually, the concept of sovereignty was universally accepted and codified, first in the 1958 Convention on the High Seas and then most notably in the United Nations Convention on the Law of the Sea. Article 2 of the Law of the Sea specifically states, in part:

> The sovereignty of a coastal State extends, beyond its land territory and internal waters and, in the case of an archipelagic State, its archipelagic waters, to an adjacent belt of sea, described as the territorial sea. This sovereignty extends to the air space over the territorial sea as well as to its bed and subsoil.[95]

The Law of the Sea also has four other significant provisions that bear upon state sovereignty. First, it allows for innocent passage of ships from all states through the territorial sea of the other states.[96] Second, the Law of the Sea recognizes additional zones, such as contiguous zones and exclusive economic zones, that may extend farther out than 12 miles and are not considered part of sovereign territorial sea.[97] Third, the Law of the Sea requires states to monitor and control ships that are flying under their flags. [98] Among other duties, the treaty requires each state to "maintain a register of ships containing the names and particulars of ships flying its flag." [99] Finally, the Law of the Sea

---

[93] *Id.* at 60-61.
[94] *Id.* at 60-62.
[95] UNCLOS, *supra* note 68, at pt. II, § 1.
[96] *Id.* at pt. II, § 3.
[97] *Id.* at pt. II, § 4, *and* pt. V.
[98] *Id.* arts. 91-95.
[99] *Id.* art. 94.

established the International Tribunal for the Law of the Sea (ITLOS) as a forum to settle disputes.[100]

B. Air Sovereignty

Roman civil law considered the air *res omnium communes*, or something that "was incapable of being the object of a private right" and thus common to all.[101] However, as property rights continued to develop throughout the centuries, Western thought treated the owner of the land as the owner of the air above it. This thought was expressed via the maxim *"cujus est solum, ejus est summits usque ad coelum,"* or "he who owns the soil owns it up to the sky."[102] However, with the beginning of the age of flight, the law quickly recognized that the idea of the landowner owning all the air above the land would lead to absurd results such as the concept of aerial trespass.[103] Thus, courts began to acknowledge the fact that at some point in the undefined "upper air," private ownership ended.[104]

Whereas the age of flight curtailed the idea of private ownership of air, it also brought on the concept of air sovereignty.[105] In response to German balloons, mostly piloted by military aviators, crossing French borders without regulation or permission, France requested and held the first diplomatic conference regarding aviation in 1910.[106] This conference considered the question of sovereignty, yet reached no agreement.[107] The prevailing views broke down into two main categories, those who supported freedom of the air and those who supported air sovereignty.

These categories were further broken down and summarized during a meeting of the International Law Association. Specifically, "freedom of the air" encompassed: (a) air freedom without restriction, (b) air freedom restricted by some special rights (not limited by height) of the subjacent states, and (c) air freedom restricted by a territorial

---

[100] *Id.* at annex VI.

[101] Charles Anthony Roberts, Air Sovereignty and International Law, at 5-7 (1959) (unpublished M.A. thesis, on file with Muir S. Fairchild Research Information Center at Maxwell Air Force Base, Alabama).

[102] *Id.* at 5.

[103] During the early 1900s, international organizations such as the Institute for International Law and the International Law Association examined and contemplated appropriate legal principles governing air. *Id.* at 9.

[104] *Id.* at 9-12.

[105] *Id.* at 30-33.

[106] *Id.* at 37; *see also* JOHN C. COOPER, *Legal Problems of Upper Space*, *in* EXPLORATIONS IN AEROSPACE LAW: SELECTED ESSAYS BY JOHN COBB COOPER, 1946-1966, ch. 14 (Ivan A. Vlasic ed., McGill Univ. Press 1968).

[107] Roberts, *supra* note 101, at 37.

zone.[108] "Air sovereignty" encompassed: (a) full sovereignty up to a limited height, (b) full sovereignty restricted by the right of innocent passage for aerial navigation, and (c) full sovereignty without any restrictions.[109]

Early in the age of flight, the increasing number of flight across the borders of European countries and across the English Channel forced resolution of the issue of air sovereignty. With no international agreement governing air, state practice began to establish international law regarding air sovereignty. Britain acted first, passing regulatory statutes in 1911 and 1913 that established its claim of sovereignty of the air over all of its land and territorial water and its ability to regulate any foreign aircraft within its jurisdiction.[110] Soon, other states took actions—such as formal declarations or shooting at airplanes that flew over their territory—that established the idea of air sovereignty over their respective land and territorial waters as well.[111] The actions of various states throughout World War I (WWI), especially neutral countries' refusal to allow overflight, firmly established air sovereignty as customary international law by the end of the war.[112]

Eventually, in 1919, 27 contracting parties signed the Convention for the Regulation of Aerial Navigation in France.[113] Commonly known as the Paris Convention, this convention codified the existing customary international law of air sovereignty. Article 1 stated, in part, "The high contracting parties recognize that every Power has complete and exclusive sovereignty over the airspace above its territory."[114] Equally as important, the Convention nominally established the idea that states had the right of innocent passage across the airspace and above the territory of other states.[115] This fundamental concept of air sovereignty continued, specifically with the Convention on International Civil Aviation, commonly referred to as the Chicago Convention, which states first signed in 1944 and have updated eight times, most recently in 2006.[116] Regardless of how the Convention changed over the years, Article I of the Chicago Convention has consistently stated, "[t]he contracting States recognize that every State

---

[108] *Id.* at 39.
[109] *Id.* at 39.
[110] *Id.* at 45-46.
[111] Roberts, *supra* note 101, at 46-48; *see also* DAVID H. N. JOHNSON, RIGHTS IN AIR SPACE 32 (Manchester Univ. Press 1965).
[112] Roberts, *supra* note 101, at 49-55; *see also* JOHNSON, *supra* note 111, at 32-33.
[113] Convention for the Regulation of Aerial Navigation, Oct. 13, 1919, 11 LNTS 173.
[114] *Id.*
[115] *Id.* arts. 2 & 15.
[116] *See* The Convention on International Civil Aviation, December 7, 1944, 61 Stat. 1180, 15 U.N.T.S. 295, *available at* http://www.icao.int/icaonet/dcs/7300.html .

has complete and exclusive sovereignty above its territory."[117] However, the Chicago Convention does not recognize the right of innocent passage as set forth in the Paris Convention. Nonetheless, the Chicago Convention does address such matters as overflight rights and aircraft nationality, and also established the International Civil Aviation Organization to govern these issues.[118] Significantly, the Chicago Convention also requires aircraft to be registered in a state and "bear its appropriate nationality and registration marks," and further requires that States provide registration and ownership information upon request.[119]

C. Outer Space Sovereignty

While states ultimately resolved the issue of state sovereignty in air, they left unresolved the question of how high sovereignty extended. The implicit solution was to simply apply the Roman maxim quoted earlier that "he who owns the soil owns it up to the sky" to international law. However, as rocket technology developed and the promise of satellites grew, so did questions as to how far up a state's sovereignty extended.

Some people advocated the theory that sovereignty extended infinitely; however, scholars dismissed this theory when considering both its application and the laws of planetary science.[120] First, because the Earth rotates on its axis and further revolves around the sun, humans have no ability to mark a fixed location in space. Moreover, if states could extend their sovereignty infinitely, the moon and other celestial bodies would effectively transfer from the sovereign territory of one state to the next as the various bodies rotated and revolved.[121] Finally, some recognized the fact that sovereignty can only truly exist if states can exert control, or sovereignty over the areas they claim.[122]

---

[117] The Convention on International Civil Aviation, *supra* note 116, part I, chap. I, art. 1.
[118] *Id.* at part II.
[119] *Id.* at part I, chap. III.
[120] GYULA GÁL, SPACE LAW 61-70 (Oceana Publ'n 1969).
[121] Additionally, as one commentator noted, "the idea of sovereignty over the various sectors of the universe is just as ridiculous as if the Island of St. Helena claimed the Atlantic Ocean." *Id.* at 67.
[122] Despite these obvious problems, experts from the two leading space powers in the late 1950s and early 1960s—the Soviet Union and the United States—nonetheless continued to advocate the notion that state sovereignty extended into outer space. Specifically, "Soviet commentators, while declaring that Soviet satellites have not violated international law . . . simultaneously claimed that Soviet airspace sovereignty extends to infinity" while the "Legal Advisor to the United States State Department in 1958 suggested that American sovereignty may extend upward for ten thousand miles, which is far beyond many present satellite orbits." Note, *supra* note 79, at 1167. Amusingly, a Soviet legal expert suggested, perhaps facetiously, that Sputnik did not pass over other states, but that other states passed under Sputnik as the Earth rotated.

As the international community began to generally accept the idea that sovereignty could not extend infinitely into the sky, it turned its focus to two important questions: determining the legal status of outer space and drawing the demarcation line between airspace and outer space. With regard to the legal status of outer space, many scholars drew an analogy from the high seas, arguing that the upper atmosphere, which like the high seas is beyond any state's control, is a zone of "open air."[123] Additionally, some scholars also looked back directly to the same principle of *res communis omnium* from Roman civil law that scholars also used when analyzing sovereignty in airspace and on the seas.[124] While not explicitly using the phrase "*res communis omnium*," state practice evidenced the belief that state sovereignty did not extend to outer space.[125] One authority noted that "(1) neither the United States nor the Soviet Union asked permission of other states before launching satellites over their territory, (2) no state has protested against such flights, and (3) the United Nations has passed certain resolutions in which the principle of national sovereignty in space is implicitly rejected."[126]

In 1967, the Outer Space Treaty solidified the legal status of outer space as free from sovereignty.[127] Article II of the Outer Space Treaty specifically states, "Outer space, including the Moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means."

The Outer Space Treaty included other provisions that bear on sovereignty. Specifically, it made clear that states were responsible for "national activities in outer space . . . whether such activities are carried on by governmental agencies or by non-governmental entities, and for assuring that national activities are carried out in conformity with the

---

Philip W. Quigg, *Open Skies and Open Space*, vol. 37, no. 1 FOREIGN AFF., Oct., 1958, at 95.

[123] For example, G.P. Zadorozhny, a Soviet professor of international law, stated days after Sputnik's launch, "By analogy to the principle of freedom of the high seas, which beyond the limits of territorial waters and special maritime zones do not belong to anyone and are in general use by all nations, the upper atmosphere, which is beyond the limits of effective air control by states, can likewise be considered a zone of open air, in general use by all nations." Gál, *supra* note 120, at 117.

[124] *Id.* at 122-129.

[125] As John C. Cooper, a noted legal scholar in both air and space, stated in March 1958, "The course of international conduct since the satellite flights were announced is consistent with no theory other than the acceptance of the principle that 'outer space' is not part of the territory of any state and may be used by all states as freely as the high seas are now used for surface shipping." Quigg, *supra* note 122, at 97.

[126] *Id.* at 97-98.

[127] Article II states, "Outer space, including the Moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means." Outer Space Treaty, *supra* note 64.

provisions set forth in the present Treaty."[128] Moreover, a later convention, the Convention on Registration of Objects Launched into Outer Space, requires states to provide information on every space launch to an international body.[129]

While the Outer Space Treaty explicitly discusses sovereignty in outer space, it does not resolve the issue of the demarcation line between airspace and outer space. Theories for where the demarcation line should be range from the outer limits of earth's gravitational field, to the earth's atmosphere, to the point where aerodynamic lift cannot be sustained, to where states can no longer exercise effective control.[130] Generally, these theories can be broken down into one group that establishes a demarcation line based upon function and one that bases the demarcation line on distance.[131] More than half a century ago, the United Nations established a committee to try to resolve this issue—an effort that remains unsuccessful.[132] This failure led to attempts by some states to extend state sovereignty far into outer space. For example, in the Bogota Declaration of 1976, "eight equatorial countries tried . . . to lay claim on the geosynchronous orbits (22,300 miles above the equator)." The reasoning put forth by these countries was that the demarcation line should be located outside Earth's gravitation pull, which objects in geosynchronous orbit use.[133] However, the international community soundly rejected their claim.[134] More conspicuously, even though China ratified the Outer Space Treaty, an "increasing number of publications by influential Chinese authors (are) advancing the principle that China's sovereignty extends through outer space."[135] The Chinese rationale for extending sovereignty into outer

---

[128] *Id.* art VI.

[129] *See* Convention on Registration of Objects Launched into Outer Space, Jan. 14, 1975, 28 U.S.T. 695, 1023 U.N.T.S. 15.

[130] GÁL, *supra* note 120, at 70-98

[131] *See generally* Alexandra Harris & Ray Harris, *The Need for Air Space and Outer Space Demarcation*, 22 SPACE POL'Y 4 (2006).

[132] To help resolve this issue, the Committee on the Peaceful Uses of Outer Space (COPUOS), which the United Nations created in 1959, and its legal subcommittee established a working group on the "definition and delimitation of outer space." Despite decades of debate, the group had been unable to resolve this issue and is unlikely to do so in the near future. *See* United Nations Office for Outer Space Affairs, United Nations Committee on the Peaceful Uses of Outer Space, http://www.oosa.unvienna.org/oosa/COPUOS/copuos.html (last visited Sept. 12, 2009).

[133] Declaration of the First Meeting of Equatorial Countries, 3 Dec., 1976, *available at* http://www.jaxa.jp/library/space_law/chapter_2/2-2-1-2_e.html.

[134] *See* Harris & Harris, *supra* note 131; *see also* NATHAN C. GOLDMAN, AMERICAN SPACE LAW: INTERNATIONAL AND DOMESTIC 68 (2d ed., Univelt 1996) (1988).

[135] Peter A. Dutton, Associate Professor, China Maritime Studies Institute, China's Views of Sovereignty and Methods of Access Control, Testimony before the U.S.-China Economic and Security Review Commission, (Feb. 27, 2008), *available at*

space is that "there is no legally accepted definition of 'outer space' that defines the demarcation point at which territorial airspace ends and outer space begins."[136]

D. Insights for Sovereignty in Cyberspace

After examining the development of sovereignty in the sea, air, and outer space, five main insights emerge.

Insight 1: An International Regime is Needed for the Development of Sovereignty in Cyberspace

Like many other concepts, there are various definitions of what constitutes a regime.[137] However, again, Stephen Krasner provides a useful construct. Specifically, he defines a regime as "a set of implicit or explicit principles, norms, rules and decision-making procedures around which actors' expectations converge in a given area of international relations."[138] Krasner defines the key terms as follows. "Principles are beliefs of fact, causation, and rectitude. Norms are standards of behavior defined in terms of rights and obligations. Rules are specific prescriptions or proscriptions for action. Decision-making procedures are prevailing practices for making and implementing collective choice."[139] Krasner continues with the key observation that "*[c]hanges in principles and norms are changes of the regime itself.* When norms and principles are abandoned, there is either a change to a new regime or a disappearance of regimes from a given issue-area."[140]

Applying these definitions and concepts to sea, air, and outer space reveals that the development of sovereignty in these domains corresponded to the development of an international regime. A basic breakdown follows in table form.

---

http://www.uscc.gov/hearings/2008hearings/written_testimonies/08_02_27_wrts/08_02_27_dutton_statement.php.

[136] *Id.*

[137] STEPHEN D. KRASNER, *Structural Causes and Regime Consequences: Regimes as Intervening Variables*, *in* INTERNATIONAL REGIMES 2 (Cornell Univ. Press 1983).

[138] *Id.*

[139] *Id.*

[140] *Id.* at 3-4 (emphasis in original).

	Principles	Norms	Rules/Procedures
Sea	The high seas should be open to every state, although states have valid territorial interests beyond their coasts	The sovereignty of a coastal State extends, beyond its land territory and internal waters and, in the case of an archipelagic State, its archipelagic waters, to an adjacent belt of sea, described as the territorial sea.	The Law of the Sea and ITLOS
Air	The air above a state is part of the territory of that state	Every state has complete and exclusive sovereignty over the airspace above its territory	Chicago Convention and ICAO
Outer Space	Outer space belongs to all humankind	Outer space, including the moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means.	Outer Space Treaty and COPUOS

Table. International Regime Breakdown

Moreover, if the principles or norms change in any of the respective regimes, the regime itself would almost certainly disappear or change. For example, if a state claimed sovereignty over the moon in outer space and could reasonably be expected to enforce its claim, the outer space regime would likely dissolve because the basic principle that outer space belongs to all humankind would no longer be valid. Alternatively, states could collectively establish a new regime encompassing a new sovereignty principle norm. For example, the new principle might be "states can claim sovereignty over the moon and other celestial bodies" and the new norm might be "outer space is not subject to national appropriation by claim of sovereignty, but the moon and other celestial bodies are."

Thus, for sovereignty in cyberspace to become a reality, states must form a consensus regarding the underlying principles and norms from which an international regime would merge. A possible principle might be "every state has a right to access cyberspace for peaceful purposes, but states have a valid interest in asserting and protecting their

sovereignty in cyberspace." Failure to agree on underlying principles and norms, however, will prevent an international regime from forming. This insight underscores one of Krasner's concepts of sovereignty stated in the introduction: to have sovereignty other states must recognize that sovereignty.[141]

Insight 2: State Interests Eventually Trump Initial Utopian Ideals

When states and individuals started developing the technological capability to enter the domains of sea, air, and outer space, strong arguments existed for each of these domains to remain free from sovereign control. However, state interests, such as trade and national security, combined with a state's technological capabilities, ultimately prevailed over these arguments and determined the current legal status of these domains.[142]

Similarly, cyberspace is still in its infancy, and like the infant stages of other domains, people are strongly advocating against government interference, and assertion of sovereignty, in cyberspace. However, as discussed in Section II, states are beginning to recognize and assert their interests in cyberspace. As states' interests crystallize and grow as technology merges and matures, states will likely want to exert more and more control in cyberspace. As a result, borrowing from the style of John Barlow[143]: *People of the Cyber World, you light speed stream of ones and zeros. I come from the Real World, the home of the state. On behalf of the present, I demand you follow our rules or you will not be welcome here. We have absolute sovereignty wherever you gather.*

Insight 3: State Practice Matters

While the determination of sovereignty in the areas of sea, air, and outer space ultimately required an international regime, state practice influenced those emerging international regimes. In the sea domain, most states did not exert control over the high seas, but established control, or at least made claims of sovereignty, extending into the seas from their coasts.[144] In the air domain, neutral states in WWI made it clear that warring states could not use their airspace and

---

[141] *See supra* notes 32-33 and accompanying text.
[142] *See supra* notes 75-136 and accompanying text. Of course, this means that a change in state interests or technological capabilities might change the legal status of these domains.
[143] Barlow, *supra* note 45 (with apologies).
[144] *See supra* notes 75-100 and accompanying text.

most states claimed absolute sovereignty over their airspace.[145] In the outer space domain, very few states made claims of sovereignty into outer space and few states claimed that another state's space objects orbiting in outer space violated their sovereignty.[146]

Currently, states are essentially silent on the issue of state sovereignty in cyberspace. Specifically, although a state can often determine a cyberattack's country of origin, rarely, if ever, does a state claim that the country violated its sovereignty. States, furthermore, are not publicly responding to cyberattacks, which could establish precedents in practice. As one commentator noted, a few years ago United States officials were hesitant to talk about cyberattacks for fear that doing so would acknowledge that an act of war occurred, which required a similar response.[147] However, recently U.S. officials are more open about cyberattacks and do not respond as if there is a requirement for "any sort of offline retaliation."[148] Ultimately, such practices will influence future attempts to establish sovereignty in cyberspace.

Insight 4: Identification of Actors in Domain is Vital

In each respective domain, the ability for a state to track and identify actors is a fundamental requirement. In the sea domain, most vessels traveling in international waters are required to register with a state. More significantly, the Automatic Identification System (AIS), "a maritime navigation safety communications system standardized by the International Telecommunication Union (ITU) and adopted by the International Maritime Organization (IMO)" recently became operational.[149] The AIS "provides vessel information, including the vessel's identity, type, position, course, speed, navigational status and other safety-related information automatically to appropriately equipped shore stations, other ships, and aircraft; . . . and exchanges data with shore-based facilities" and "similarly fitted ships."[150] In the air domain, aircraft are required to register with a state and that state must provide information on that aircraft when required. Additionally, aircraft carry transponders that provide in-flight information pertaining to

---

[145] *See supra* notes 105-119 and accompanying text.
[146] *See supra* notes 120-136 and accompanying text.
[147] Ben Worthen, *Is a Cyber Attack an Act of War?*, WALL ST. J., Aug. 14, 2008, *available at* http://blogs.wsj.com/biztech/2008/08/14/is-a-cyber-attack-and-act-of-war/.
[148] *Id.*
[149] U.S. Dep't of Homeland Sec., U.S. Coast Guard, The Navigation Center of Excellence, Frequently Asked Questions, http://www.navcen.uscg.gov/enav/AIS/AISFAQ.htm#1 (last visited Aug. 24, 2009).
[150] *Id.*

identification, location, and heading. Finally, in the space domain, states are required to provide the following information when launching an object into space: the name of launching state or states, an appropriate designator of the space object or its registration number, date and territory or location of launch, basic orbital parameters, and the general function of the space object.[151] Moreover, the state is responsible for the activities of non-governmental entities in outer space.[152]

With regard to cyberspace, the lack of attribution is one of the greatest difficulties surrounding cyber attacks. While a state can often trace cyberattacks back to a specific country and a specific ISP, it typically cannot identify the individual actor without help from the country of origin, if at all. As demonstrated in the other domains, a key to establishing sovereignty in cyberspace is gaining the ability to identify actors and thus trace back cyberattacks, or other acts in cyberspace, to specific individuals or computers. Thus, if an international regime forms regarding sovereignty in cyberspace, an agreement between states on the need to track and identify specific actors in cyberspace will likely also emerge. Section IV will examine briefly the question of whether this is feasible.

Insight 5: States Must Be Able to Exert Control

As stated in Section I, the ability to control both territory and transborder movements is an important factor in establishing sovereignty, and control played an important role in the development of sovereignty in all three domains.[153] In the sea domain, the concept of territorial waters developed, in part, from the capability of a state to fire a cannon from its shore, and the concept of "open sea" developed from the lack of capability of states to exert control over the high seas.[154] Moreover, states have proved capable of addressing violations of their territorial waters by using force against the violator.[155] In the air domain, states have the capability to track violations of their air sovereignty and have proved capable of using force against violators to

---

[151] Convention on Registration of Objects Launched into Outer Space, *supra* note 129, Article IV.

[152] *See supra* notes 128-129 and accompanying text.

[153] *See supra* notes 33-36 and accompanying text.

[154] *See supra* notes 84-91 and accompanying text.

[155] For example, in March 2007, Iran detained 15 sailors from the United Kingdom for allegedly entering Iran's territorial waters. Associated Press, *U.K. Says 15 Sailors Detained by Iranian Navy*, MSNBC, Mar. 23, 2007, *available at* http://www.msnbc.msn.com/id/17752685/.

enforce that sovereignty.[156] Finally, in the outer space domain, the inability of any state to exert any sort of control in outer space significantly contributed to The Outer Space Treaty, prohibiting the extension of sovereignty into outer space.[157] However, as states gain the technological ability to assert control in outer space, the current outer space regime may be changed significantly, or disappear altogether.[158]

Similarly, for sovereignty to develop in cyberspace, states must be able to exert control in cyberspace. As with the other domains, this encompasses the capacity of a state to protect its borders. More importantly, this also encompasses the capacity of a state to respond directly to any violation of that sovereignty. While the exact means a state would use to address a specific violation of its sovereignty in cyberspace is beyond the scope of this article, it is important to note that states defend their sovereignty in other domains by resorting to force and similar responses could be expected for violations of sovereignty in cyberspace.[159]

The development of sovereignty in the sea, air, and outer space domains were all distinct, yet shared significant similarities. These similarities, in turn, provide significant insights into how sovereignty can develop in the cyberspace domain as well. First, the development of sovereignty in cyberspace requires an international regime. Second,

---

[156] *See supra* note 111 and accompanying text. In addition to the U-2 incident in 1960 previously mentioned in Chapter One, numerous other incidents have involved the shooting down of military aircraft that violated, or at least allegedly violated, another state's sovereignty. *See supra* note 28 and accompanying text; JOHNSON, *supra* note 111, 70-74. The most notable recent cases involved the incident between the US Navy EP-3 and Chinese F-8 in which China alleged the aircraft was violating its sovereignty by conducting a reconnaissance mission over China's exclusive economic zone. EMBASSY OF THE P.R.C. IN THE U.S., U.S. SERIOUSLY VIOLATES INTERNATIONAL LAW (Apr. 15, 2001), http://www.china-embassy.org/eng/zt/zjsj/t36383.htm (last visited Aug. 27, 2009).

[157] *See supra* notes 120-22 and accompanying text.

[158] Unlike the other domains of land, sea, and air, no state has been compelled to use force to defend its sovereignty or sovereign interests in outer space. Additionally, no state has used force to defend its right to use outer space, nor has a state used force to assert its sovereignty in outer space. However, states have used force against objects (e.g., satellites) other states have placed in outer space. Specifically, China "has secretly fired powerful laser weapons designed to disable American spy satellites by 'blinding' their sensitive surveillance devices." Francis Harris, *Beijing Secretly Fires Lasers to Disable US Satellites*, TELEGRAPH, Sept. 26, 2006, http://www.telegraph.co.uk/news/worldnews/1529864/Beijing-secretly-fires-lasers-to-disable-US-satellites.html (last visited Aug. 27, 2009). This capability is in addition to the anti-satellite capabilities some countries are developing that destroy satellites. Thus, even though outer space is a global commons and state sovereignty does not extend into outer space, states are beginning to appreciate the need to both protect their space assets against force and to use force to respond to attacks against their space assets.

[159] Of course, what constitutes "use of force" in cyberspace is also a contested area. *See* SHARP, *supra* note 22; WINGFIED, *supra* note 22.

states must critically assess their interests in cyberspace, because those interests will eventually trump the desires of those actors who want cyberspace to remain free from state sovereignty. Third, current state practice regarding the concept of sovereignty in cyberspace, as well as how a state responds to violations of its sovereignty in cyberspace, will influence how, and if, an international regime governing sovereignty in cyberspace ultimately develops. Fourth, the capability to identify specific actors in cyberspace will become an important requirement. Finally, a state must be able to exert control of cyberspace and respond to those actors who violate its sovereignty in cyberspace.

IV. ISSUES CONFRONTING STATE SOVEREIGNTY IN CYBERSPACE

Using the insights gained from examining the development and limits of sovereignty in other domains, this chapter examines the practical considerations of attempting to establish state sovereignty in cyberspace. Specifically, states must address four significant issues before they can realize sovereignty in cyberspace.

A. Recognizing Cyberspace as a Sovereign Domain

The most fundamental issue facing the development of sovereignty in cyberspace is persuading states that cyberspace is a domain over which they can assert sovereignty. In 2006, the Secretary of Defense signed the *National Military Strategy for Cyberspace Operations*, which states, in part, that cyberspace is its own domain, along with the other recognized domains of land, sea, air, and space.[160] However, treating cyberspace as a separate domain is not without controversy. In fact, even some within the Department of Defense believe that cyberspace does not constitute a domain.[161] While important, the debate over whether cyberspace is technically a domain should not obscure the more fundamental fact that cyberspace is a human creation, and thus states can assert control over, and shape, cyberspace.

As discussed in Section II, cyberspace requires a physical architecture to exist, cyberspace needs governmental regulation to function effectively, and states are attempting to exert increasing control over cyberspace.[162] More importantly, "there is no intrinsic reason why

---

[160] *See* U.S. DEP'T OF DEF., THE NATIONAL MILITARY STRATEGY FOR CYBERSPACE OPERATIONS 3 (2006), *available at* http://www.dod.mil/pubs/foi/ojcs/07-F-2105doc1.pdf [hereinafter NMS-CO].

[161] *See* David R. Luber & David H. Wilkinson, *Defining Cyberspace for Military Operations*, 93 MARINE CORPS GAZETTE, Feb. 2009, at 40.

[162] *See supra* notes 46-57 and accompanying text.

cyberspace cannot be made more territorial."[163] As a "human creation," cyberspace and its foundational technology are political, "shap[ed] by social actions and institutions."[164] "Global digital networks have the features they do—of placelessness, anonymity, and ubiquity—because of politics, not in spite of them."[165] Therefore, regardless of beliefs about the cyberspace domain, states have the capability to transform it into a domain in which they can exert their sovereignty.

As discussed in the previous section, a state's current practices will influence its future ability to assert any claims of sovereignty in cyberspace. Thus, states must first accept that cyberspace is, or at the very least can be, a domain in which they can exert sovereignty. States must then take additional steps to shape cyberspace to make it easier for them to assert their sovereignty.

B. Wanting Sovereignty in Cyberspace

While recognizing that cyberspace is a domain where states can assert their sovereignty is a fundamental problem, the larger question is whether states even want sovereignty in cyberspace. Developing sovereignty ultimately requires an international regime with specific rules and procedures regulating state activity in that domain, including a requirement to identify and track transnational actors. Certain states, however, may oppose state sovereignty in cyberspace and the international oversight that results. Examining the possible motivations of the United States and China gives insight into this proposition.

An unfettered cyberspace offers the United States an enhanced potential to spread American, or democratic, ideals and virtues. As articulated in the 2006 *National Security Strategy* (NSS),

> The United States has long championed freedom because doing so reflects our values and advances our interests. It reflects our values because we believe the desire for freedom lives in every human heart and the imperative of human dignity transcends all nations and cultures. Championing freedom advances our interests because . . . promoting democracy is the most effective long-term measure for strengthening international stability, reducing regional conflicts, countering

---

[163] Geoffrey L. Herrera, Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space 12 (prepared for the 47th Ann. Int'l Stud. Ass'n Convention, Mar. 22-25, 2006), *available at* http://www.allacademic.com/meta/p98069_index.html.
[164] *Id.* at 11.
[165] *Id.* at 11-12.

terrorism and terror-supporting extremism; and extending peace and prosperity.[166]

Considering these objectives, cyberspace generally, and the Internet specifically, provide the ideal medium for the United States to both spread democracy and engage in the battle of ideas. Because the United States believes that every human yearns to be free, securing a forum for the free expression and exchange of ideas to take place is a key means of spreading freedom. Thus, the United States can meet its objectives indirectly by advancing a free and open Internet.

While this is an idealistic view, evidence increasingly demonstrates that the Internet's impact furthers the interests of the United States. For example, the Internet has changed the interaction between the Chinese state and society by undermining the communist regime's monopoly of information and allowing for the formation of a "digitally mediated civic society;" providing a public space for civilians to engage in politics; and fostering public distrust of public institutions.[167] Despite these positive outcomes, China's political liberalization is not the same as political democratization, but it is still an important step towards political democratization, and one that the United States would find in line with its national security strategy.[168]

Iran is another country where the United States would consider cyberspace a positive influence. As of 2005, nearly 100,000 blogs had sprung up in Iran, and Iranians were increasingly relying on the Internet for news and opinion.[169] Moreover, after Iranian bloggers and online journalists were confined and tortured, public protests resulted in the release of many those arrested.[170] More recently, the Internet played a significant role in both organizing protests after the controversial Iranian

---

[166] GEORGE W. BUSH, THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES 3 (2006), *available at* http://www.strategicstudiesinstitute.army.mil/pdffiles/nss.pdf. The NSS continues, "From the beginning, the War on Terror has been both a battle of arms and a battle of ideas—a fight against the terrorists and against their murderous ideology. . . . In the long run, winning the war on terror means winning the battle of ideas, for it is ideas that can turn the disenchanted into murderers willing to kill innocent victims." *Id.* at 9.

[167] YONGNIAN ZHENG, TECHNOLOGICAL EMPOWERMENT: THE INTERNET, STATE, AND SOCIETY IN CHINA 103-34 (Stan. Univ. Press 2008). Zheng concluded that the Internet "has played an important role in facilitating political liberalization [through collective action] in different aspects such as political openness, transparency, and accountability." *Id.* at 11.

[168] *Id.* at 186.

[169] Omid Memarian, *Internet Yearns to Be Free in Iran*, SAN FRANCISCO CHRON., Dec. 9, 2005, http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2005/12/09/EDG7VG4KK31.dtl (last visited Aug. 27, 2009).

[170] *Id.*

presidential election in June 2009 and showing the rest of the world the brutality with which the Iranian regime responded.[171]

While a free and open Internet greatly facilitates U.S. goals to spread democracy and freedom, a strong international regime regulating sovereignty in cyberspace, might provide states a greater opportunity and capability to control speech and the spread of information by allowing them to monitor cyberspace content and individual actors more closely. Moreover, the United States might also oppose state sovereignty in cyberspace because it views itself as the dominant cyber power that would benefit the most from a cyberspace free from state sovereignty.[172] While the media often reports about cyberattacks against the United States, news outlets seldom mention U.S. actions in cyberspace. However, the lack of news regarding U.S. activity in cyberspace does not mean the activity does not exist. For example, an article on the leak of an Osama Bin Laden video reported that a "commercial intelligence firm that specializes in intercepting al-Qaeda's Internet communications, often by clandestine means," uncovered "a security gap in the terrorist group's internal communications network" and learned of an upcoming Osama Bin Laden video.[173] While a commercial company was behind the leak, this example highlights how organizations within the United States are conducting cyberattacks against other computer networks, presumably in other countries.

China may also prefer to preclude state sovereignty in cyberspace because cyberspace offers China possible asymmetric advantages when confronting the United States. American experts note that cyberattacks "even the playing field" because the U.S. infrastructure relies so heavily on Internet and online technologies.[174] China apparently agrees with this assessment, believing that U.S. dependency

---

[171] *See e.g.*, Patrick Quirk, *Iran's Twitter Revolution,* FOREIGN POL'Y IN FOCUS, June 17, 2009 (discussing the influence of technology in the aftermath of the 2009 Iranian presidential election), http://www.fpif.org/fpiftxt/6199 (last visited Sept. 10, 2009).

[172] Moreover, the United States is open about its belief that it has advantages in cyberspace and promoted this belief in the *National Military Strategy to Secure Cyberspace* (NMS-CO) when it stated, "the United States currently enjoys technological advantages in cyberspace."[172] Although the NMS-CO went on to state that "these advantages are eroding," the fact remains that the United States believes it has the advantage. NMS-CO, *supra* note 160, at 9.

[173] Joby Warrick, *U.S. Intelligence Officials Will Probe Leak of Bin Laden Video,* WASH. POST, Oct. 10, 2007, at A13, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/10/09/AR2007100902055.html.

[174] William Matthews, *Security Experts: Cyberattacks Will Increase,* A.F. TIMES, Nov. 4, 2008 (quoting Howard Schmidt, a former cybersecurity adviser to the White House), http://www.airforcetimes.com/news/2008/11/airforce_cyberattacks_110408/ (last visited Aug. 27, 2009).

on information technology "constitutes an exploitable weakness."[175] Four main reasons motivate the Chinese: the comparatively low costs of cyber operations, the difficulty of tracing a cyberattack's source, the chaos such attacks can create, and the "underdeveloped legal framework to guide responses."[176] Thus, establishing state sovereignty in cyberspace could restrict Chinese freedom of action in this militarily relevant domain.

Furthermore, state sovereignty in cyberspace might also force a degree of openness that China does not want. Examining the development of sovereignty in sea, air, and outer space shows that the respective regimes acknowledged some form of innocent passage or made allowances for the transborder movement of other states.[177] Transferring this concept to cyberspace, developing sovereignty might require agreed-on rules and procedures for when and what type of content or information can pass through cyberspace, across borders, and directly to the citizens of each state. As Article 19 of the Universal Declaration of Human Rights states, "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[178] Thus, any international regime regarding cyberspace might incorporate these values; something that China might oppose.

Finally, both the United States and China may now prefer cyberspace without sovereignty because cyberspace capabilities

---

[175] U.S.-CHINA ECON. AND SECURITY REV. COMM'N, 2008 ANNUAL REPORT TO CONGRESS 166 (2008), *available at* http://www.uscc.gov/annual_report/2008/annual_report_full_08.pdf.

[176] *Id.* at 167.

> China is likely to take advantage of the U.S. dependence on cyber space for four significant reasons. First, the costs of cyber operations are low in comparison with traditional espionage or military activities. Second, determining the origin of cyber operations and attributing them to the Chinese government or any other operator is difficult. Therefore, the United States would be hindered in responding conventionally to such an attack. Third, cyber attacks can confuse the enemy. Fourth, there is an underdeveloped legal framework to guide responses.

Id.

[177] Specifically, as discussed earlier, states are sovereign in their territorial waters, but ships from other states have a right of innocent passage in those territorial waters. *See supra* note 96 and accompanying text. Moreover, states have sovereignty in the air above their territory, but the regime also provides rules and procedures governing how airplanes from one state can enter and traverse the airspace of another state. *See supra* note 118 and accompanying text.

[178] Universal Declaration of Human Rights, G.A. Res. 217A, U.N. GAOR, 3d Sess., 1st plen. mtg., U.N. Doc. A/810 (Dec. 12, 1948).

continue to grow and neither state wants to prematurely limit future operations. With the continual expansion of cyberspace's potential and capability, states might want to wait to enter agreements that define acceptable and prohibited activity until they obtain a better understanding of cyberspace's strategic potential. While states can withdraw from international agreements, such actions are not without some costs.

In sum, the United States and China may have valid reasons for not wanting sovereignty in cyberspace to exist, reasons that other states may share. Although no one can predict the conditions under which an international consensus towards sovereignty in cyberspace might evolve or how long that development might take, the process will begin only after more and more states realize that cyberspace is a domain where they can exert sovereignty and that it is in their interests to do so.

C. Civilian Expectations

Another challenge to state sovereignty in cyberspace comes from global views regarding the ability to access the Internet freely and anonymously. For example, a French measure to cut off Internet connections to individuals who persisted in illegally downloading movies and music recently passed only after early defeats and vocal opposition.[179] Additionally, a European Union directive that would "require all Internet service providers to retain information on email traffic, visits to websites and telephone calls made over the Internet, for 12 months" prompted outraged response from various privacy groups over its gestapo-like intrusions.[180] If states were to impose sovereignty in cyberspace, they would require greater identification of cyberspace actors. That in turn would likely result in a large outcry from individuals who presume that anonymous activity in cyberspace is both

---

[179] Many members of the National Assembly skipped the initial vote on the measure, which had always been unpopular with ordinary voters, and it was initially defeated in what some characterized as a "victory for the citizens and the civil liberties over the corporate interests." Eric Pfanner, *France Rejects Plan to Curb Internet Piracy*, N.Y. TIMES.COM, Apr. 9, 2009, http://www.nytimes.com/2009/04/10/technology/internet/10net.html (last visited Aug. 27, 2009). Ultimately, the National Assembly, which Sarkozy's party controls, passed the measure in a later vote, though lawsuits are expected. AFP, *French Parliament Adopts Tough Internet Piracy Bill*, May 12, 2009, http://www.google.com/hostednews/afp/article/ALeqM5i1XOUmbCAIkSpiwtCgSncSr2mtkw (last visited Aug. 27, 2009).

[180] David Barrett, *Internet Records to be Stored for a Year*, TELEGRAPH, Apr. 5, 2009, http://www.telegraph.co.uk/scienceandtechnology/technology/technologynews/5105519/Internet-records-to-be-stored-for-a-year.html (last visited Aug. 27, 2009). Various privacy groups were outraged, with one group even stating, "[t]his is the kind of technology that the Stasi [the secret police of East Germany] would have dreamed of." *Id.*

a current reality and a right. Despite a state's interests in establishing sovereignty in cyberspace, individuals also have valid privacy interests that must be accounted for, and protected, by any international regime.

D. Technical Issues Regarding Sovereignty

Finally, states face numerous technical challenges in attempting to impose sovereignty in cyberspace. While the detail of these technical challenges is outside the scope of this article, they do exist, but so do solutions. This section briefly addresses two issues and provides possible solutions. First, creating a system that can specifically identify actors in cyberspace is a daunting task. One possible solution is something akin to the DOD's common access card (CAC), which members use to log into DOD computer systems and also allows tracking in cyberspace.[181] Similarly, the state, or some other designated organization, could issue a specific CAC that the individual must use to gain access to an ISP that can access information from other states. Alternatively, users wanting to access the Internet globally could be required to use a biometric scanner before continuing. In either situation, states—or a designated international body established as part of an international cyberspace regime—could then trace back the illegal movements of specific actors in cyberspace.

The second issue is that states must also be able to establish a cyberspace border that a state can both monitor and control. Without the capability to perform this function, the concept of sovereignty in cyberspace is meaningless. One approach is to establish Internet border inspections similar to the physical border crossings that exist today.[182] This approach relies on the limited number of entry and exit points that route Internet traffic in and out of the United States. Thus, the United States could perform basic searches looking for specific IP header information such as IP addresses.[183]

While these solutions are far more complex than discussed here, still, "there is no intrinsic reason why cyberspace cannot be made more territorial."[184] States have the power to shape cyberspace in a manner that makes both actor identification and border control easier. While overcoming these technical issues is daunting in terms of technical

---

[181] *See* DoD Common Access Card, Welcome to the Next Step in Homeland Security, http://www.cac.mil/ (last visited Sept. 12, 2009).

[182] Captain Oren K. Upton, Asserting National Sovereignty in Cyberspace: The Case for Internet Border Inspection (June 2003) (unpublished M.A. thesis, Naval Postgraduate School), *available at* http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA417582&Location =U2&doc=GetTRDoc.pdf.

[183] *Id.* at 45-55.

[184] Herrera, *supra* note 163.

ability and cost, the costs of not having sovereignty in cyberspace is daunting as well. For example, the cost of defending the DOD against cyberattack in a recent six-month period was more than $100 million.[185] More importantly, the cost to the United States of a successful cyberattack against its critical infrastructure could be in the billions or more. Thus, overcoming these technical issues is worth the investment.

States must overcome a number of problems to make sovereignty in cyberspace a reality. This chapter addressed four problems, although there are numerous more—both known and unknown. The technical problems highlighted here are probably the least problematic of the four; if states want sovereignty to exist in cyberspace, then they will find a way to overcome the technical difficulties. Moreover, influencing states to recognize cyberspace as a domain and persuading individuals to accept greater control in cyberspace may also be challenging. However, perhaps the greatest obstacle facing sovereignty in cyberspace is from states that do not want state sovereignty in cyberspace and the international regime governing cyberspace that would need to emerge.

V. CONCLUSION

Without question, cyberspace offers staggering possibilities to mankind. Individuals and states have correctly seized upon these possibilities and flung themselves into cyberspace, looking to take advantage of its opportunities and leverage its capabilities. Unfortunately, this rush into cyberspace created significant vulnerabilities—military, economic, and social—that individuals, organizations, and states alike continue to exploit. As with other technologies, individual states and the international community as a whole must catch up to cyberspace in terms of creating laws and institutions that can regulate, protect, and punish activity in cyberspace. The fundamental step that states need to take is recognizing and establishing state sovereignty, the foundational principle of the current international order, in cyberspace.

While examining the possibilities for sovereignty in cyberspace, states must realize that cyberspace neither is immune from state sovereignty nor can it be considered a global commons. Moreover, the development of state sovereignty in the sea, air, and outer space domains offers insights as to how state sovereignty might develop in cyberspace. A major insight is that an international regime is needed to

---

[185] Jim Garamone, *Cyber Defense Cost Pentagon $100 Million in Six Months, Officials Say*, AM. FORCES PRESS SERVICE, Apr. 8, 2009, *available at* http://www.defenselink.mil/news/newsarticle.aspx?id=53852.

successfully extend state sovereignty beyond a state's territorial area to these other domains. While a number of issues confront the development of state sovereignty, the main obstacle is the states' belief that sovereignty in cyberspace and an international regime governing cyberspace might be contrary to their best interests.

The key question thus becomes what the United States should do with regard to establishing state sovereignty in cyberspace. While the United States might have much to gain from operations in cyberspace, it may also have the most to lose. Specifically, cyberspace provides states and non-state actors the opportunity to negate the United States' conventional military advantage, circumvent its natural boundaries, and directly attack critical infrastructure inside the United States. Yet, problematically, when the United States views cyberspace, it sees a domain in which it needs to conduct military operations instead of a domain that it could shape, either on its own or collectively within the international community.

The United States could take several practical steps to develop the concept of sovereignty in cyberspace unilaterally, multilaterally, and internationally. Unilaterally, the United States could unequivocally declare that it considers its cyberspace to be part of its sovereign territory. To support this declaration, the United States can assert control over its cyberspace borders by creating a means to block traffic from ISPs or countries from which cyberattacks originate. More importantly, the United States can send a clear message to the world about cyberattacks as it has with terrorist attacks. The United States stated that it makes "no distinction between those who commit acts of terror and those who support and harbor them."[186] It could do the same by stating that it will not distinguish between those who commit cyberattacks and those who support and harbor them.

Multilaterally, the United States could reach agreements with other countries to recognize state sovereignty in cyberspace, to assist each other in tracing cyberattacks to their original sources, to identify the specific actors responsible for those cyberattacks, and to either prosecute or extradite those individuals responsible for the cyberattacks. Internationally, the United States could work within such organizations as the United Nations to establish common cyberspace principles and norms to form building blocks for a cyberspace regime. The key to these efforts—both multilaterally and internationally—is not only focusing on state actors in cyberspace, but on non-state actors as well. As expressed by Michael Chertoff, former Secretary of Homeland Security, "The modern international legal order must be predicated on a new principle, under which individual states assume reciprocal

[186] BUSH, *supra* note 166, at 12.

obligations to contain transnational threats emerging from within their borders so as to prevent them from infringing on the peace and safety of fellow states around the world."[187]

The United States can choose to take the lead in recognizing and establishing state sovereignty in cyberspace. By establishing state sovereignty in cyberspace, the United States, as well as every other state, will develop the framework to consider other cyberspace issues. Any resulting cyberspace regime will set forth acceptable activity in cyberspace, help identify and track harmful threats, and establish appropriate forums to address cyberspace issues. Alternatively, the United States can choose to continue its *ad hoc* responses to developments in cyberspace, hoping to maintain its advantage, and hoping that no other state or non-state actor will be able to attack the United States via cyberspace successfully and devastatingly. Of course, hope is not a strategy.

[187] Michael Chertoff, *The Responsibility to Contain: Protecting Sovereignty Under International Law*, vol. 88, no. 1 FOREIGN AFF., Jan./Feb. 2009, at 130, 131.