REPROGRAMMING THE WORLD: CYBERSPACE AND THE GEOGRAPHY OF GLOBAL ORDER

by

P.J. Blount

A Dissertation submitted to the

Graduate School-Newark

Rutgers, The State University of New Jersey

in partial fulfillment of the requirements

for the degree of

Doctor of Global Affairs

written under the direction of

Professor Jean Marc Coicaud

and approved by

_____

_____

_____

_____

Newark, New Jersey May 2016

ABSTRACT

Reprogramming the World: Cyberspace and the Geography of Global Order

By P.J. Blount

Dissertation Director:

Prof. Jean Marc Coicaud

This dissertation argues that Cyberspace is causing shifts in the world scale geography deployed by the international system. Starting with the observation that international law has been unable to extend its regulatory purview over the transnational technologies that constitute Cyberspace, this research attempts to construct a framework for understanding how and why the technology of Cyberspace is changing the nature of global order.

The dissertation employs a two step methodology. It first constructs a geography of Cyberspace through evaluation of the spatial, legal, and political geographies that are constructed within the architecture of the geography. It then takes this geography of Cyberspace and layers it onto international geography in order to understand how the governance assemblage of territory, authority, and rights is being challenged and changed. This second step requires the analysis of numerous international incidents in order to draw conclusions about the nature of global order when these two geographies encounter each other.

The research concludes that Cyberspace is a phenomenon that is having and will continue to have dramatic effects on the understanding and organization of world scale governance. It argues that understanding how Cyberspace is embedded in social life as well as governance structures will be increasingly important in evaluating global affairs in the future.

Acknowledgments

This research has been supported throughout by a numerous of individuals. First and foremost, I would like to thank the four scholars that served on my committee: Prof. Jean-Marc Coicaud, Prof. Yale Ferguson, Prof. Ellen Goodman, and Prof. David Post. Each of these individuals served as mentors and gave valuable feedback throughout the drafting process. In addition to their support on the committee, the scholarship of each of these individuals plays an important role in the final product, and I can truly say that their foundational influence has been an important part of my development as a scholar.

My institutional home of Rutgers, the Newark Graduate School, and the Division of Global Affairs for providing financial support in the form of fellowships.

I would also like to thank Prof. Joanne Gabrynowicz who asked me to develop an International Telecommunications Law class at the University of Mississippi School of Law. The material gathered for this course was the bedrock on which my future research would be built. Additionally, I would like to thank T.J. Koger who helped me gather the materials that made up the initial syllabi in this class.

Numerous friends who, though not subject matter experts, engaged me repeatedly discussion of my topic and posed challenging questions that shaped my thinking. I would like to thank in particular: Wil Cook, Dave Molina, Chris Hearsey, Jeff Benvenuto, Matthew Holly, and James Woods.

My family has been absolutely supportive, even after they heard I was moving to New Jersey. I'd like to thanks my siblings and their spouses: Jeb & Carrie, Lucy & Brad, Serena & Wyn, and Patrick & Leye. My parents, Percy and Sandra Blount, have supportive throughout my over schooling and their encouragement has been critical in helping me complete this project. In particular, I'd like to thanks them for not only providing me with a computer well before they were household items (a Commodore 64 is the first computer I remember), but also succumbing to my requests and getting an

Internet connection in 1994. One might argue that I've been thinking about this dissertation ever since.

Finally, I'd like to thanks Kelly James, my love, my fiance, and my soon to be wife. She tolerated strange writing hours, conversations in which I was not wholly present, and the general malaise of the writer at work. She also read incoherent drafts and gave valuable feedback. Most importantly she distracted me and reminded me that the dissertation is part of the journey and not the goal.

Table of Contents

Abstract	iii
Acknowledgments	iv
Table of Contents	vi
Table of Figures	viii
Table of Acronyms	ix
Introduction	1
1. The Problem of New Spaces	2
Part I: Networked Geography	30
2. Cyberlandscapes	31
3. Legal Terrains	70
4. Political Places	109
Interlude	133
5. The Nomos of Cyberspace	134
Part II: Digital Encounters	162
6. Conflicting Territories	163
7. Standardizing Authority	197
8. Unbordered Rights	227
Conclusion	262
9. Reprogramming the World	263

Bibliography 286

Table of Figures

Fig. 2.1: Various Layered Models 38

Fig 3.1: Helen, GA 101

Fig. 5.1: The Dymaxion Map 137

Fig. 5.2: Map of Cyberspace 147

Fig. 5.3: QR Codes 154

Fig. 7.4: YouTube counter notification notice 220

Fig. 9.1: The Boilerplate Rhino 264

Fig. 9.2: Microcontroller Code 269

Table of Acronyms

AOL	America Online
CB	Citizen Band Radio
DBS	Direct Broadcasting Satellite
DMCA	Digital Millennium Copyright Act
DNS	Domain Name System
FTP	File Transfer Protocol
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICP	Internet Content Provider
IETF	Internet Engineering Task Force
IGC	Internet Governance Communities
IO	International Organization
IoT	Internet of Things
IRC	Internet Relay Chat
ISOC	Internet Society
ISP	Internet Service Provider
ITAR	International Traffic in Arms Regulations
ITU	International Telecommunication Union
NGO	Nongovernmental Organization
NSA	National Security Agency
NSF	National Science Foundation

MNC	Multinational Corporation
PCLOB	Privacy and Civil Liberties Oversight Board
PGP	Pretty Good Privacy
PP-14	ITU Plenipotentiary Conference 2014
PSP	President's Surveillance Program
R2P	Responsibility to Protect
TCP/IP	Transfer Control Protocol/Internet Protocol
TV	Television
UDHR	UNiversal Declaration of Human Rights
UDRP	Universal Dispute Resolution Policy
UK	United Kingdom
UN	United Nations
UNCOPUOS	UN Committee on the Peaceful Uses of Outer Space
UNGA	UN General Assembly
URI	Uniform Resource Identifier
URL	Uniform Resource Locater
US	United States
USML	United States Munitions List
W3C	World Wide Web Consortium
WWW	World Wide Web

Introduction

“Sir, line your borders with soldiers, arm them with bayonets to keep out all the dangerous books which may appear, and these books excuse the expression, will pass between their legs and fly over their heads and reach us.”

- Denis Diderot

Chapter 1

The Problem of New Spaces

I. Introduction

In June of 2013, Edward Snowden ignited a global debate about the nature of government surveillance in the electronic sphere. The government documents leaked by the former National Security Agency (NSA) contractor revealed mass electronic surveillance by the United States and a number of partner governments such as the United Kingdom.[1] These leaks raised serious legal, political, and ethical questions about the nature of individual privacy in the face of hidden government surveillance programs. The dominant narrative of the Snowden affair, as it unfolded in the media, was one of expanding government power impinging on individual rights in the electronic sphere. But there was also a counter narrative involved in this incident that exhibits a complimentary ebbing of the state's power to control information.

Perhaps one of the best illustrations of this counter narrative is the farcical vignette that takes place in the basement of the *The Guardian*'s building in London. In July of 2013, "a senior editor and a Guardian computer expert used angle grinders and other tools to pulverize the hard drives and

---

[1] Glenn Greenwald and James Ball, "The Top Secret Rules That Allow NSA to Use US Data without a Warrant," *The Guardian*, accessed May 6, 2014, http://www.theguardian.com/world/2013/jun/20/fisa-court-nsa-without-warrant; Nick Hopkins and Julian Borger, "Exclusive: NSA Pays £100m in Secret Funding for GCHQ," *The Guardian*, August 1, 2013, http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden ; and Philip Dorling, "Snowden Reveals Australia's Links to US Spy Web," *The Sydney Morning Herald*, July 8, 2013, http://www.smh.com.au/world/snowden-reveals-australias-links-to-us-spy-web-20130708-2plyg.html.

memory chips on which the encrypted" leaks from Snowden were stored.[2] These two men were overseen by note taking government officials who had ordered the destruction of the equipment.[3] This scene functions as a tableau that illustrates the core issue that Snowden exposed: the increasing dissonance Cyberspace causes in the application of state power. In *The Guardian's* basement, the state appears in physical form and asserts a right to control information based on physical realities. It uses legal and physical coercion to destroy a machine that contains information. In the pre digital era, this same tableau might be one of police destroying a printing press; the destruction of a printing press being an efficient means of containing information and destroying a message.

In 2013, the UK government remained insistent on this same method of control. It physically destroys the machinery of the newspaper, despite the fact "that other copies of the files existed outside the country and that *The Guardian* was neither the sole recipient nor steward of the files leaked by Snowden."[4] The effectiveness of the state's power to coerce is limited within a specific space and time, because the object of its control exists outside the space of the state. More specifically, not only was this information outside of the space of the UK, it existed outside the space of any state. The leaks themselves existed in a global space. In the past, the rationale for destroying the printing press was was linked to the press' locality and its central position

---

[2] Julian Borger, "NSA Files: Why the Guardian in London Destroyed Hard Drives of Leaked Files," *The Guardian*, Aug. 20, 2013, http://www.theguardian.com/world/2013/aug/20/nsa-snowden-files-drives-destroyed-london.
[3] *Id.*
[4] *Id.*

in the distribution network for its messages. Now, the message is no longer linked to the locality of the machine, and in McLuhan's word "the medium" has been transfused with "the message."[5] As a result, the state's ability to control information is bounded, and *The Guardian* "preferred to destroy [its] copy rather than hand it back to them or allow the courts to freeze [its] reporting."[6] While the individuals using the angle grinders are helpless in the face of the state, the state is helpless in the face of technology: reporting on the leaks continued. Interestingly, the very leaks being destroyed expose how states are attempting to shift this proposition and reassert power to control information.

New spaces create unique governance issues. This theme can be traced through the historical development of the international system of governance, which is highly tied to the conceptualization and division of space. From empires to Westphalian states to the modern state, the way in which global space is conceptualized, divided, and compartmentalized is a critical component in understanding the distribution of governance across the globe. This research takes up this thread and argues that Cyberspace creates an alternative geography that is facilitating a respatialization of the world. This respatialization, from an international space to a global space, is directly tied to the networkization of real space which creates new abutments and intersections of within Cyberspace.

Specifically, the argument herein is that Cyberspace recodes international borders in such a way that international governance has been

---

[5] Adam Brate, *Technomanifestos: Visions of the Information Revolutionaries*, (New York: Texere, 2002), 195-200.
[6] Borger, "NSA Files."

unable to effectively regulate Cyberspace. The traditional understandings are those that are centered on the state centric system that develops post-Westphalia and entrenches itself in the post-1945 settlement. It is state centered such that international space itself is defined by the sovereign equality of nations states. The international in this spatial order is an extension of the national and an expression sovereignty. This geographical shift in borders is understood not to be a matter of physical terrain. Instead, this study understands territory as "a political and legal concept, and not merely a geographical term."[7] Changes in geography require that both the practice and theory of international law and international relations be reevaluated in light of the opening up of a global digital information space that exists external to international space.

As is evident in the episode in the London basement from above, this project does not claim that the state, as the subject of the international, is devoid of power, and certainly not that the state is breathing its last gasps. The state still maintains the primary authority and legitimacy to compel the individuals located within its borders to comply with the regulatory mechanisms, and this power is reified through the system of international governance. Instead, the claim here is that geography of Cyberspace dramatically *changes* state power in ways that both strengthen and weaken the state. In a global geography the state becomes only one subject among many in global space. While this bifurcation of the international from the global may

---

[7] Hannah Arendt, *Eichmann in Jerusalem: A Report on the Banality of Evil* (New York: Penguin, 1963) at 262.

seem like an exercise in semantics, it represents deeper questions about the notion of governance system at a world scale. The international system is premised on the state as a primary actor, but the idea of the global acknowledges other actors and thus other participants in the construction of governance mechanisms. Globality in this sense is spatial geography that encompasses the state system, but is not defined in terms of the borders of that system. It is a geography that serves as an alternative to geography defined by the borders of states and the political-legal content of those borders.

II. Technology and the Global

It is no coincidence that "ages" of human time are often named after the dominant technology: stone age, iron age, bronze age, machine age, atomic age, space age. These references to technology carry the implication that the referenced technology was instrumental in shifting social relations and power structures in human society within the span of a temporal bracket. The contemporary Information Age is no different. The Information Age moniker suggests that world power structures are being shaped by information communication technologies (ICT). As such, it is a natural place for inquiry into how governance systems that operate on a worldwide scale are being shaped.

This brings us to the central problem being taken up by this research. International law has historically been capable of governing technologies that have transnational effects. The primary example being the law of the sea, which since the historic debate between *mare librum* and *mare clausum* in the

1600s, has been able to adapt to changes in technology that have increased the state's ability to extend claims over the sea abutting their borders.[8] This trend can be traced throughout the history of international law: the telegraph emerged in the 1830s and in 1865 the International Telegraph Union was formed to govern transnational telegraphy and it absorbed telephone and broadcast technologies in due course;[9] Little Boy was dropped on Hiroshima in 1944 and the Non-proliferation Treaty (NPT) entered into force in 1970;[10] Sputnik was launched in 1957 and the Outer Space Treaty entered into force in 1969;[11] and there are numerous other examples. Cyberspace seemingly bucks this trend.

The first Internet connection was established in 1968, and the network quickly grew after that with a successful public demonstration in 1972.[12] Today, it goes without saying that Cyberspace has become ubiquitous in everyday and that it facilitates new types of transnational exchanges. Unlike past transnational technologies, though, international law has been slow to react to Cyberspace. To date there has been one treaty that directly deals with

---

[8] Malcolm Shaw, *International Law*, 4th ed. (Cambridge: Cambridge University Press 1997) 390-392.

[9] George A. Codding Jr, "The International Telecommunications Union: 130 Years of Telecommunications Regulation," *Denver Journal International Law & Policy* 23 (1994): 502.

[10] *Treaty on the Non-Proliferation of Nuclear Weapons*, 729 UNTS 161 (entered into force March 5, 1970). The limited test ban treaty was adopted even earlier. *Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water*, (entered into force October 10, 1963).

[11] *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies* (entered into force October 10, 1967).

[12] Barry M. Leiner et al., "A Brief History of the Internet" (The Internet Society, October 15, 2012), http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet.

Cyberspace negotiated, the Budapest Convention on Cybercrime.[13] This Convention though was promulgated though the Council of Europe and has few state parties from outside of Europe. Additionally, its requirements are limited to creating regulatory harmony on Cybercrime, and it vests this power into the states themselves in the form of obligations for state parties to adopt legislation. Indeed, much of the problem behind negotiating a treaty is that states are skeptical about the trade offs meaning that topics such as cyberwar, cyber intelligence gathering, content restrictions,privacy and other human rights, and national security are likely to be excluded from any international agreement on Cyberspace.[14]

International law scholars have struggled with this exact issue, and the scholarship is marked by attempts to identify international norms that govern Cyberspace. Power and Tobin argue for "soft law" principles to govern the Internet in the face of the dearth of international law, and the soft law sources they identify are often external to international governance meaning that they have to argue for a new understanding of international legal processes.[15] Similarly, Zalnieriute argues for the existence of a customary international

---

[13] *Convention on Cybercrime* (entered into force July 1, 2004)

[14] Abraham Sofner, David Clark, and Whitfield Diffie, "Cyber Security and International Agreements," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, ed. Committee on Deterring Cyberattacks: Informing Strategies and Developing Options; National Research Council (Washington, DC: National Academies Press, 2010), http://www.nap.edu/catalog.php?record_id=12997 at 191. *See also* Charles J. Dunlap Jr., "Perspectives for Cyberstrategists on Cyberlaw for Cyberwar," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton: Taylor & Francis, 2013) 273 ("it is not likely that any new international treaty governing cyberwar or cyberweaponry will be forthcoming for the foreseeable future").

[15] Andrew Power and Oisín Tobin, "Soft Law for the Internet, Lessons from International Law," *SCRIPTed* 8, no. 1 (2011): 31–45, http://www2.law.ed.ac.uk/ahrc/script-ed/vol8-1/power.pdf at 39-44.

norm on data privacy, but she has to advocate for a "modernist" understanding of customary international law, a formulation likely to be found unacceptable by a majority of states.[16] A final example is Kulesza's volume titled *International Internet Law,* which argues that some international mechanisms can be extended into Cyberspace, but spends substantial time discussing other systems of regulation including an entire chapter on domestic law.[17]

The question of why international governance has been unable to extend its reach effectively to Cyberspace as a technology, despite its ability to regulate other transnational technologies, will be the primary line of inquiry driving this research. This broad question has several specific questions that must be answered in order to draw conclusions. The first of these questions is fundamental in international law: where is cyberspace? In the territorial oriented body of international governance, the location of an action and actors is the first question that must be answered when determining applicable law. Next, we must ask whether the location that is identified for Cyberspace fits into any of the categories understood by international law. If so, then baseline international norms can be established for Cyberspace. If it does not, then the next line of inquiry is to ask how this new category of space interacts with international space. Such interactions will reveal the specific sites at which international governance runs out and is unable to extend its reach.

---

[16] Monika Zalnieriute, "An International Constitutional Moment for Data Privacy in the Times of Mass-Surveillance," *International Journal of Law and Information Technology* 23, no. 2 (2015): 99–133.

[17] Joanna Kulesza, *International Internet Law*, trans. Magdalena Arent and Wojciech Wotoszyk (Routledge, 2013).

Similar questions have been addressed in the literature on globalization, which, though contested definitionally, is at its core an idea about the changing of the spatial terms of the world.[18] This research, though closely connected, does not intend to situate itself within this body of scholarship. Globalization is often conceived of as a "respatialization" that "has geographical scope, volume, and density of transactions."[19] Some theorists view globalization as a process, while others consider the term to indicate a theory, and still others use it to indicate a specific temporal era.[20] Others reject it as a "fad."[21] The literature on the whole though places into question the "constellation" of international space.[22] Reference to ICT is almost obligatory in these works as it is associated with shortening space and time and facilitating global flows, but globalization theory has "economic roots."[23] In this context, technology is not ignored, but it often is given a supporting role in the shaping of world scale,[24] thereby pushing technology to the edges of the inquiry.[25] For instance, Jayakar analyzes

---

[18] Frederick Cooper, "What Is the Concept of Globalization Good For? An African Historian's Perspective," *African Affairs* 100, no. 399 (2001): 196; Krishna Jayakar, "Globalization and the Legitimacy of International Telecommunications Standard-Setting Organizations," *Indiana Journal of Global Legal Studies* 5 (1998): 713; Michael Goodhart, "Human Rights and Global Democracy," *Ethics & International Affairs* 22, no. 4 (2008): 396-97.

[19] Yale H Ferguson and Richard W Mansbach, *Globalization: The Return of Borders to a Borderless World?* (New York: Routledge, 2012), 41-42

[20] *Id. See also* Jürgen Habermas, *The Postnational Constellation: Political Essays*, ed. and trans. Max Pensky (MIT Press, 2001) 65 and Michael Geyer and Charles Bright, "World History in a Global Age," *The American Historical Review* 100, no. 4 (1995): 1034–60.

[21] Cooper, "Concept of Globalization," 189-190.

[22] Habermas, *Postnational Constellation,* 60.

[23] Jayakar, "Globalization and the Legitimacy," 714; Cooper, "Concept of Globalization," 196; Saskia Sassen, Territory, Authority, Rights: From Medieval to Global Assemblages (Princeton University Press 2006) 168 and Mike Featherstone and Couze Venn, "Problematizing Global Knowledge and the New Encyclopaedia Project: An Introduction," *Theory, Culture & Society* 23, no. 2–3 (2006): 1.

[24] The concept of "world scale" is borrowed from Sassen. *Id.* at 14.

[25] *But see* J. Habib Sy, "Global Communications for a More Equitable World," in *Global Public Goods: International Cooperation in the 21st Century*, ed. Inge Kaul, Isabelle Grunberg, and

globalization in terms of commercial interests in ICT standard setting bodies, but never addresses how the technology itself is shaping the space in which those decisions unfold.[26] Thus despite the globalization literature's preoccupation with flows and interconnections of all types, there is little scholarship that embarks to understanding how technology itself serves as an endogenous factor that shapes the space in which flows and interconnections unfold.[27] The scholarship most often presents technology as an external factor at best understood in terms of disciplinary accepted points of inquiry such as conflict or the global political economy. While globalization implies "expanding integration, and integration on a planetary scale," global space itself has been ill defined.[28] Indeed, one of the deep problems with the definition of global space is that it is often presented as a counterfactual to international space, and not as an independent spatial structure existing autonomously from international space.[29]

Marc Stern (New York, Oxford: Oxford University Press, 1999) at 333 ("Global telecommunications underpin globalization.")

[26] Jayakar, "Globalization and the Legitimacy," 711–38.

[27] Stefan Fritsch, "Technology and Global Affairs," *International Studies Perspectives* 12, no. 1 (2011): 28 (arguing that "standard explanations of systemic changes in global affairs usually focus on political or economic variables, neglecting technology's core role as a driving force behind systemic transformation as well as its reciprocal relations with politics, economics, and culture."). This strain does exist within information theory. Adam Brate, *Technomanifestos,* 195-200.

[28] Cooper, "Concept of Globalization," 196. Cooper notes that "[a]ttempts to posit a transition from multiple worlds to a single world system with a core and a periphery have been mechanistic and inadequate to understand the uneveness and the dynamics of such a spatial system." *Id.* at 200-01.

[29] For example, statements like "[i]f the nation state system is in decline" resonate with counterfactual inquiry. Jayakar, "Globalization and the Legitimacy," 737. Another example is Ferguson and Mansbach's perceptive subtitle to *Globalization*, "The Return of Borders to a Borderless World," which indicates that within globalization scholarship global space is fragmented by rises state power. Ferguson and Mansbach, *Globalization*. *See also*, David J Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power* (London: Routledge, 2011) 55-56.

To some extent this is natural. International governance scholarship has often addressed technology as an externality because it was controlled by the state and therefore a function of blood and treasure. The state was the arbiter of technology both through law and policy, and as a result, systems of governance that were established to stabilize states were well suited to establishing frameworks for governing those technologies at the world scale. This is why the International Telegraph Union (ITU) was established in 1865 and continues to govern international telecommunications.[30] When the state is addressed as the sole arbiter of power, it means that *international* understandings are applied, which place the state at the center of the inquiry. Such a perspective is functional when the state controls technologies of power. For instance, during the Cold War nuclear weapons were controlled by states, and nuclear politics and power unfolded within the context of the state. Cyberspace is different. The state does not control this technology absolutely, despite the fact that state power often unfolds within the space of Cyberspace. This indicates that Cyberspace has different scope and meaning than previous transnational technologies that function at a global scale, such as nuclear and space technologies. This leaves theory somewhat in the lurch, as a transnational phenomenon seemingly without international control maintains and propagates itself throughout society worldwide.

Instead of a state oriented perspective, this research investigates Cyberspace as an "endogenous and political factor deeply embedded in the

---

[30] *See generally* George A. Codding Jr, "The International Telecommunications Union: 130 Years of Telecommunications Regulation," *Denver Journal International Law & Policy* 23 (1994): 501.

global system."[31] Where earlier technologies existed as the subject of state power, state power is addressed here as a subject of Cyberspace. This distinction is important, because it indicates that Cyberspace shapes the space in which governance at all scales unfolds. That is not to say that the state does not shape the space in which Cyberspace unfolds, quite the contrary, states still hold significant power over parts of Cyberspace and social life in general.[32] This is the problem with addressing global space as a counterfactual to the international: it presupposes a zero sum relationship best understood in terms of either/or. Cyberspace, instead, presents a global space best understood as a co-factual to the national and international. It is a new space that is emerging in addition to international space, and its emergence is central to contemporary structuring of world scale governance. It is not necessarily a space that is always in a contestation with the national as states maintain interests in Cyberspace and often pursue their interests through Cyberspace. This dynamic interaction at the border of the state and cyberspace is the focal point of this research, because it is in this dynamic that reprogramming of international space into global space can be observed.

This research asserts that the key to understanding the unfolding of law and politics at the world scale is through an understanding of how Cyberspace shapes social experience of world space through a key value of interoperability. Interoperability, it will be shown, is the core organizing logic for Cyberspace and it has strong sway over the social construction of Cyberspace as a global

---

[31] Fritsch, "Technology and Global Affairs," 28.
[32] Jack Donnelly, "Human Rights: A New Standard of Civilization?," *International Affairs* 74, no. 1 (1998): 16 ("One need not be a realist to allow power and perceived self-interest will continue to dominate foreign policy in the coming decades.")

space. This value puts a primary focus on facilitating cross-platform, cross-network communications. While highly relevant to and not in opposition to globalization, this study does not seek to root itself squarely within the globalization debate.[33] Instead, it seeks to present that the "chang[ed] meaning over time of spatial linkages can be understood in a better way than globalization."[34] Instead of focusing directly on the transnational flows invoked by the concept of globalization, this study focuses on the technological landscape in which these flows unfold. Its focus is the medium of these flows and how that medium structures and facilitates transnational and global information exchange. This cyber-landscape - addressed in terms of spatial, legal, and political geography - creates global space that pushes against international borders in opposition to the concept of the international. This research asserts that Cyberspace imposes an alternate geography that results in redistribution of governance capabilities from international space to global space. It will trace this redistribution through examination of interactions often used as focal points in international studies as a way to illustrate how key assumptions based on the territory of the state are being reconstituted within a new geography.

III. Methodology and Scope

As a qualitative study, the core goal of this study is to articulate a coherent understanding of whether, how, and why Cyberspace changes

---

[33] Cooper notes that the "imagery of globalization derives from the World Wide Web," but notes that there is a long history of "long-distance connections." Cooper, "Concept of Globalization," 196, 200-01.
[34] *Id.* at 195.

international space. To do this, it will first construct a geography of Cyberspace, and then it will examine how that geography interacts with international space. Rather than arguing for a new world order, this study adopts the international governance as a given fact in world scale governance. As a result, the methodology will have two steps: an articulation of a geography of Cyberspace and the layering that geography onto international geography in order observe how the space has changed shape.

The first task will be to articulate a holistic geography of Cyberspace in both practical and theoretical terms. Using geography as a heuristic for understanding cyberspace necessitates an interdisciplinary approach, since scholarship on Cyberspace is dispersed across a number of disciplines. A primary focus will be on works that directly address legal and political theory, but themes from sociology, history, and computer science will be evident in the description of the complex interconnections between technical and social processes. This interdisciplinary approach will be used to conceptualize a geography of Cyberspace by describing its borders and boundaries through its spatial, legal, and political characteristics.

This alternate geography will then be used to facilitate observation of points at which Cybergeography interacts with international geography. These two geographies will be conceptually stacked in order observe points of interaction and analyze content of those interactions in terms of spheres of governance. This analysis will be executed using terms of international governance, which is understood to contain both international law and international relations. Despite the disciplinary divide, between international

law and politics, they are in practice are clearly entangled, thus here they are presented as integrated parts of the international governance system. For ease of application the international will be understood to consist of the system in which the traditional Westphalian state is the primary subject and object of governance.

Once a geography of Cyberspace is developed, this theoretical understanding will then be used to investigate thematically grouped case studies that exhibit specific interactions of Cyberspace with international space. To accomplish this conceptual layering of geographies, a hermeneutic approach that seeks to construct meaning through analysis of media narratives and primary legal and political documents will be used. The methodology will be somewhat similar to Reisman's international incident approach. This approach argues that the epistemic unit in international law is the international incident, which is marked by a conflict among states that leads to clarifications in the content and meaning of international law through the negotiated resolution of incidents.[35] Similarly, the case studies in this paper will investigate transnational incidents that would traditionally fall within the realm of the international and examine how Cyberspace changes the content and meaning of those incidents. The cases chosen are grouped thematically, and these themes have been selected for their salience in revealing the shifting nature of the international. Specifically, the themes are built around the territorial, legal, and political geography of international space in order to

[35] *See generally* W. Michael Reisman, "International Incidents: Introduction to a New Genre in the Study of International Law," *Yale J. Int'l L.* 10 (1984): 1. The author has adapted this approach before, *see* P. J. Blount, "Renovating Space: The Future of International Space Law," *Denv. J. Int'l L. & Pol'y 40 (2012): 515–686.*

match the geography adopted in the first part of the research. This will allow the identification and analysis of encounters where cyber and international geographies come into proximity. As a result these themes reach directly to critical issues addressed by the international system: the nature and limitation of interstate conflict; the state's central position in the making of international governance; and the nature and limits of individual rights. The selected cases or incidents themselves are archetypical of types often examined in international studies, but the specific incidents should not be taken as archetypical of the interactions they represent. Instead, they are intended to show trends, as more research would be required to chart these trends across a diverse range of interactions.

The examples used in this research were chosen to reveal a common narrative of governance redistribution. While individual cases may have alternative readings in light of traditional international relations or international law theory, it is submitted that if these theories are maintained across the narrative as a whole, then they become dissonant. Nor is this research an attempt to disprove more traditional theories. The purpose is to illustrate the multidimensional nature of global space, and show the limits of such theories in light of the complex nature of networked world of Cyberspace. Just as this research argues that Cyberspace is separate from international space, so too do traditional theories run separately from the alternative geography presented herein.

This study will limit its scope to understanding how spatial redistribution occurs and how this changes power structures at the world scale.

It will not seek to normalize or naturalize these processes. Though the conclusion will argue that cyber-technologies can act as a facilitator of developing governance at the global levels, it does not embrace technological determinism. Indeed, it is well documented that technology is dual use and can be turned from liberation to oppression with ease.[36] Technology itself has no ethical content until it is transfused with the politics of human interaction. It is this political content that will be investigated in this research and not necessarily the virtue or vice of that content.

IV. Definitions and Usage

In order to avoid confusion, the usage of a number of terms should be clarified at the outset. First, there are a number of spatial terms that are adopted in this research and the author has attempted to be consistent in their usage throughout. 'Space' is used to designate an area or region in both a physical sense (i.e. the space of a room) and a metaphorical sense (i.e. a safe space for discussion). Implicit in the idea of space though is that it has contours, boundaries, and borders that demarcate the extent and nature of that space. This means that the term 'space' is often used with qualifiers that designate the limits of a space: physical space, digital space, legal space, political space. Of note are two spaces that have world scale that are central to the analysis: 'international space' and 'global space.' World scale indicates that these are spaces that cover most, if not all, of the surface of the Earth.

---

[36] For example, Evgeny Morozov, "Political Repression 2.0," *The New York Times*, September 1, 2011, sec. Opinion, http://www.nytimes.com/2011/09/02/opinion/political-repression-2-0.html.

'International space' designates a world scale space that is demarcated by borders that construct sovereign territorial states. International space is constituted by the national borders deployed by international governance mechanisms. It should be noted that in this conception, though highly entangled 'national space' constitutes a separate category from 'international space.' It should be noted that in this analysis 'international space' is considered to be a construct of 'international governance," and the condition of 'international governance' and 'international space' is often referred to in short hand as 'the international.' Global space," on the other hand, designates a space of world scale that is not marked by national borders. This type of space exists independent of the state system. It should be noted that while, for the purposes of simplifying this analysis, these two world scale spaces are juxtaposed, they are not always easily separable. Central to this argument is that these spaces overlap and intersect, and as a result global space, and specifically in this research, Cyberspace is often marked by the borders of international space and vice versa. It is this interaction that is at issue, and juxtaposition serves as a useful tool for examining the interaction between the two spaces.

The idea that spaces have boundaries that demarcate them means that spaces, both physical and metaphorical, can be said to have 'geography.' 'Geography' is used herein as heuristic to describe the particular structure of a space. In real space, this means a description of the physical attributes of that space. In metaphorical spaces, this means a description of the various limitations that mark the contours of that space. For instance, below 'legal

geography' is deployed as a way of understanding jurisdiction, which demarcates the limits of the law's application. The term 'alternative geography' is used as a way to designate the new understanding of geography that Cyberspace creates by juxtaposing it to the accepted geography of the international.

In addition to the spatial terminology, there are a variety of governance terms that are used that should be clarified. The core concern with this research is that of governance at the world scale, and 'governance' is used to designate the network of mechanisms that distribute rights, obligations, and limitations within a society, whether legal, political, economic, or of another nature. In this research, 'law' is most often used to designate formal legal systems exercised by organized government; however, law is occasionally used to designate less formal systems that have high regulatory ability, such at in the 'code is law' principle found in Chapter 3. 'Regulation' on the other hand is used in a very broad sense to designate a variety of mechanisms that serve to exert control over actors in a given system. Regulatory processes, in this sense, do not need to flow from formal processes of law, and may come from informal or non-binding processes external to government action. 'Politics' is part of 'governance,' since politics helps to define the content of law and regulation giving further contour to the space that regulatory mechanism inhabit.

V. Structure of the Argument

A. Part I: A Networked Geography

Part I (chapters 2-4) will establish a heuristic geography of Cyberspace. This geography will be approached from three different perspectives: spatial, legal, and political. The goal of this exercise is to describe a complete geography of Cyberspace as a location with a distinct set of rules and a distinct set of political arrangements. While the model presented will paint Cyberspace as a distinct space from national or international space, it will not go so far as to argue that Cyberspace exists entirely outside the space of the state. Instead, the geography of cyberspace is one that often intersects the space of the national.

- *Chapter 2: Cyberlandscapes*

Chapter 2 will investigate what Cyberspace is from both technical and sociological perspectives. Its objective is to establish Cyberspace geography in spatial terms. To accomplish this task, this chapter will first describe the technical architecture of Cyberspace using a layered conceptual model, which will help give shape to Cyberspace through a description of its physical and logical components. It will then investigate how the social construction of Cyberspace gives it spatial meaning through a spatial narrative. The spatial narrative is the sociological phenomenon in which Cyberspace is conceptualized as a place. The language that is used to describe the digital space is such that it imbues the digital with characteristics of physical space. When read together these aspects of Cyberspace create an articulable geography of a global network that is different in scope and location from world scale space understood through international geographies.

- *Chapter 3: Legal Terrains*

This chapter will describe the variety of regulatory mechanisms that are active in Cyberspace and how these function together as a legal geography, i.e. jurisdiction. The goal of this chapter is to establish the ways in which regulatory power is exerted in Cyberspace, and the limits of such power. First, it will seek to explain the concept of jurisdiction as a legal geography, which will lay the groundwork for understanding how regulation is deployed in Cyberspace. Then, it will use the 'code is law' principle to analyze how regulatory power is exerted across the layered model used in Chapter 2.[37] Finally, this chapter will argue that the architecture or code of Cyberspace shows a preference for governance mechanisms that exist outside the jurisdictional bounds of the state. This represents a significant shift in power as it means that the code of cyberspace changes the legal geography of state jurisdiction by recoding regulation.

- *Chapter 4: Political Borders*

Chapter 4 argues that if computer code establishes both the spatial geography (through the layered conceptual model) and the legal geography of Cyberspace (through the 'code is law' principle) then this code, to some extent, fulfills a constitutional function of setting the bounds of the political space in which society unfolds. This claim is not premised on the idea of a constitution in its formal sense, but instead on the notion that constitutional documents

[37] For "code is law" see Lawrence Lessig, *Code 2.0* (Basic Books, 2006), 5. For layers see Kevin Werbach, "Breaking the Ice: Rethinking Telecommunications Law for the Digital Age," *J. on Telecomm. & High Tech. L.* 4 (2005): 59 and David G. Post, *In Search of Jefferson's Moose: Notes on the State of Cyberspace* (Oxford; New York: Oxford University Press, 2012), 80-89.

and code both achieve similar ends, albeit by different means, in the structuring of the political space in which individuals interact. This technologically defined constitution, similar to a legal constitution, allocates "the distribution of power [among] the rulers and ruled."[38] Chapter 4 will then demonstrate that founders of Cyberspace structured the network in such a way as to enable open political interaction among individuals. The chapter will briefly address the political philosophies embedded into the technical design through a discussion of the historical roots of the Internet and the political philosophies of the individuals that designed its underlying code. Finally, this chapter will argue that the core value of interoperability is foundational to the political geography of Cyberspace. Interoperability as a value will be used to demonstrate how Cyberspace mediates transaction points among actors, thus setting the parameters for its political sphere.

B. Interlude - Chapter 5: The Nomos of Cyberspace

Chapter 5 uses the geography established in Part I and juxtaposes it to the geography of international space. This juxtaposition is a critical point of analysis as it reveals the gaps and ambiguities in the international caused by Cyberspace. It differentiates the geography of Cyberspace from the core territorial assumptions of international space indicated by the compression of spatial, legal, and political geographies into sovereign states by international

---

[38] Jean-Marc Coicaud, *Legitimacy and Politics A Contribution to the Study of Political Right and Political Responsibility*, trans. David Ames Curtis (Cambridge: Cambridge University Press, 2002), 52. The preposition in this quote has been changed from "between" to "among" to denote that in Cyberspace this is not a binary or two way process, but a multi-dimenisonal process.

order. The chapter first explores and critiques the construction of borders in international space, and argues that these borders constitute discrete geographic compartments that contain territorial, legal, and political space. Then, the chapter demonstrates how Cyberspace recodes the content of those borders. Specifically, it argues that networked space allows actors within the sphere of Cyberspace to reimagine the content of the national border. Finally, it asserts that an examination the components of the governance assemblage of territory, authority, and rights - identified by Sassen - serves as a useful tool for revealing the intersection of the Cyberspace and the international. These components reveal points at which meaningful interaction between the international and Cyberspace may be observed in order to determine the extent to which Cyberspace recodes borders. These categories will be deployed in Part II to facilitates the conceptual overlay of geography.

C. Part II: Hyperlinking Geography

Part II (Chapters 6-8) will overlay the geography of Cyberspace articulated in Part I onto thematically grouped cases. These cases are selected to reveal meaningful points of interavtion between Cyberspace and the international to show reconfigurations of internationally conceptualized spatial, legal, and political geography. The three chapters in this section deploy the categories of territory, authority, and rights introduced in Chapter 5 as the means through which to critique the geographic categories developed in Part I. Focusing on primary documentation and secondary documentation, these case

studies will focus on using transnational incidents as epistemic moments that reveal fault lines in the international.

- *Chapter 6: Bracketing Cyberwar*

Chapter 6 reflects on the concepts of cyberwar and cyber-conflict and their effects on the territorial bracketing of war found in international governance. This chapter's inquiry rest on the delineation of of territory in the international system as one of the central mechanisms for pursuing a primary goal of limiting the occurrence of international armed conflict. It will argue that cyber-conflict redistributes territory away from the state by redefining the scope of transnational violence. This chapter will use the concept of cyber-conflict to illustrate how Cyberspace changes the spatial dimensions of international geography by reducing the role of territory in containing conflict. This chapter will use Stuxnet, deterrence, and the North Korea-Sony hack to illustrate the changed conditions of territorial space as understood from the international perspective. This chapter's core assertion is that the digitization of violence substantially erodes the concept of "territorial integrity" of the state, which results in a corresponding shift in international space. The cases used in this chapter will illustrate how cyberspace reallocates power over territory.

- *Chapter 7: Standardizing Authority*

This chapter will analyze the category of 'global multistakeholder governance' and argue that a unique set of non-state actors now maintain the authority to directly regulate the architecture of Cyberspace. This authority

allows these actors to assert regulatory authority to which states are subject without consent. Using cases such as the ITU's interaction with Cyberspace governance, the rise of IGCs and multistakeholder governance, and corporate regulation of Cyberspace, this chapter will seek to elucidate how authority to manage transnational interactions has shifted out of the international arena. This analysis will use a comparison to the traditional model of International Telecommunication Union (ITU) governance of telecommunications to cybergovernance structures in order to show how the authority the legal geography of authority is changing.

- *Chapter 8: Unbordered Rights*

The final chapter of cases will use the category of rights to observe how international political geography is shifting. This chapter will focus on cases that show how individual rights are being increasingly mediated outside of international processes. The studies include an evaluation of encryption technologies, the use of mass surveillance technologies by states, and the phenomenon of hacktivism in order to demonstrate the reshaping of political space. This chapter adopts the category of rights as a lens through which to understand the scope of political space in which an individual exists. Once applied, this chapter will show that individual rights are increasingly mediated outside of international governance. Importantly, this chapter argues that the changes in the international space can not simply be simply understood as a retraction of state power. Instead, this chapter argues that Cyberspace creates a two way street in which state power increases in spite of international

governance and its reliance on borders. The construction of political space as a result becomes increasingly more complex as the individual must negotiate various sources of rights that often flow from outside traditional political borders.

.

D. Conclusion - Chapter 9: Reprogramming World

The final chapter will conclude by examining the implications of Cyberspace for international space. The chapter will inverse the 'code is law' principle and argue that 'law is code." This metaphor will be used to explain why Cyberspace has been able to reconfigure international space. The chapter will argue that the 'program' of international governance is short circuited by digital technologies that meld the message to the medium. It argues that computer programming deploys a world of ideas that the international is not equipped to regulate, and that this world of ideas transforms the international by reprogramming its processes and procedures. This analysis will be coupled with consideration of what a reprogrammed world means in terms of international theory with an emphasis on Realism and Cosmopolitanism. It will also offer a discussion of questions that define paths future research into the alternate geography of Cyberspace and its future shaping of international space.

V. Trajectory

This research situates itself in scholarship seeking to explain how technology changes law and politics that affect global order. Cyberspace is a

phenomenon happening at a world scale and as such it's relevance is not simply an externality affecting the power distribution in the international. Instead, what this research argues for is that Cyberspace should be understood as embedded in the processes that shape global order through the mediation of human interaction. The alternate geography of Cyberspace is a new space in which international governance unfolds, and it is critical to have a model for understanding the transformative effects of Cyberspace. This research pursues this model using the heuristic of alternative geography, which effectuates a redistribution of territory, authority, and rights among global legal and political actors. It is hoped that this model sheds light both on how technology mediates global processes and reprograms governance.

While the final chapter will concern itself with identifying specific questions raised by this research, it is submitted here that the new conceptualization of global space offered herein is becoming fundamental to understanding the unfolding of transnational and global events. As Cyberspace continues to grow, it is noteworthy that world news outlets increasingly report on events that occur either entirely or partially within Cyberspace. Additionally, Cyberspace has become a key issue in international relations, and its pervasiveness seems to be fully entrenched. As a result, the research includes important insights that can be applied in untangling the meaning of future transnational incidents by conceptually delimiting the geographies in which these incidents occur. The International is not dying, but it is folly to argue that it is not changing. International space can no longer be understood as a static compression of territory, law, and politics. Instead, it must be

understood as a space marked by geographic shifts recoded borders, which raises serious questions for the theory and practice of international governance. This research can be seen as a starting point for understanding the origins of these questions, and it offers a framework for evaluation of future developments.

Part I
Networked Geography

"The objective space of a house - its corners, corridors, cellar, rooms - is far less important than what poetically it is endowed with, which is usually a quality with an imaginative or figurative value we can name and feel: thus a house may be haunted, or homelike, or prison like or magical. So space acquires emotion and even rational sense by a kind of poetic process, whereby the vacant or anonymous reaches of distance are converted into meaning for us here."

-Edward Said

Chapter 2

Cyberlandscapes

"What difference does that make, what channel you got?" complains Ed Lindsey while he flips the stations on a television (TV) in a boarding house common room. Lindsey, a character in a 1961 episode of *The Twilight Zone*, is frustrated with the rapt attention that his housemates pay to the television. Soon after this exchange, Lindsey retrieves his 1935 console radio from the basement, and he finds that it receives, literally, broadcasts from the past. The radio's mystical power eventually transports Lindsey into the past for which he longs.[39]

The episode, named "Static," avoids the usual, cliched plot of the fear of advancing technology coupled with eroding humanity, so often found in science fiction.[40] It makes a more subtle point about technology that is implicit but often overlooked in these narratives, namely that technology shapes the social experience of time and space. Though a permutation of the same broadcast technology, the TV world has different spatial and temporal reference points than does the world of radio. This can be seen in Lindsey's characterization of a musical performance on TV as "ruining a perfectly good song." The values imposed by the TV (i.e. video) are different from the values imposed by radio (i.e. audio). This is more than just an issue of production quality, it changes the interactions of the individuals within those spaces.

---

[39] "Static," *The Twilight Zone*, season 2, episode 20 (1961)
[40] *See, for example,* "A Thing About Machines," *The Twilight Zone*, season 1, episode 40 (1960)

Television's visual values prompts Lindsey to refers to his housemates as "hypnotized" as they watch. This is different from the space of radio, which created an interactive social space around its speakers, so when Lindsey reconstructs his space to the 1940s, the radio is not the focal point in the room, instead the focal point is his love interest.

At the surface, this fictional tale is wrapped in a narrative of social fragmentation caused by mass media, but beneath this narrative lies a deeper theme that sits at the heart of inquiries into modernity: the effects of technology on the construction of social space. What Ed Lindsey observes is that, though analogous, these technologies each change how the world around him is ordered in unique ways. They literally shape the space the space of the boarding house.

Cyberspace, as a technology, is no different. It shapes space, and it does this because the technology creates unique spatial orientations. The goal of this chapter is to describe the spatial geography of Cyberspace in terms of its technical manifestations, and in terms of the dominant conceptual narrative through which Cyberspace is understood. This description will resist adopting a definition of "Cyberspace" in absolute terms. Part of this impetus comes from the diverse definitions that already exist in the literature describing Cyberspace, but never in complete terms.[41] As a result, the chapters in Part I

---

[41] *For example*: David C. Gompert and Phillip C Saunders, *Paradox of Power: Sino-American Strategic Restraint in an Age of Vulnerability* (Washington, DC: National Defense University Press, 2012) ("Cyberspace [is] shorthand for the capabilities and content of computer networking."); Lessig, *Code*, 9; ("But 'cyberspace' is something more. Though built on top of the Internet, cyberspace is a richer experience."); Chris Toulouse, "Introduction," in *The Politics of Cyberspace*, ed. Chris Toulouse and Timothy W. Luke (New York: Routledge, 1998) 5 (". . . a new transnational realm of civil society . . ."); Timothy W. Luke, "The Politics of Digital

will focus on describing Cyberspace to facilitate a richer understanding of its contours.[42] This approach flows from a central hypothesis that Cyberspace is a geography in which social which social relations unfold. here. description is prioritized over definition due to the difficulty in defining a dynamic space both accurately and coherently. Definition is a tool to simplify concepts. Description, on the other hand, reveals nuance and complexity critical to a rich understanding, as sought herein.[43]

This chapter will first use a layered model to describe the technical architecture and of the Internet, which is distinct from Cyberspace. Once this technical space has been articulated, the spatial conceptualization of Cyberspace will be explored. Section of this chapter argues that the dominant human understanding of Cyberspace is through a spatial narrative, and that this narrative has powerful implications for the social conceptualization of Cyberspace. Finally, the chapter will conclude by examining how the technical architecture creates space through examination of the inhabitants of Cyberspace and the implications of networked populations. The spatial geography of Cyberspace is critical to understanding the larger thesis that Cyberspace recodes borders and reprograms the world.

I. Networked Space

Inequality: Access, Capability and Distribution in Cyberspace," in *The Politics of Cyberspace*, ed. Chris Toulouse and Timothy W. Luke (New York: Routledge, 1998) at 121 ("Cyberspace might best be understood as the latest manifestation of nature's pluralization."); and Betz and Stevens, *Cyberspace and the State,* 13 ("Cyberspace is notoriously difficult to pin down.").

[42] This approach is not novel and was employed by Post. Post, *Jefferson's Moose*.

[43] This is akin to the difference of a definition of a particular nations state, say China, which w, and a book on its history and government.

Ed Lindsey's question of "what does the channel matter" can be answered easily: a lot. The technology of TV is such that choosing a channel means choosing a network, and choosing a network means accepting the content chosen by the network. Changing the channel changes everything, and it was the only way to change the output of the TV. The networks accessible on a given TV is limited by the location since broadcast TV is a function of proximity to the transmitter, and that accessibility was limited to reception from, but not interaction with the broadcaster. The space that TV creates is one of viewers relegated to peering in.

If "Static" were updated for contemporary airing, one could imagine the boarding house crowd all gathered in the common room, but the focal point would be their own personal electronic devices. Ed Lindsey, instead, would yell because they were not taking part in the social act of watching the TV in the common area and building community through the shared experience of viewing. While Lindsey's technological skepticism would be built on substantially the same rhetorical claims, the space in which he would be making his claims would be very different. In this updated version, each individual would be focused on being in Cyberspace and, importantly, interacting with others in Cyberspace. Each individual will have chosen their own channel. Some of these channels, such as services like Pandora or Netflix, mimic previous information technologies. Other channels though create vastly different opportunities for engagement and interaction. Indeed, many individuals in this alternate take would be interacting with *more* individuals as a result of this technology. This simple shift changes the constitution of the

common room space, because "the Internet is not like TV - you use it, it doesn't use you."[44]

Technology, in particular information technologies, change human interactions.[45] This is because these technologies are capable of providing more and richer information and information sits at the core of social interactions. Space is understood as constructed by humans, and humans experience spaces differently depending on the way technology deployed within them changes interactions. Ed Lindsey experiences the common room of the boarding house differently when different technology is deployed. This is similar to trends noted by Cohen, in which surveillance technologies alter public space. Surveillance technologies, beyond simple observation, achieve "the active production of categories, narratives, and norms."[46] Cohen argues that these technologies change space by "constrain[ing] the range of available behaviors and norms."[47] Surveillance technology is emblematic of how the "prolifera[tion]" of "transaction points" changes the experience of physical geography.[48]

Before abandoning a happy Ed Lindsey in the 1940s, we should take a closer look at the nature of the technology that is defining the space in which he

---

[44] Toulouse, "Introduction," 12.
[45] This can be traced throughout history. For instance, this explains the attention given to the Mongolian Empire's *yam* system. Jane Burbank and Frederick Cooper, *Empires in World History: Power and Politics of Difference* (Princeton: Princeton University Press, 2010) 109-110; early telegraph, Armand Mattelart, *Networking the World, 1794-2000* (University of Minnesota Press, 2000) 1-13; and broadcast, Douglas Kellner, "Intellectuals, the New Public Sphere, and Technopolitics," in *The Politics of Cyberspace*, ed. Chris Toulouse and Timothy W. Luke (New York: Routledge, 1998), 175-79.
[46] Julie E. Cohen, "Privacy, Visibility, Transparency, and Exposure," *The University of Chicago Law Review*, 2008, 181.
[47] *Id.* at 190.
[48] *Id.* at 200.

lives, or more precisely defining his transaction points. Mass communication in this world is the product of centralized, one-way communication. In this model, power is located at a central position, and is understood as the power to transmit. The entity that controls the transmitter also controls the content that the viewer or listener sees. The end device only receives; none of the knobs or buttons allow the user to send a message back to the transmitter. Mass media in this space is about transmission *to* the masses that receive it.[49] It is a one way street, and the space at the receiving end of that street is shaped by this technology. The Internet dismantles this one way paradigm and presents the user with an array of opportunities to engage in multi-way communication with other individuals, with the masses, and with nearly any other type of entity capable of communication. This fundamental difference creates dramatic changes for the nature of human interaction and social order, because transaction points become myriad and are distributed worldwide.

The Internet is distinct from Cyberspace. The Internet, for present purposes, can be understood as the technology that makes Cyberspace possible.[50] The technology of the Internet facilitates and is inseparably entangled with the phenomenon we know as Cyberspace, which inhabits broader social dimensions. This means that in order to describe Cyberspace, on must first describe the Internet which structures Cyberspace. In order to

---

[49] On the transmission view of communication see James Carey, "A Cultural Approach to Communication," in *McQuail's Reader in Mass Communication Theory*, ed. Denis McQuail, 2002, 36–45.

[50] Lessig, *Code*, 9. Lessig notes that there is "no sharp line that divides Cyberspace from the Internet. But there is an important difference in experience between the two." *Id. See also* Joanna Kulesza, *International Internet Law*, trans. Magdalena Arent and Wojciech Wotoszyk (Routledge, 2013) at 31.

understand the technical architecture of Internet a layered model is adopted here. This model "was developed by computer scientists to explain the functional components of the Internet and how they work together to convey Internet traffic."[51] A number of legal scholars have adopted the layered approach to explain policy and regulation on the Internet.[52] While these regulatory aspects will be explored later, at present the layered model presents a useful model for breaking down the component systems that work in concert to make the Internet possible. The layers approach is a "conceptual tool" that "divides a networked information system into a hierarchical 'stack,'"[53] presenting the Internet as a combination of different technologies with different functions stacked together to form the whole. This approach is useful, because the "interconnectivity among networks" is "so complex that it is not easily understood."[54] Layering creates a model for categorizing diverse, yet interrelated, technologies by function and reveals how each "self-contained" category is linked to the layers above and below it.[55]

Different authors have used different stacks of layers. So for instance, Post simplifies the Internet into two distinct layers, the network layer and the

---

[51] Ellen P. Goodman and Anne H. Chen, "Modeling Policy for New Public Service Media Networks," *Harv. JL & Tech.* 24 (2010): 115

[52] For *instance*, Goodman and Chen argue that the layered model should be used to "shape public media reform." Goodman & Chen, "Public Service Media 116; Werbach argues that the layered model can be used to update media policy from an analog two-layer model. Werbach, "Breaking the Ice," 78-80; Solum and Chung situate the layers model as central to understanding regulatory effects. Lawrence B. Solum and Minn Chung, "The Layers Principle: Internet Architecture and the Law," *Notre Dame L. Rev.* 79 (2003): 821.

[53] Werbach, "Breaking the Ice," 71, 66.

[54] Gompert and Saunders, *Paradox of Power* 116. The Internet can be described as an "unprecedented integration of capabilities," which indicates both its scope and complexity. Barry M. Leiner et al., "A Brief History of the Internet" (The Internet Society, October 15, 2012), http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet.

[55] Werbach, "Breaking the Ice," 66.

applications layer,[56] Kulesza uses three layers,[57] whereas Solum and Chung use a six layer stack (See Fig. 1.1).[58] The differences in the models are not substantive in nature and are, instead, based on the resolution of the analysis.[59] A medium grain four layer stack will be used here to avoid both oversimplification and unneeded complexity. Werbach and others have identified a four layered stack, which contains a physical layer, a logical layer, an applications layer, and a content layer.[60] This four layer stack will guide the analysis here.[61]

<table>
<tr><td rowspan="2">Network Layer</td><td rowspan="2">Physical Layer</td><td rowspan="2">Physical Layer</td><td>Physical Layer</td></tr>
<tr><td>Link Layer</td></tr>
<tr><td rowspan="2">Logical Layer</td><td rowspan="2">Logical Layer</td><td>IP Layer</td></tr>
<tr><td rowspan="3">Applications Layer</td><td rowspan="3">Transport Layer</td></tr>
<tr><td rowspan="2">Content Layer</td><td>Applications Layer</td><td>Applications Layer</td></tr>
<tr><td>Content Layer</td><td>Content Layer</td></tr>
</table>

[56] Post, *Jefferson's Moose,* 80-83.
[57] Kulesza, *International Internet Law*, 125-126.
[58] Solum and Chung, "Layers Principle," at 816.
[59] Werbach describes layered models as a "conceptual tool" and as such they "need not be uniform." Werbach, "Breaking the Ice," 71 .
[60] *Id.*; Kevin Werbach, "A Layered Model for Internet Policy," *J. on Telecomm. & High Tech. L.* 1 (2002): 37; David P. Reed, "Critiquing the Layered Regulatory Model," *J. on Telecomm. & High Tech. L.* 4 (2005): 281; Craig McTaggart, "A Layered Approach to Internet Legal Analysis," *McGill L.J.* 48 (2003): 573; Lessig, *Code,* 144-145.
[61] It should be noted here that the technical description is meant to be a rudimentary account of the workings of the Internet. This archetypical description of the Internet is meant reveal its basic structure as a network of interactions, but is not necessarily a description of each individual interactions which can take place in myriad ways as each of the network of networks can apply different technologies at their respective logical layers. Additionally, the applications layer leaves a wide range of opportunity to change the nature of Internet transactions.

Post	Kulesza	Werbach	Solum & Chung

Fig. 2.1: Various Layered Models

i. The Physical Layer

At the bottom of the conceptual stack is the physical layer. The physical layer is made up of the hardware on which Internet runs. This hardware consists of routers, servers, cables (copper and fiber optic), cell towers, satellite links, and other telecommunications technologies.[62] This infrastructure is essentially the connective tissue of the Internet providing the medium through which information is transmitted. The physical layer includes all the physical equipment associated with the Internet. This importantly includes the Internet backbones and telecommunications networks, which provide the physical means through which data flows.

Internet backbones are a group of services providers that connect to route information transfers between autonomous networks.[63] These providers sell internetwork connectivity access to other providers who provide services to third parties such as individual users or corporations.[64] This secondary set of providers are commonly known as Internet service providers (ISP). An Internet backbone

> essentially forms its own network that enables all connected end users and content providers to communicate with one another. End users, however, are generally not interested in

[62] Werbach, "Layered Model," 60.
[63] Rick Osgood, "Net Neutrality and the FCC Hack," in *Hackaday Omnibus 2014*, ed. Mike Szczys, 2014 at 32
[64] *Id.*

> communicating just with end users and content providers connected to the same backbone provider; rather, they want to be able to communicate with a wide variety of end users and content providers, regardless of backbone provider. In order to provide end users with such universal connectivity, backbones must interconnect with one another to exchange traffic destined for each other's end users.[65]

Backbones route the flow of information among networks. It is important to note that their function is only the transfer of data: the core function of backbones is not storage of the information on the Internet; it is the transmission of data among networks.

The backbone providers and the providers to whom they sell, send data to users via telecommunications networks. For instance, most home users connect to the Internet via telephone wires or coaxial cable - both of which were installed to be used as a medium for different technologies. But users can also connect to the Internet via cellular networks, radio frequency or wifi, or through dedicated lines. Two things should be noted at this point. First, the Internet is running on a diversity of networks that deploy different connective technologies. This means that it facilitates a high level of interoperability among diverse technologies. Second, these networks are owned by a diverse group of actors, meaning there is a high level of interoperability among entities. The Internet's functionality is centered on this technological ambivalence towards the medium of transmission as well as the identity of the transmitter or recipient of the transmission. This is dramatically different from previous telecommunications technologies which were regulated according to the

---

[65] Michael Kende, "The Digital Handshake: Connecting Internet Backbones" (Washington, D.C.: Federal Communications Commission, 2000), 3.

specific technological parameters which limited interactivity. For instance, broadcast was regulated according to principles that maximized the efficient use of the scarce electromagnetic spectrum, whereas telephone regulation was used to maximize public access.[66] Technological ambivalence is indicative of a trend that can be seen at all layers of the conceptual stack: convergence. Convergence is a process through which the "historical distinctions between communications networks are melting away."[67] Convergence is a product of the logical layer, which is next in the conceptual stack of layers.

ii. The Logical Layer

Convergence occurs at the physical layer because the logical layer re-configures how information is sent over the physical layer. The logical layer consists of the software protocols that define the data being transferred by the Internet. All telecommunications systems transfer data electronically, but traditionally this signal was analog and was limited by the strictures of the technologies that carried analog signals.[68] The advent of computers enabled digitization, which allowed for the same content to be encoded as standardized data, which are "fundamentally just a string of ones and zeros" and are

---

[66] *See generally*, Thomas G. Krattenmaker, *Telecommunications Law and Policy*, 2nd ed. (Durham, NC: Carolina Academic Press, 1998) and Charles H. Kennedy and M. Veronica Pastor, *An Introduction to International Telecommunications Law* (Boston: Artech House, 1996).

[67] Werbach, "Breaking the Ice," 61. *See also*, Kulesza, *International Internet Law*, 53; Wayne McIntosh and Cynthia Cates, "Hard Travelin': Free Speech in the Age of the Information Super Highway," in *The Politics of Cyberspace*, ed. Chris Toulouse and Timothy W. Luke (New York: Routledge, 1998) 95, 102-03; Damian Tambini, Danilo Leonardi, and Christopher T. Marsden, *Codifying Cyberspace: Communications Self-Regulation in the Age of Internet Convergence* (Routledge, 2008) 3-4; Jayakar, "Globalization and the Legitimacy," 719.

[68] Leiner et al., "A Brief History of the Internet."

"ultimately interchangeable, meaning any communications platform can in theory, offer any service."[69]

The heart of the Internet is the Transfer Control Protocol/Internet Protocol (TCP/IP).[70] This protocol sets the standards for transmission of data on the Internet. It defines two distinct functions. First, it defines how the information being sent should be packaged. Digital information, unlike analog information, is easily severed and reassembled. When information is sent over the Internet, a computer program on the end user's device, will slice it up into small packets of data. Each packet is labeled with the order it should be reassembled. The second function it describes is the internet protocol, which places a distinct address on each packet that tells nodes on the network where it should be sent. This process known as packet switching.[71]

Packet switching revolutionized telecommunications, which to that point transmitted analog signals and depended on circuit switching. Every device on the Internet has an IP address, a numeric identifier for all traffic to and from that device, which is similar to a phone number.[72] Historically when a call was made on a landline, an analog signal was sent that must be connected in a constant circuit to the other end of the call.[73] That circuit is connected

---

[69] Kevin Werbach, "Breaking the Ice," 62; David G. Post, "Against 'Against Cyberanarchy,'" *Berkeley Technology Law Journal* 17 (2002): 1375-76.
[70] For a variety of other explanations of the TCP/IP architecture see Post, *Jefferson's Moose,* chapters 4-6; Lessig, *Code,* 43-45; and David D. Clark and Susan Landau, "Untangling Attribution," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, (2010) 27.
[71] Brate, *Technomanifestos,* 104-05.
[72] For a deeper understanding of IP addresses, *see* Laura DeNardis, *The Global War for Internet Governance* (New Haven: Yale University Press, 2014) 37-41.
[73] Leiner et al., "A Brief History of the Internet."

through a centralized operator, a process known as circuit switching.[74] A visual of this process was a common feature of early television, which would often use a split screen to show the operator physically connecting the continuous circuit on a switchboard with a patchcord. Packet switching on the other hand does not require a continuous connection because the information is broken into data packets instead of a continuous analog signal. This means that the packets can be routed via any combination of routes through the network in order to get them to the proper IP address. Instead of a centralized operator, there are decentralized routers and nodes through which a packet travels. This type networking allows for more efficient transfer speeds by distributing the loads across the network.[75] In other words, the packets do not need to travel along the same path or arrive in the same order, so packets are routed along the most efficient route possible. In practical terms this means that an email, for instance, once broken down into packets could travel through numerous different servers located in geographically disperse places. Packet switching avoids the strain on the central operator from which circuit switching suffers.[76]

A number of salient features of this system should be emphasized. First, the TCP/IP protocol is designed to transfer a packet regardless of information it contains. Importantly, as currently configured, the routers on which the protocol runs do not register what is "in" the packet.[77] The router simply passes the packet along to the next waypoint on its journey. This is why the Internet is

---

[74] *Id.*
[75] *Id.*
[76] For more on network configurations see Post, *Jefferson's Moose*, 47-59.
[77] This is how the Internet was designed to operate, but it should be noted that deep packet inspection technologies are in used by some entities. *See* DeNardis, *Global War,* 206-07.

sometimes called "stupid."[78] The design of the Internet is simply to allow information to be freely transferred among the various nodes on the network meaning that the content of those packets is not stored in the logical layer.[79] Second, this means that the transmission of the data is neutral in regards to the technology on which it travels. The Internet can run over copper cable, fiber optics, radio waves, satellite transmissions, or anything else that can carry electronic communications. TCP/IP provides a standardized manner for packaging and addressing data for transmission. Third, as a result of this technological ambivalence the Internet has the potential to be widely accessible. The Internet is not a single network, it is a network of networks facilitated through a standard protocol. The Internet, when viewed at the protocol layer facilitates the linking of dissimilar networks as data packets can ride on any telecommunication infrastructure.[80] Finally, since the standard protocol is meant to ensure interoperability, the network itself is rhizomatic in nature inasmuch as it is a non-hierarchical assemblage of networks.[81]

It was stated earlier that the logical level functions as the heart of the Internet. This is because it serves as the vital link between the physical layer below it and the applications layer above it through an "open network

---

[78] Post, *Jefferson's Moose*, 80.
[79] This is the third of four ground rules that were theorized to undergird open network architecture. Leiner et al., "A Brief History of the Internet."
[80] Mattelart, *Networking the World,* 4 ("Communicating means standardization and doing away with chance.").
[81] Betz and Stevens, *Cyberspace and the State,* 38. The original design of ARPANET, the Internet's precursor, "was based on the idea that there would be multiple independent networks of rather arbitrary designs . . ." Leiner et al., "A Brief History of the Internet." *See also* James D. Fielder, "The Internet and Dissent in Authoritarian States," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton: Taylor & Francis, 2013), 168.

architecture," which is the "key underlying technical idea" of the Internet.[82] Open network architecture provides a link among disparate physical layer technologies and disparate applications layers technologies by creating a common language of communication *among* them as opposed to *between* them.[83] The logical layer drives convergence at the physical layer because of these attributes, but this convergence is experienced at the applications layer.

iii. The Applications Layers

The statement that the Internet is stupid is based on the logical layer's functionality to be non-discriminatory in the transferring of data packets, and is commentary on the popular conceptualization of the Internet as a vast archive of knowledge. The Internet is dumb because it is an end to end network, which means intelligence is "vested in the edge."[84] The devices and applications they run at the edges of the network are where the Internet "happens," so to speak. The data packets that the logical layer transmits are only intelligible at the ends of the network, because "the Internet . . . was not designed for just one application, but as a general infrastructure on which new applications could be conceived."[85] Essentially, to use a buzz phrase ushered in by smartphones, "there's an app for that."[86]

---

[82] Leiner et al., "A Brief History of the Internet."
[83] Circuit switching is network architecture that facilitates communication between technologically equivalent devices. Leiner et al., "A Brief History of the Internet."
[84] Lawrence Lessig, *Code*, 111
[85] Leiner et al., "A Brief History of the Internet."
[86] The advertising phrase, trademarked by Apple, was notably appropriated by US Secretary of State Clinton in a speech on Internet freedom. Hillary Clinton, "Internet Rights and Wrongs: Choices & Challenges in a Networked World," remarks, *U.S. Department of State*, (February 15, 2011), http://www.state.gov/secretary/20092013clinton/rm/2011/02/156619.htm. (" . . . we

The World Wide Web (WWW) serves as an excellent example. If asked "what is the Internet?" many people would likely describe it as the WWW as this is still one of the most common ways that people experience the Internet.[87] But the WWW is an application that runs on a device and functions at the applications layer.[88] A rudimentary explanation of how the WWW works will help to show how the applications layer functions as well as the end-to-end principle. If you want to view a web page you type a Uniform Resource Locator (URL), for instance http://www.dudeism.com, into your web browser's address bar.[89] The first thing to be noted is that there are multiple web browsers made by a variety of entities including corporations, non-profits, and individual programmers.[90] The web browser then sends a request via your Internet Service Provider (ISP) to a server which contains a file with a list of URL's associated with the .com root name.[91] It searches this list, called a root file, for dudeism.com, and finds the IP address of the device that is associated

---

believe there is no silver bullet in the struggle against internet repression. There's no app for that.")

[87] *For instance*, Toulouse, "Introduction," 2 ("What has made all the difference to the Internet . . . is the invention of HTML . . . and the extraordinary wild-fire development of the World Wide Web.") and Betz and Stevens, *Cyberspace and the State,* 13.

[88] Leiner et al., "A Brief History of the Internet." *See also,* Verizon v. FCC, No. 11-1355, 740 F. 3d 623 (Court of Appeals, Dist. of Columbia Circuit 2014) at 36.

[89] The HTTP portion of the URL denotes the type of data being sought, in this case it stands for Hypertext Transfer Protocol. This portion of the address is a Uniform Resource Identifier (URI), and it identifies that a hypertext file is being sought. There are numerous URIs indicating the type of data a given application is seeking. These include the common File Transfer Protocol (FTP), Internet Chat Relay (IRC), and HTTP Secure (HTTPS). In modern browsers there is no need to type this portion because the software defaults to HTTP addresses.

[90] For instance, Firefox, Opera, Microsoft Explorer, Google Chrome, and Safari are all different web browsers.

[91] .com is a generic Top Level Domain (gTLD). Domain names are part of the Domain Name System (DNS), which is administered by ICANN. Mark VB Partridge and Scott T. Lonardo, "ICANN Can or Can It?: Recent Developments in Internet Governance Involving Cybersquatting, Online Infringement, and Registration Practices," *Landslide* 1, no. 5 (2009): 24–29. *See also*, DeNardis, *Global War*, 41-44.

with dudeism.com through the Domain Name System (DNS).[92] In simple terms, 'dudeism.com' is a text based identifier for the IP address, which is 216.172.106.18.[93] The ISP, on your behalf, then contacts this device, which has been configured to act as a server,[94] and looks for a directory named "www."[95] Once there, the browser will look for a default file, most commonly titled "index.html," the ISP will transfer a copy of this file, which your computer downloads.[96] A copy of the file named index.html now exists on your computer, and your browser opens this file, which contains computer code that a web browser understands and executes.[97] This code tells the browser what to display on your screen. This entire transaction is facilitated by the logical layer and is transferred as digital electromagnetic signals across the physical layer.

In this example, we can see very clearly that the information that we access while connected to the Internet is stored at the periphery. The web page

---

[92] The URL is essentially a tool "[t]o make it easy for people to use" the Internet by associating strings recallable text with strings of hard to remember numbers. The DNS "permitted a scalable distributed mechanisms for resolving hierarchical hostnames" into IP addresses. Leiner et al., "A Brief History of the Internet."

[93] Partridge and Lonardo, "ICANN Can or Can It?", 24.

[94] A server is another application on the applications layer. A server, though usually on specialized hardware, is simply a computer application that makes computer files available to other computers on a network. In this case the server has been configured to be open to requests from any network. Servers are essentially file systems configured in a hierarchical directory, and can be understood to function in a substantially similar way to the file and folder system found in most desktop operating systems.

[95] WWW in this case denotes a file folder on the server that contains files for the World Wide Web. While WWW here indicates that the these resources are for the Internet, it is often unnecessary. Indeed dudeism.com resolves the same as www.dudeism.com. Nor does this portion of the URL need to be www. For example, the author owns www.blountsfolly.com, but hosts a blog at space.blountsfolly.com. URLs are read hierarchically from right to left.

[96] Tambini et al, *Codifying Cyberspace,* 7. "index.html" is simply a filename, similar to dissertation.doc, which indicates a Microsoft Word document named "dissertation." "index" is an arbitrary default filename for which browsers search as a result of their programming. Servers can also be programmed to serve a default file different from index.html. "html" is a file type which indicates a text file written in hypertext markup language (HTML). HTML is computer language that browsers understand and use to display a web page.

[97] It is easy to see the code of the web page in a browser window. Most browsers allow you to see the source code through a "view source" option located in that browser's tool menu. When used this tool will display the text of the loaded html file.

is not "on" the Internet, rather it is accessible via the Internet, and it exists on a connected device. The file that you see is literally copied to your computer, meaning that information from afar becomes immediately localized, even if temporarily, in the memory of the user's device so that it can be manipulated by the software on that device.[98] This is the end-to-end principle in practice, which is "hard-wired into the Internet's architecture."[99] In technological terms, this is known as "peering."[100] Peering implies equality created between devices through the common protocol.[101]

A practical effect of the end-to-end principle means that convergence is experienced for the user at the applications level. Indeed, the "there's an app for that" catchphrase captures this very idea. Convergence is experienced because information can be digitized, and technological ambivalence facilitates a diversity of applications with different outputs. This has resulted in a bloom of technological innovation as applications and networks have proliferated.[102] Possibly the best example is the nascent Internet of Things (IoT) concept in which devices other than traditional computers are being networked for applications such as home automation. IoT allows nearly any machine that can

---

[98] Lawrence Lessig, *Code,* 268. ("There is no way to use a work in a digital environment without making a copy")
[99] Damian Tambini et al, *Codifying Cyberspace,* 2.
[100] Leiner et al., "A Brief History of the Internet."
[101] This is equality in technological terms only. Equality in a technological sense should not be confused with equality in a legal or political sense.
[102] Tambini et al, *Codifying Cyberspace,* 9 (linking interoperability to innovation) and Leiner et al., "A Brief History of the Internet." (the Internet as an "infrastructure" for "new applications") and Goodman and Chen, "Modeling Policy," 120. Examples of how closed standards restrict innovation by restricting interoperability include, the Marconi Company's telegraph standards, Jayakar, "Globalization and the Legitimacy," 722 and AT&T's attempts to maintain it's monopoly by disallowing non-AT&T devices to connect to it's network. Krattenmaker, *Telecommunications Law and Policy*, 367-69. *See also* American Broadcasting Company v. Aereo, 573 U.S. (2014) (court holding that technology that online streamed a broadcast signal received by tiny antennae is functional equivalent of cable TV).

be manipulated by a circuit board to be network into the spatial geography of Cyberspace, so for example there are now lightbulbs on the Internet.[103] Innovation at the applications layer is further driven by the decentralization of the logical layer, which gives more individuals access to information systems.[104]

Another reason that innovation happens at the applications layer is that in order to facilitate interoperability of networks, the protocols of the logical layer are open, allowing anyone with proficient skill in programming to be able to write an application that facilitates new types of information flows. This significantly lowers the cost of development of new products, but it also means that individual programmers can change how Internet communications work - or more precisely change the nature of communications through the applications layer. A good example is Phil Zimmerman who wrote the Pretty Good Privacy (PGP) program. This public key encryption program was developed to allow users to send secure encrypted messages to other individuals via the Internet.[105] However, encryption programs like PGP are classified as weaponry under the US International Traffic in Arms Regulations (ITAR).[106] These restricted the export of PGP as a defense article.[107]

---

[103] Jane Wakefield, "Smart LED Light Bulbs Leak Wi-Fi Passwords," *BBC News*, July 8, 2014, http://www.bbc.com/news/technology-28208905.
[104] Verizon v. FCC at 36 (noting that the WWW is an example of such innovation as it was developed by "Sir Tim Berners-Lee, who although not working for an entity that operated the underlying network, was able to create and disseminate this enormously successful innovation without needing to make changes to previously developed Internet protocols or securing any approval from network operators.")
[105] Andy Greenberg, *This Machine Kills Secrets : How WikiLeakers, Cypherpunks and Hacktivists Aim to Free the World's Information* (New York: Dutton, 2012) 70-76.
[106] Id. at 72-74.
[107] International Traffic in Arms Regulations, 22 C.F.R. 121.1 Category XII(b) (2015).

The example of PGP illustrates, three important things that will be seen in a variety of contexts within this research. First, the nature of Internet transactions was changed by a single coder. This means that a single individual, taking advantage of the innovation friendly nature of the end-to-end network was able to change the possibilities for human interactions on the Internet and in Cyberspace. Second, this technology was unable to be contained by the state. ITAR is specifically directed at the export of weapons technologies that appear on the United States Munitions List (USML). These regulations apply to technology crossing the border of the United States, yet PGP is freely available worldwide, indicating a breach of the space of the state. This availability is driven in part by ephemeral nature of software, which is easily shared online. Finally, this application, for the purposes at hand, can not be imbued with normative power. The descriptive bent of this chapter requires that PGP, like all programs at the applications layer, be recognized as a technology that can enable good interactions (e.g. giving voice to political dissidents in repressive regimes) as well as bad interactions (e.g. giving cyber criminals the ability to transmit illicit data free from scrutiny). The innovation facilitated by the applications layer is such that it creates openings for all entities - whether they be normatively good or bad; state or non-state; commercial or criminal; individual or collective - to engage in a variety of measures of control and liberation.

iv. The Content Layer

Content is what concerns most people using the Internet. They neither care to know nor need to know the specifics of the code that is running beneath the content layer at either the application or logical layer. Nor do they likely understand the intricacies of the physical network past their connection to the ISP. They are concerned with content, and in a digital world, content can be just about anything. While sights, sounds, and words have been the traditional domain of the Internet, in no way is the Internet limited to transferring only these types of information.

The Thingaverse website is instructive.[108] Thingaverse is an online repository of 3d printable objects. Or more precisely, it is a repository for programs that will instruct a 3d printer to print a specific three dimensional object. The object itself is not sent through the Internet, but the effect is the same as the object materializes at the user's device. Essentially, if hardware can be developed that can output a type of information digitally at the applications layer, then that data can be transferred across the Internet. What the end device outputs is the content layer.

The content layer is, obviously, the layer where most of the public debate on Internet regulation occurs. This is because the interaction of the three layers below the content layer allow for large amounts of data to be transferred quickly to anyone no matter where they are, so long as they have network access. The content layer of the Internet is dramatically different from the content layer of previous telecommunications sources, which disaggregated different functions. Broadcast is a one directional method that reaches mass

[108] Thingaverse, https://www.thingiverse.com/ (last accessed September 30, 2015).

numbers of people, and telephone allowed for bidirectional interactions but not on a mass scale. The centralization of broadcast made it easily susceptible to societal controls over the content (whether through regulations or norms). Telephone on the other hand, offered little control over content, but architecturally minimized the possible reach of the phone. Content on the Internet is both multidimensional and mass, meaning there is low control over content and the reach of information. This can most clearly be seen in the concerns that numerous states have about content coming in through their borders such as political propaganda or pornography.[109]

Much of the discussion on Internet governance is on issues such as free speech and censorship, which means that the focus is often on the content layer. This is because the three underlying layers in concert amplify traditional societal concerns with flows of information. Information now flows across networks that are distributed in nature, permeate borders, and maximize access by individuals. This is a paradigm shift in telecommunication technology, and its effects on society are broad. The content layer is the locus of these effects, as it is the content - whether the content is in the form of

---

[109] This concern has a rich history in international law. For examples in other mediums see generally Madelaine Eppenstein and Elizabeth J. Aisenberg, "Radio Propaganda in the Contexts of International Regulation and the Free Flow of Information as a Human Right [notes]," *Brooklyn Journal of International Law* 5 (1979): 154; Horace B. Robertson, "The Suppression of Pirate Radio Broadcasting: A Test Case of the International System for Control of Activities Outside National Territory," *Law and Contemporary Problems*, 1982, 71–101;United Nations General Assembly, "Res. 37/92: Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting," December 10, 1982 at A(1); and EUTELSAT, "Eutelsat condemns jamming of broadcasts from Iran and renews appeals for decisive action to international regulators," PR/62/12, Oct. 4, 2012, http://www.eutelsat.com/home/news/press-releases/Archives/2012/press-list-container/eutelsat-condemns-jamming-of-bro.html.

economic activity, religious ideology, political activism, or criminal conduct - crossing the Internet that creates issues for society.

II. Cyberspace

A genre of movies & songs from the late 70s and earlier 80s celebrate the culture of Citizen Band (CB) radio.[110] These cultural nuggets give a glimpse into a culture built around a network of people that interact on CB radio channels. In these films, news often spreads quickly across the network leading to collective group action, which usually finds expression in highway hijinks. The CB goes hand in hand with the automobile as both served as potent symbols of individual autonomy.[111] One of the most notable things in this genre is that the CB has its own language which socializes the participants in the network. CB in these films is portrayed as more than just a communication technology. Instead, it is the glue that structures the social space of mobility driven culture.

---

[110] In particular the catalog of Burt Reynolds is notable with *Smokey and the Bandit* (1977), *Smokey and the Bandit 2* (1980), *Cannonball Run* (1981), and *Cannonball Run II* (1984). Aficionados might also appreciate television series such as the *Dukes of Hazzard* (1979-1985); *B.J. and the Bear* (1979-1981), and *Movin' On* (1974-1976). Additionally, country music offered up a plethora of songs such as C.W. McCall's "Convoy" (1975), Red Sovine's "Teddy Bear" (1976), and Cledus Maggard's "CB Lingo" (1976).

[111] It is no coincidence that CB narratives such as *Smokey and the Bandit* often glorify running from the law enforcement in high speed chases.

If the Internet is a stack of functional layers, then Cyberspace is the Internet with the addition of a social layer.[112] This may seems a little obvious, the Internet is not a natural phenomena and is a human creation, meaning a social layer may be presupposed. While true, the point here is to highlight something more than just human usage of the technology. It is, instead, to highlight the scope and integration of the Internet into societies globally. The social layer creates a "structure of metaphors and visions" that conceptualize the space that the Internet creates.[113] The technology of CB radio still exists and is used, but when was the last time that a story about human activities on CB topped the news? The reason for the dearth of media coverage of the CB network is that much of the social layer has been removed. CB was supplanted by cellular phones which better served most people's needs. The drop in scale of usage means that the network has less importance.[114] It is precisely the fact that 43% of the world's population is connected to the Internet and this number is rapidly growing that makes Cyberspace a such an important social phenomenon.[115] Social interactions of all sorts are taking place there, but where is *there*?

This section will first establish the spatial narrative of cyberspace as the dominant conceptualization of cyberspace. Then it will probe the attendant

---

[112] Lessig, *Code 2.0*, 9; Kulesza notes that limiting understanding of the Internet to "physical elements . . . does not reflect the current nature of the phenomenon." Joanna Kulesza, *International Internet Law*, x-xi.

[113] John Streck, "Pulling the Plug on Electronic Town Meetings: Participatory Democracy and the Reality of Usenet," in *The Politics of Cyberspace*, ed. Chris Toulouse and Timothy W. Luke (New York: Routledge, 1998) at 20.

[114] *See generally* Post, *Jefferson's Moose*, 68-69 ("Scale really **does** matter.")

[115] International Telecommunications Union, *ICT Facts and Figures 2015* (2015) at 2. This report also notes that a digital divide between developed countries and developing countries still exists, but that divide is shrinking. Id. at 3.

metaphors to this spatial narrative and attempt to identify cyberspace in terms of location and place.

i. Cyberspace as Space

A great deal of the early literature on Cyberspace debated specifically whether it constituted a new space distinct from the space inhabited by states. The legal debate was focused on the multijurisdictional effects of Cyberspace, is best exhibited in the scholarly exchange between Jack Goldsmith and David Post. Goldsmith argues that Cyberspace presents no novel legal problems, and that "Cyberspace transactions do not inherently warrant any more deference by national regulators, and are not significantly less resistant to the tools of conflict of laws, than other transnational transactions."[116] Post on the other hand, a self-proclaimed "cyberexceptionalist," argues that cyberspace should be approached as a new geography that humans inhabit. At the heart of this debate is one fundamental issue: is cyberspace a space?

Goldsmith's answer that inasmuch as Cyberspace exists on the Internet, then cyberspace exists where the physical links and users do. The physical layer and users exist within physical territory of the state. Through this lens Cyberspace only has a "space" to the extent that its physical components do. Post on the other hand would argue that something fundamentally different is happening, because Cyberspace is now mediates the vast number of human interactions without regard to the physical and political boundaries of the

[116] Jack L. Goldsmith, "Against Cyberanarchy," *The University of Chicago Law Review* 65, no. 4 (1998): 1201.

terrestrial sphere.[117] He argues that the difference between real space and Cyberspace is akin to the difference between "life on land" or "life in the sea."[118] In this model, Cyberspace's spatial dimension is defined by the entire layer stack, and not just the territorially grounded physical layer.

The problem is that, to some extent, both authors are correct. Most of Cyberspace's physical manifestations do exist within state borders, thus a regime such as that in North Korea can control the spread of cyberspace by maintaining tight controls on the dispersion of physical technology.[119] Cyberspace, at the same time, defies containment by the state and seemingly exists everywhere. The Pirate Bay, a prominent torrent website carrying links to copyrighted material, has repeatedly evaded being shut down by state power structures through the use of mirrors which disperse the site across servers in various geographic regions.[120] The reality is that Goldsmith's argument while logically solid is often 'more honoured in the breach than in the observance.'

---

[117] Post, "Against 'Against Cyberanarchy,'" 1374.
[118] Post, "Against 'Against Cyberanarchy,'" 1374.
[119] This is why activists often try to physically subvert the border by sending technology across with balloons. Thor Halvorssen and Alexander Lloyd, "We Hacked North Korea With Balloons and USB Drives," *The Atlantic*, January 15, 2014, http://www.theatlantic.com/international/archive/2014/01/we-hacked-north-korea-with-balloons-and-usb-drives/283106/.
[120] *For instance*, Mark Brown, "Pirate Bay Mirror Is Proxy-Friendly, Bypasses UK Ban," *Wired UK*, May 24, 2012, http://www.wired.co.uk/news/archive/2012-05/24/the-proxy-bay; Stephanie Mlot, "The Pirate Bay Is Back Online (Sort Of)," *PCMAG*, December 15, 2014, http://www.pcmag.com/article2/0,2817,2473661,00.asp; and Jasper Hamill, "Pirate Bay Is BACK - Torrent Site to Return in One Week," *The Mirror*, January 26, 2015, http://www.mirror.co.uk/news/technology-science/technology/pirate-bay-back---torrent-5045073. There are a number of sites that list the mirrors such as Proxy Bay, https://proxybay.la/ (last accessed September 30, 2015). see also Daniel Domscheit-Berg, *Inside Wikileaks : My Time with Julian Assange at the World's Most Dangerous Website* (New York : Crown Publishers, 2011), 21 (". . . But they weren't aware that another part of the Wikileaks principle: when you took down one page from the Internet, twenty more would pop up in different locations to take its place. It was virtually impossible to take us off the Internet.")

One of the problems with Goldsmith's view is that it ignores a simple fact: humans understand Cyberspace as a space. Cyberspace is conceptualized as space through a spatial narrative that serves as a dominant metaphor for human understanding of cyberspace.[121] Goldsmith's argument seems facile when applied to the Internet, but it becomes dissonant when applied to Cyberspace. This is because the spatial narrative makes technological reductionism impossible, because "the way we describe a thing can change the nature of that thing."[122] The spatial narrative that accompanies Cyberspace is very much a description of social experience in Cyberspace.[123] The spatial narrative "transform[s]" the "experience" of cyberspace."[124]

The spatial narrative is found within the common vocabulary used to describe cyberspace. Users go *on*line and visit chat*rooms* or web*sites*. These can be found by typing in an IP *address* which is often denoted by a Uniform Resource *Locater* (URL) which includes a *domain* name. That name is understood to be *owned* by an entity, which will probably have a fire*wall* up to keep intruders out of its *local* server. Lessig notes that "cyberspace is something you get pulled 'into.'"[125] Ferguson and Mansbach note terminology

---

[121] In other words, Goldsmith "presuppose[s] a hard division between a regulated physical layer and everything else." Werbach, "Breaking the Ice," 79. Competing conceptual models include cyberspace as time David Gelernter, "The End of the Web Search and Computer as We Know it," *Wired*, February 1, 2013, http://www.wired.com/opinion/2013/02/the-end-of-the-web-computers-and-search-as-we-know-it/; and cyberspace as a quantum space, Charles Seife, *Decoding the Universe* (New York: Penguin Books, 2006) and Seth Lloyd, *Programming the Universe* (New York: Alfred A. Knopf, 2006).

[122] Streck, "Pulling the Plug on Electronic Town Meetings," 26.

[123] Fritsch, "Technology and Global Affairs," 31 (Technology "is part of our social reality and only gains meaning when described and interpreted in social terms.").

[124] Streck, "Pulling the Plug on Electronic Town Meetings" 26. ("Experience, or at least our understanding of it, follows language, it does not precede it.")

[125] Lawrence Lessig, *Code 2.0*, 9.

such as "electronic highway, electronic mail, infobahn, infosphere, . . . information superhighway . . . online community, virtual community, and virtual reality."[126] Barlow's influential "Declaration of Independence for Cyberspace" declares that states have "no sovereignty" in the "new home of the mind."[127] Resnick refers to the "land of Cyberspace,"[128] and Post uses the metaphor of exploring a new territory to evaluate law in cyberspace.[129] In short Cyberspace has a "placeness."[130]

This metaphor is central to the social construction of cyberspace, because "metaphors have a profound effect on computing."[131] As the Internet reached more users, these concepts could often be found in the iconography of Internet Service Providers (ISP). For instance, America Online (AOL) was one of the first mass market ISPs, and, as a result, AOL was the initial first online experience for a large portion of the Internet users that flooded the Internet when it was privatised in the mid-1990s.[132] AOL used skeuomorphs to orient these new users. For example, the sound of an opening and closing door was used to denote entrance and exit of users from chatrooms. Similarly, an icon of a traditional roadside mailbox denoted the email server thereby linking the email concept to its physical counterpart which would have specific geographic

---

[126] Ferguson & Mansbach, *Globalization*, 10.
[127] John Perry Barlow, "The Declaration of Independance for Cyberspace," February 8, 1996, https://projects.eff.org/~barlow/Declaration-Final.html.
[128] David Resnick, "Politics on the Internet: The Normalization of Cyberspace," in *The Politics of Cyberspace*, ed. Chris Toulouse and Timothy W. Luke (New York: Routledge, 1998) at 51.
[129] Post, *Jefferson's Moose*.
[130] David R. Johnson and David Post, "Law and Borders: The Rise of Law in Cyberspace," *Stanford Law Review* 48, no. 5 (1996): 1379; *see also* Betz and Stevens, *Cyberspace and the State,* 13.
[131] Gelernter, "The End" and Streck, "Pulling the Plug on Electronic Town Meetings," 26 ("Whoever controls the metaphors, controls cyberspace.")
[132] For more on AOL see Lawrence Lessig, *Code 2.0* (Basic Books, 2006) 88-94.

location denoted by a physical address. AOL is not an isolated example; skeuomorphs have been used extensively in digital design to help orient users.[133] The desired effect is the creation of a visual, spatial geography that new users can easily orient themselves using concepts associated with physical geography.

The pervasiveness of the spatial metaphor illustrates something very important which is often overlooked in Goldsmithian type arguments. No matter whether Cyberspace exists in a physical place, it is conceptualized and understood as a space by its users. Cyberspace is experienced as space, and it is "different from real space."[134]

ii. Cyberspace as a Place

If Cyberspace is a space then where is it? Space is intrinsically linked to the idea of location. Locating Cyberspace is a difficult task, and the spatial narrative can only be pushed so far.[135] Part of the problem is that an individual can never be wholly in Cyberspace, yet this has not kept cyberspace from being understood in terms of spatial concepts. The Internet's layers, discussed above, construct the spatial geography of Cyberspace by setting the metes and bounds of human interaction online. In the same way that rivers and mountains create natural boundaries, Internet technology also creates "natural" boundaries for

---

[133] Mostafa Heddaya, "See A Map, Not a Territory: Apple and the End of Skeuomorphism," *Hyperallergenic*, June 27, 2013, http://hyperallergic.com/74308/a-map-not-a-territory-apple-and-the-end-of-skeuomorphism/

[134] Joanna Kulesza, *International Internet Law*, xii.

[135] *For instance*, Johnson and Post, "Law and Borders," 1378 ("Efforts to determine 'where' the events in question occur are decidedly misguided, if not altogether futile.")

human interactions.[136] The spatial metaphor invokes a number of important concepts that shape social understanding of Cyberspace.

The cyber realist claims that Cyberspace is located within the physical bounds of the state. For instance, in terms of the WWW, URLs denote a specific server on the Internet, which does exist in a physical location and is owned by an entity. The URL is conceptually very similar to the idea of an address, which denotes a specific geographic location. So the URL points to a place with a location that is within the borders of a state, and to a specific *res* within that state.[137] This answer to the location problem is not without issues, though. URLs are freely associable to other servers that can contain either the same information or different information.[138] The server itself may be static, but the website that is visited in Cyberspace is not. It can move with a simple change to the DNS root file, which will resolve the URL to a different IP address, and to a different *res*. The distinct *site* that the user *visits* is indeed fluid in a spatial sense. Cyberspace exists in a geographic duality. Like Papa Legba with one foot in the grave, Cyberspace has one foot firmly planted inside a state borders, but the other foot is planted somewhere outside those borders.

The spatial narrative is a social conceptualization that renders Cyberspace as a "distinct 'place.'"[139] As a place it exists concurrently yet

---

[136] Natural here is used analogously, not to imply that Cyberspace is natural. Cyberspace is by definition unnatural. *See* Lessig, *Code 2.0*, 31 ("If there is any place where nature has no rule, it is Cyberspace.")

[137] For instance, the Silk Road was housed on a server in Iceland. Joshua Bearman, "The Untold Story of Silk Road, Part 2: The Fall," *WIRED*, May 14, 2015, http://www.wired.com/2015/05/silk-road-2/.

[138] The URL is a tool for making WWW addresses easy to remember. It is only a string of text that is resolved to an IP address which is actually where a WWW pages exists. Leiner et al., "A Brief History."

[139] Johnson and Post, "Law and Borders," 1378.

separately from the state, meaning it both borders and intersects the state. Because Cyberspace has transnational effects that are unbounded by physical geography, it is submitted here that Cyberspace constructs and is located in a global space.[140] A global location implies two things. First, Cyberspace is a space with world scale, and its growing level of integration into societies world wide is hardly deniable. Second, Cyberspace is a geography that is exterior to international space. The network architecture that underlies Cyberspace allows it to evade the strictures of national borders. Global space is located where internationally defined territory thins and runs out.

To understand this, one must first recognize that the concepts of space and location also implicate further notions such as borders and property. The often quoted trope from the early days of the Internet that "borders are just speed bumps on the information superhighway" points directly to Cyberspace's spatial character and global location. Indeed the spatial metaphor of a highway is a reminder that all the locales in Cyberspace exist in the same place, or maybe better put: they all have addresses on the same street. All IPs on the Internet are equally close to the user. While the ability of states to raise borders in cyberspace is not completely absent, the user's ability to thwart those mechanisms allows for penetration of those borders at will, showing that software borders are indeed soft. The rhetoric of the spatial narrative supports this. For instance, John Perry Barlow's "Declaration of Independence for Cyberspace" declares explicitly that "[c]yberspace does not lie within [a state's]

---

[140] Similarly Kulesza argues that the Internet "[establishes] a new supranational space."Joanna Kulesza, *International Internet Law*, 29.

borders."[141] Barlow is linking the independence of Cyberspace to its own territorial sovereignty, stating later that he "felt like the answer to sovereignty was sovereignty. To fight them on their own terms."[142] The spatial narrative gives conceptual credence to extraterritoriality of Cyberspace.

The concept of property is also implicated. The Western norm of ownership and exclusion are set on end in places in cyberspace, which "makes a hall of mirrors out of conventional understandings of what constitutes private and public property."[143] Take the website example used above. Users often reference ownership of a web*site,* but this is inexact at best. What these users are describing is two different phenomena of "ownership." First, they are describing the URL which indicates location of the website, but this domain name is only registerable and not owned so an individual's rights in it do not represent traditional property rights.[144] Entities must maintain their registration in order to keep the URL, whether they use the URL or not. Interestingly, this means that it is possible to register a URL to keep it from becoming a place on the Internet. Furthermore, the URL can easily be pointed to another server by associating it to a new IP address, meaning that the URL as an owned space is to some extent ephemeral. This points to the second phenomena of ownership that users are describing when they discuss ownership of a website, which is ownership of the content that is displayed in

---

[141] Barlow, "A Declaration."
[142] Greenberg, *This Machine,* 256.
[143] Toulouse, "Introduction," 13.
[144] An individual can have intellectual property rights through a trademark used in the domain name. *See generally*, Robert P. Merges, Peter S. Menell, and Mark A. Lemley, *Intellectual Property in the New Technological Age, Sixth Edition*, 6 edition (New York: Aspen Publishers, 2012) 911-930.

the browser window, which can be thought of in terms of intellectual property.[145] Since the webpage is available worldwide, questions about the territory that protects those intellectual property rights arise. This becomes messier when one takes into account that a great deal of web content is copied and stored on the local machine, and when one contemplates that the success of social networking websites is often predicated on serving content that is sourced from somewhere other than the website's "owner." Interestingly, a third concept of ownership is not usually invoked when referencing website ownership, which is ownership of the server in the physical layer, where the cyber realist focuses analysis. This type of ownership is diminished in importance since a URL and data can be moved to new servers at will, meaning that the physical location changes fluidly.[146] Additionally, the entity that places the content on the server often rents that server space from a third party and has no physical control over it further muddying the ownership waters.[147]

The website example hints at the underlying issue for property narratives in Cyberspace: hard physical location is ephemeral because property in Cyberspace is practically infinite. Western understanding of property is predicated on scarcity, which rests in the idea that "they aren't making anymore of it." In Cyberspace, property is fragmented across physical space and metaphysical space, as a result of the logical layer which makes data

---

[145] Quite literally all three types: copyright for the contents, Lawrence Lessig, *Free Culture : The Nature and Future of Creativity* (New York: New York : Penguin Books., 2004); trademark for the URL and other branding, Partridge and Lonardo, "ICANN Can or Can It?."; and patent of the code itself, Vera Ranieri, "EFFecting Digital Freedom," *2600: The Hacker Quarterly*, v. 31/3, 2014, 52-53.

[146] Domscheit-Berg, *Inside Wikileaks,* 21.

[147] This server site is often outside the borders of the individual responsible for the date. *See* Bearman, "The Untold Story."

fungible in such a way that it can move freely from place to place, and it exists in all those places. Property in Cyberspace expands simply by adding devices with computer memory to the network, or by adding new files to established servers (e.g. adding a new post to a blog).[148] Notions of property based on scarcity and ownership become tenuous as scarcity decreases and ownership fragments.[149] So for instance scarcity of land is central to Schmitt's conception of the land generating the law, as it is the scarcity of land that drives its division. However, when territory is infinite the need for division is functional as opposed to economic.[150]

None of this is to say that traditional notions of borders and property do not still have sway. As noted earlier, Goldsmith's observation of physical location granting state's territorial control over Cyberspace technologies is relevant, because users are "always in both places."[151] This however, is only part of the story, because states can only control the parts of the Internet they can literally touch, but not necessarily all the parts of the Internet that can touch them. The technological landscape that intersects state territory is architected in such a way that much of cyberspace is located outside the state.

---

[148] Debora L. Spar, "The Public Face of Cyberspace," in *Global Public Goods: International Cooperation in the 21st Century*, ed. Inge Kaul, Isabelle Grunberg, and Marc Stern (New York, Oxford: Oxford University Press, 1999) 348 (The Internet "is almost infinitely expandable."); McIntosh and Cates, "Hard Travelin'," 95 (" . . . scarcity will be replaced by infinity . . .").

[149] Electromagnetic spectrum, for instance, is allocated on the basis of scarcity. Tambini et al., *Codifying Cyberspace,* 68; Ellen P. Goodman, "Media Policy and Free Speech: The First Amendment at War with Itself," *Hofstra Law Review* 35 (2007) 1221.

[150] This is not to argue that there is no economic value in domain names, but that value is derived not necessarily from scarcity, but from the idea contained in the domain name, which is most often linked to the name recognition associated with a company or brand. Thus any URL, in theory, has the potential to be of high value if it achieves high recognition, whereas real properties value is linked to physical attributes.

[151] Lawrence Lessig, *Code 2.0*, 298.

III. Metaphysical Geographies

The critical notion in this chapter is that Cyberspace is understood by humans as a space and as such it also has location and place. Despite its metaphysical nature, individuals can not help but envision Cyberspace in terms of its spatial characteristics. This is no surprise to anyone familiar with the literature on Cyberspace, which constantly struggles with the ethereal nature of a place that is both there and not there in the sense of "traditional dimensionality."[152] Indeed, the concept of virtual reality embeds the spatial narrative quite deeply into understandings of Cyberspace. At its inception, virtual reality was portrayed as the ability to go into a new space and to experience it as real.[153] This concept first materialized in technologies such as Second Life, which allowed a user to explore and interact in a virtual world that was created by the individuals that inhabited it.[154] Virtual reality's current inception through devices such as Microsoft's Hololens allows the users to visit virtual spaces as well as real spaces.[155] Additionally, led by the pornography industry, devices are being created that allow for a richer level interactions of individuals in cyberspace.[156] These technologies move beyond an audio/visual experience in cyberspace and allows users to take part in the experience

---

[152] Betz and Stevens, *Cyberspace and the State*, 35.
[153] For instance, *The Lawnmower Man* (1992) was one of the first major treatments of virtual reality in pop culture. In this film, virtual reality is a psychedelic computer rendered space but real interaction occur there. Such a narrative can be traced to the film *The Matrix* (1999), in which the vast bulk of the population exists within a virtual programmed world rendered to mimic the real world.
[154] On Second Life see Lessig, *Code 2.0*, 108-111.
[155] The advertising material for the HoloLens markets the device as a way to connect to others through the ability to be virtually *in* the room with someone else. Microsoft, "HoloLens," https://www.microsoft.com/microsoft-hololens/en-us (last accessed October 6, 2015).
[156] Mandy Stadtmiller, "Virtual Reality Sex Is Coming — and the Toys Are Already Here," *Mashable*, May 29, 2015, http://mashable.com/2015/05/29/virtual-reality-sex/.

portended by AT&T's 1980s ad slogan "Reach Out and Touch Someone."[157] The ability to physically "touch," even through an Internet connected device means that the metaphorical has become the experiential. Physicality is now freely transportable beyond borders, which become much less benign in an example like Stuxnet where code was used to physically and surreptitiously manipulate centrifuges in an Iranian nuclear facility.[158] Cyberspace cannot remove a mountain in between two places, but it can render many of the mountain's effects irrelevant.

The idea of touch leads to a final observation that must be made about Cyberspace: as a space it has inhabitants.[159] Granted these individuals live both in Cyberspace and out. There is developed rhetoric that refers to netizens and cybercitizens, both of which implicate a core concept of citizenship that is traditionally linked directly to territorial authority.[160] Arguably the term "global citizen" found in the literature on global governance can only be conceptualized with a technology that can free the individual from the strictures of their national citizenship.

---

[157] Christopher H. Ramey, "When AT&T Asked Us to 'Reach out and Touch Someone', Did They Mean That Literally?," *Psychology Today*, July 7, 2008, http://www.psychologytoday.com/blog/the-metaphorical-mind/200807/when-att-asked-us-reach-out-and-touch-someone-did-they-mean.

[158] Eric P. Oliver, "Stuxnet: A Case Study in Cyber Warfare," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton: Taylor & Francis, 2013), 127–59.

[159] Post, *Jefferson's Moose,* 31-36 (noting "population" on the Internet) and Lessig, *Code 2.0*, 298 ("Cyberspace is a place. People live there.")

[160] Luke, "The Politics of Digital Inequality," 123.

While such ideas might be dismissed as purely rhetorical, we can see that they indeed do have manifestations such as Estonia's e-Residency campaign, which extends digital rights to registered entities.[161]

Digital natives may be the most potent of these metaphors for inhabitation, as society has not yet to entered a time in which individuals have no concept of what it is like to not be contained within networked space.[162] Digital natives, a naturally rising part of the population, will not conceptualize spatial organization without the inclusion of Cyberspace. Rhetorically, the term digital natives indicates that these individuals are more than just transitory surfers. Their geographic experience will always be networked and machine mediated. In such a world, a digital self existing on the network becomes a normalized human attribute, and the population as a whole becomes respatialized as social constructions of space becomes morphed by networks.

Machine mediated space means that new and different boundaries are experienced based on the architecture of those machines. This is not to imply a dystopian science fiction plot, such as that of *The Matrix*, in which the human conscience only exists within digital bounds. The individual will certainly still exist and move through physical space, but there will be new understanding of the nature of boundaries and borders as individuals recognize an

---

[161] Estonian e-Residency is meant to give digital Estonian personality to individuals who want to start online businesses. As such it is still linked to physical territory, but it represents an important innovation on where individuals are engaging in transactions. e-Estonia, "What is e-Residency?", https://e-estonia.com/e-residents/about/ (last accessed October 6, 2015).

[162] The author was an early adopter of the Internet after cajoling his parents into getting a connection in 1995, but he still remembers using a rotary phone.

"extraordinary possibility for many to participate in the process of building and cultivating a culture that reaches far beyond local boundaries."[163]

As already noted, IoT is indicative of such networked space. IoT allows the networking of devices that can be controlled by electrical current, thus a small computer known as a microcontroller can be used to spin motors, adjust electrical current levels, flip switches, and accomplish a variety of other tasks. Microcontrollers with a network connection allow a user to exert control over physical space through a network connection.

One of the most popular applications of IoT is enabling home automation via the Internet, effectively networking an individual's physical personal space. Transaction points literally proliferate through the space of the home. For instance, lights have traditionally been controlled with a physical switch implicitly requiring a person to move through the physical in order to operate it. IoT, though, ends the "who is turning off the lights" debate that so many couples have by removing the distance to the switch. More striking, it allows the user to turn the lights on or off from a foreign country and even allows an outside party to control the lights. The interior space once defined exclusively by the walls of a room is now open to new forms of control as those walls are breached.[164] The borders physically defined by walls are no longer boundaries to certain types of computer mediated changes in that space. Needless to say this changes the experience and perception of the space of "home" for that user.

---

[163] Lessig, *Free Culture,* 9

[164] It should be noted that the advent of wifi means that traditional copper wire no longer even needs to breach those walls.

* * * * *

This chapter has described the spatial geography of Cyberspace, focusing on both its technical and conceptual landscapes. The spatial orientations that are employed in Cyberspace create strong metaphors that steer social understanding. On of the attributes discussed in this chapter was the dynamism of Cyberspace, and its ability to expand nearly infinitely, making the contemplation of its borders difficult. The next two chapters in Part I will use the concepts of legal geography and political geography in able to better understand the true limits of Cyberspace and define its borders.

Chapter 3

Legal Terrains

One of the striking things about engaging in air travel is labyrinthian airport layouts that create and demarcate a variety of distinct spaces for the traveler. Passengers move through underground passages and shopping mall-esque avenues en route to boarding their airplane. They move from a non-sterile zone to a sterile zone after crossing security borders that demarcate changes in rules. While travelers experience these layouts as minor annoyances, they often fail to recognize how airports are architected to control the travellers within them. Airports by design are divided to demarcate and produce the rules of behaviour within different zones of space. This is not a characteristic unique to airports, as nearly all architecture deploys some sort of control.[165] For instance, architected control is the underlying premise of Jeremy Bentham's Panopticon, but it can be also seen deployed in the layouts of public spaces such as Wal-marts and museums.[166] Architected control can be seen in private spaces as well, as doors and walls are architectural mechanisms that help to maintain privacy. Architecture controls how individuals experience space by enabling and disabling them in a variety of ways, and Cyberspace's open network architecture is no different.

Along these same lines, airports use architecture to segregate international travellers, particularly international arrivals, from the rest of the

---

[165] Lessig, *Code 2.0*, 38-60.
[166] Cohen, "Privac y , V isibilit y , T ransparency , and Exposure," 184.

airport population. International arrivals are ushered into an arrivals halls. These arrivals halls are designed with a series of counters at which sits an authority of the state that checks the passport and documentation of each traveler in that counter's respective line. This line of counters is often marked by signs that informs that these authorities are sitting on the border of the country the plane has landed in. The travellers are usually deep within the interior of the territory of that state, yet they have not entered the state. In this case, the geography of the border is warped to match the legal geography of jurisdiction, creating nearly unmappable zones of exclusion on a map of national borders.

These examples illustrate different sides of the same coin. Legal geographies can be deployed by technologies of enforcement to limit individual ability to transgress the norm being enforced. Additionally, these geographies can also be reimagined to include or exclude space despite the physical location of that territory. The state's ability to dynamically conceptualize its borders in such a way as to create legal fictions within territory renders borders into markers of a legal geography based on jurisdiction.[167] This is why architectures of control are used at borders; they give materiality to imaginary lines. A state's borders are only as solid as the state itself can make them.[168]

---

[167] Bowman notes imagery of "pushing the U.S. border outward" as part of U.S. reconfiguration of jurisdiction at Cargo entry and exit points. Gregory W. Bowman, "Thinking Outside the Border: Homeland Security and the Forward Deployment of the US Border," *Houston Law Review* 44, no. 2 (2007): 1192-95.

[168] Maybe the best classical example is the three mile territorial rule in the law of the sea, which links territorial waters to the control of the state as denoted by the range of a cannon. Carl Schmitt, *The Nomos of the Earth in the International Law of the Jus Publicum Europaeum*, trans. G.L. Ulmen (New York: Telos Press, 2003) 183.

The legal geography of Cyberspace is a question of how architectures of control are deployed within it. The analysis here applies across the layered model established in Chapter 2. First, it will probe the idea of jurisdiction as a type of geography. To do this it will examine the traditional link between territory and jurisdiction. The second section will use the link between architecture and control to examine a fundamental principle of how regulatory power is distributed in Cyberspace through examination of Lessig's principle that "code is law." Finally, this chapter will turn to the idea of code as a constitution of Cyberspace and explore the governance implications that flow from such an idea. The final section will then draw conclusions on the dispersion of jurisdiction in Cyberspace

I. The Space of Law

Jurisdiction is the space of law. It can be understood, in at least one sense, as the literal geographic limitations of the law.[169] As a legal concept, jurisdiction, can seem ephemeral, but it is literally part of the language that often we use to locate ourselves within the world. "I'm from . . . " is a phrase that is probably most often ended with a designation of a legal jurisdiction such as a state or its political subdivisions such as provinces, counties, or municipalities. These subdivisions, which are often nested like matryoshka dolls, each denote space with a particular set legal characteristics. This is what is meant by legal geography. Something to note here is that these nested jurisdictions overlap in such a way that an individual is often standing in a

[169] Kulesza, *International Internet Law*, 2-3 ("The execution of territorial competence is, above all, a territorial phenomenon.")

hierarchical stack of overlapping jurisdictions. It is argued here that Cyberspace also deploys a legal geography of jurisdiction over the individual, but this geography cannot be conceptualized as contained within jurisdiction conceptualized through international space.

As noted in Chapter 2, Cyberspace alters spatial experience. Jurisdiction, in the modern state system, is linked directly to territory. Territory serves as the critical link between jurisdiction and power in a state's deployment of governance, because historically there has been "a general correspondence between borders drawn in physical space . . . and borders drawn in 'law space.'"[170] This is by no means a 'natural' connection, but it has been a *de facto* connection based on technologies through which power is exerted and global order unfolds.[171] Jurisdiction is the that aligns state power with its territorial boundaries.

To this end, international law has recognized five bases from which a state may extend it jurisdiction and thereby exert its power: territorial, personal, protective, passive personality, and universal.[172] Each of these principles for extending jurisdiction have their own internal logic, but all - save

---

[170] Johnson & Post, "Law and Borders," 1368.

[171] Indeed, one of the reasons that Islamic terrorism poses a challenge for international governance systems is its conception of spatial organization in terms of theocratic law, which supersedes spatial organization premised on international law. *See generally*, Bernard Lewis, *The Crisis of Islam: Holy War and Unholy Terror* (Random House LLC, 2004) 8 and Didier Bigo, "The Emergence of a Consensus: Global Terrorism, Global Insecurity, and Global Security.," in *Immigration, Integration, and Security. America and Europe in Comparative Perspective*, ed. Ariane Chebel d'Appollonia and Simon Reich (University of Pittsburgh Press, 2008), 76–94.

[172] Michael Akehurst, "Jurisdiction in International Law," *Brit. YB Int'l L.* 46 (1972): 145 and William A. Schabas, *Genocide in International Law: The Crime of Crimes,* 2d ed. (Cambridge: Cambridge University Press 2009) 409. The author has previously applied these principles to outer space, *see* P. J. Blount, "Jurisdiction in Outer Space: Challenges of Private Individuals in Space," *J. Space L.* 33 (2007): 299.

one - are tied back to physical territory, which embeds territorial understandings into the concept of jurisdiction within international space.[173] So, personal jurisdiction is linked back to a territory via auspices of nationality; protective jurisdiction is linked to protecting the the territory of the state from harm; and passive personality links to the concept of nationality which in turn links to territory. Only universal jurisdiction seems to evade the territorial link, because its original incarnation was as a mechanism to address actors external to the territorial borders of the state, such as pirates.[174] Universal jurisdiction, though, does require that malefactors be brought into the territorial jurisdiction of the state in order for it to exert legal power.[175]

What these accepted principles of jurisdiction exhibit is that territory is foundational to jurisdiction in the international system, and that jurisdiction can be understood as the space in which the state can exert its power, both juridical and through its monopoly on violence.[176] It is important to understand the territorial limitation of state power, because territory sits at the heart of the international legal system. The borders drawn by that system show a particular configuration of jurisdiction superimposed on the space of the world. While "[w]e take for granted a world in which geographical borders . . . are of primary importance in determining legal rights and responsibilities," this configuration

---

[173] Kulesza, *International Internet Law*, 4 (noting the extraterritorial claims to jurisdiction "raises . . . questions fundamental to international law").
[174] Schmitt argues that the high seas sit outside the spatial order of terra firma. Schmitt, *Nomos of the Earth*, 42-44.
[175] See for example the cases of Adolf Eichman, Arendt, *Eichmann in Jerusalem* at 262-263; Augustus Pinochet, Naomi Roht-Arriaza, "The Pinochet Precedent and Universal Jurisdiction," *New England Law Journal* 35, no. 2 (2001): 311–19; and Humberto Álvarez Machaín, Mark S. Zaid, "Military Might versus Sovereign Right: The Kidnapping of Dr. Humberto Alvarez-Machain and the Resulting Fallout," *Hous. J. Int'l L.* 19 (1996): 829.
[176] Kulesza, *International Internet Law*, 6.

is only a static rendering of a dynamic set of lines that indicate a variety of fluid spaces.[177]

The argument advanced by this section is that jurisdiction, understood as a legal geography, is not a continuous nor static space, and that it is reconfigurable not only through a state's own conceptualization of its borders but also through external processes that reshape the nature of legal space. This section will proceed in two parts, both of which are designed to show the gaps in the link between territorial space and regulatory space. First, this section will show how Cyberspace fractures national jurisdiction, and then, it will pursue the same goal in term of international space. It should be noted that the claim made in this section is not that state jurisdictions have wilted away, but that Cyberspace illustrates that jurisdiction is not "already, and forever, 'settled.'"[178] The state retains a great deal of power in relation to objects and individuals within its territory. However, Cyberspace creates a spatial situation in which regulatory power associated with territory runs out, and at this point we can see where Cyberspace's legal geography begins to pick up.

i. National Space

The debate on the nature of Cyberspace typified by the exchange between Post and Goldsmith discussed in Chapter 2, is important in the discussion of legal geography. The debate was centered on whether or not Cyberspace was a new space, but specifically as legal scholars, the dispute centered on whether Cyberspace created new alternative legal geographies of

[177] Johnson & Post, "Law and Borders," 1368.
[178] Post, "Against 'Against Cyberanarchy,'" 1373.

jurisdiction. Such claims had been advanced in Barlow's "Declaration of Independence for Cyberspace." Barlow's claim that states "were not welcome" in Cyberspace, is rooted in the notion of an independent territorial sovereignty as the source of legitimate governance in Cyberspace.[179]

While Goldsmith rejects such rhetoric outright, Post takes a more nuanced position. He claims that "cyberspace *is* somehow different" and that this difference "matters for the purposes of understanding these jurisdictional questions."[180] Post's argument is rooted in the idea that cyberspace creates a world "of inter-connected and geographically complex cause and effects."[181] He notes that

> transactions in cyberspace can take place at much greater physical remove; they are consummated by means of the movement of bits rather than atoms; they are digitally encoded; they are unaffected by the participants' sense of smell; they are embedded in and mediated by computer software; they travel at the speed of light, etc.[182]

Massively distributed computer mediation of transactions, in Posts' view, requires reevaluation of "settled understandings" of concepts such as jurisdiction.[183]

To understand Post's arguments, the critical gaze must again turn to the borders that define the state. Older transborder technology was often controlled by technological standards that were adopted by a given state. This was a unique function of legal jurisdiction that could create architectural

---

[179] Barlow, "Declaration."
[180] Post, "Against 'Against Cyberanarchy,'" 1368.
[181] *Id.* at 1381.
[182] *Id.* at 1375-76.
[183] *Id.* at 1373 ("The world sometimes does that - changes profoundly."). Post does acknowledge that transborder interactions did occur before Cyberspace, but these events occurred "at the margins of the legal system and of sufficient rarity to be cabined off into a small corner of the legal universe." *Id.* at 1383.

controls at the border of a state. So for example, by adopting a different railroad gauge a state could ensure that all train shipments were disembarked and reloaded under the state's watchful eye.[184] Standard setting is tool by which technology is directly regulated.[185] The logical layer of the Internet adopts standards that enforces universal interoperability, meaning that the logical layer bypasses borders by rendering a state's physical telecommunications standards irrelevant.[186] The physical technology of the border is undermined as Cyberspace reroutes border crossings to the applications layers running of the Internet. The proliferation of transaction points, also drives the proliferation of border intersections. For the territorial border, "[d]igitization means dematerialization."[187]

This is not to say that border crossing technologies have not been issues for the international community before. Indeed, radio transmissions[188] and satellite broadcasting[189] both caused debate in the international arena. As Post notes though, the scale of cyberspace is dramatically different from previous technologies.[190] The ability to instantaneously communicate with the entire

---

[184] Mattelart, *Networking the World,* 1-13. Werbach compares US Telecom law in 2005 as "a direct descendent of railroad laws developed in the 19th century." Werbach, "Breaking the Ice," 60.
[185] Standard setting organizations will be addressed more fully in Chapter 7.
[186] Here it should be noted that digital communications still travel on physical networks and that a state can limit such transmissions. Key to the argument, though, is that the physical standards and infrastructure that once effectuated these controls has lessened in its importance.
[187] Luke, "The Politics of Digital Inequality," 125.
[188] Horace B. Robertson, "The Suppression of Pirate Radio Broadcasting: A Test Case of the International System for Control of Activities Outside National Territory," *Law and Contemporary Problems*, 1982, 71–101 and Eppenstein & Aisenberg, "Radio Propaganda."
[189] The Direct Broadcasting Satellite Principles adopted by the UNGA in 1982 were adopted after controversially bypassing the consensus principle used at the UN Committee on the Peaceful Uses of Outer Space (UNCOPUOS). *See* Francis Lyall & Paul B. Larsen, *Space Law: A Treatise* (Ashgate 2009) 256-269 and UNGA, "DBS Principles."
[190] Post, *In Search of Jefferson's Moose*, 60-89.

online population forces new understandings of jurisdiction, since this means that data transmissions cross all borders at once.

The architecture of Cyberspace is such that it forces geographically remote states into direct contact with each other by bringing their borders together. This often means that "multiple noncoordinating jurisdictions" are brought into proximity as the Internet networks those jurisdictions into contact.[191] Cyberspace creates a contact point between and among all networked physical space. This is problematic because laws "mostly concern national spaces."[192] This can be seen in the quintessential *France v. Yahoo!* case.[193] Suit was brought against Yahoo! in France because Yahoo! maintained an auction website that facilitated the sale of Nazi paraphernalia, which is illegal in France.[194] Yahoo! an American company was held culpable in France for the availability of this website within France's territory.[195] Two things should be made clear. First, this website was available to anyone with an Internet connection and a web browser regardless of location. Second, France's legal claim was only that the availability within the territory of France was illegal. If Yahoo! capitulated to the French demand for removal, the

---

[191] Lessig, *Code 2.0*, 300.
[192] Kulesza, *International Internet Law*, 86.
[193] Post, *In Search of Jefferson's Moose,* 164-71; Lessig, *Code 2.0*, 294-97; Kulesza, *International Internet Law*, 107-08. A similar case is the German *CompuServ* case which addressed the availability of pornography via CompuServ services. *See* Kulesza, *International Internet Law*, 106-107 and Lessig, *Code 2.0*, 39.
[194] Kulesza, *International Internet Law*, 107.
[195] At the outset, it should be noted that the technology that led to the *Yahoo!* case predated technology that allowed for geolocation of users through their IP addresses. Kulesza, *International Internet Law*, xiii. Debates on the geographic control of IP addresses persist Leiner et al., "A Brief History of the Internet."; ITU, "Resolution 102 (Rev. Busan, 2014) ITU's Role with Regard to International Public Policy Issues Pertaining to the Internet and the Management of Internet Resources, Including Domain Names and Addresses," 2014 at 148; ITU, "Resolution 133 (Rev. Busan, 2014) Role of Administrations of Member States in the Management of Internationalized (Multilingual Domain Names," 2014 at 183.

website would not be available anywhere in the world, including places where sale of such memorabilia is legal leading to French law and values being enforced globally. Yahoo! sought a declaratory judgement in a United States federal court to render the decision unenforceable, but the 9th Circuit declined to grant the declaratory judgement on the grounds that it did not have jurisdiction over the French entity LICRA.[196]

While the cyberunexceptionalist might argue that this is indicative of courts being perfectly capable of applying law to cases involving cyberspace, the *Yahoo!* case has deeper implications that make such a stance t tenuous. If this transaction were to occur in a pre-Internet environment there are a number of factors that would make it different. First, a French citizen would need to leave France in order to take part in the auction making it a costly endeavor. That citizen would then need to physically transport the item over the French border and negotiate regulatory pressure points applied at border crossings. The Internet on the other hand allows all French citizens to take part in auctions that are "in" the United States in terms of server location. Three things are important here. First, the border crossing is not physical. This means that the state has lost some control over where its border is drawn. Second, the border crossing occurs on a private network. The state's apparatus for controlling borders is located physically at those borders in terms of checkpoints which are public places of inclusion and exclusion. In this case, the "checkpoint" has been routed around and the state has been excluded from its usual control function. Finally, the scale of Yahoo!'s actions are at a much

[196] Yahoo! Inc. v. La Ligue Contre Le Racisme, 433 F. 3d 1199 (9th Cir. 2006).

different level of magnitude, as actions in Cyberspace have a "multi-site effect" fragmenting the idea of the *lex loci*.[197]

Yahoo!'s auction site allowed everyone in France with Internet access to take part in these auctions by minimizing the transaction costs associated with borders. The physical geography pre-Internet stood as a barrier to all but the wealthiest and most dedicated of collectors. Now technology facilitates easy access by all to these auctions. Yahoo! was acting within the jurisdiction of France, yet France lacked the jurisdictional capacity to reach out and physically touch Yahoo! meaning that jurisdiction tapers as France's territory runs out. Before the Internet such interactions were marginal, but post-Internet they are facilitated.[198]

Jurisdiction as a function of territory requires that transactions be located "geographically somewhere in particular," which is "most unsatisfying."[199] The enduring lesson from *Yahoo!* is that state control over persons and property is being diminished as the borders that define that jurisdiction no longer represent a barrier to social transactions.[200] The space of the state runs out as a social space beyond its control opens.

ii. International Space

---

[197] Kulesza, *International Internet Law*, 103. *See also* Spar, "The Public Face of Cyberspace," 345.
[198] Post, "Against 'Against Cyberanarchy,'" 1383.
[199] Johnson & Post, "Law and Borders," 1378.
[200] *See* Kulesza, *International Internet Law*, 14 ("The very fact of rendering certain content available within a certain geographic location cannot widen sovereignty to enable domestic powers to impose their legal regulations on authors of electronic content actually residing in various other states.") and McIntosh & Cates, "Hard Travelin'," at 85 ("Cyberspace "[creates] significant questions in some heretofore fairly understood threshold areas such as geographic location and space.")

Since the scale of transactions on the Internet is global in scope, many scholars have turned to international law as the way in which Cyberspace can be appropriately regulated. This approach is seemingly a natural one, since flows of information in Cyberspace are often transnational in nature, but this too presents several issues, and the dearth of international law addressing Cyberspace is telling.

First, it should be noted that the national is embedded in the international and vice versa. International space is a conceptual extension of national space.[201] The international system itself is made up of states that participate based on principles of nonintervention and sovereign equality.[202] As a result, modern international law is oriented toward the "territorial integrity" of the state itself.[203] International law must be understood to reify the geography of the state by rendering jurisdictional edges as borders of exclusion through the principle of nonintervention.[204] Indeed, until very recently, international law's regulatory focal was the border of the nation state, and only the most marginalized of territories are without legal standing in international law.[205]

States have long debated the control of transborder information flows as a matter of international law. Radio Free Europe and Voice of America are

---

[201] Habermas, *The Postnational Constellation,* 63 ("The territorial principle furthermore, underlies the separation of international relations from the sphere of state sovereignty.")
[202] Christopher Clapham, "Degrees of Statehood," *Review of International Studies* 24, no. 02 (1998): 145 and Michael Walzer, "The Moral Standing of States: A Response to Four Critics," *Philosophy & Public Affairs*, 1980, 212.
[203] UN Charter (1945) Art. 2(4).
[204] Habermas, *The Postnational Constellation,* 64 (. . . the state justifies its sovereignty by its rights to maintain the integrity of mutually recognized borders. ").
[205] Sassen, *Territory, Authority, Rights*, at 54. (" . . . today's interstate system where just about all territory is encased in what are formally considered mutually exclusive states. There are exceptions, but they are few.")

excellent examples of state attempts to penetrate the borders of other states with telecommunications technology.[206] But these interventions were limited in scope as both technology and geography ran out. Radio technology is limited by the ease of jamming as well as geographic constraints on the transmission power of the station.[207] Similarly, satellite technology raised issues resulting in a controversial set of principles adopted by the UN General Assembly.[208] Cyberspace is a new context for these same issues as it gives users "new opportunities for exchanging information and opinions."[209]

This concern with international communications is reflected in the international forum for addressing such issues, the International Telecommunication Union (ITU), which is the "oldest international organization in the world."[210] The ITU is the IO tasked with coordinating international telecommunications with the "object of facilitating peaceful relations, international cooperation among peoples and economic and social development by means of efficient telecommunications services.[211] The ITU has three sectors,[212] each with its own mandate: the Radiocommunication Sector "ensur[es] the rational, equitable, efficient, and economical use of the radio-frequency spectrum"[213]; the Telecommunications Standardization Sector

---

[206] Eppenstein & Aisenberg, "Radio Propaganda."
[207] *Id.* at 154-156.
[208] UNGA, "DBS principles."
[209] Council of the European Union, "EU Human Rights Guidelines on Freedom of Expression Online and Offline," May 12, 2014, at I.D.35.
[210] *See* Codding, "International Telecommunications Union," 501. For other historical IOs *see* Mattelart, *Networking the World,* 6-8.
[211] Constitution of the International Telecommunication Union (2010) at preamble.
[212] The sectors were established at the 1992 Geneva Conference. Codding, "International Telecommunications Union," 508.
[213] ITU Constitution, Art. 12.

which promotes standards that work across national borders[214]; and Telecommunication Development Sector which promotes the development of telecommunications systems in developing countries.[215] Cyberspace, while clearly a technology implicated by ICT, does not fit distinctly within these well defined silos of the ITU. As a result the ITU has had little power to assert any sort of direct governance over cyberspace.[216]

The gap that the ITU cannot fill has also been left empty by other international law making processes. There is a notable dearth of treaty law. The only cyber-oriented, multilateral treaty is the Budapest Convention on Cybercrime, and it is weak at best.[217] The Budapest Convention[218] attempts to set standards on the prevention and prosecution of cybercrime, but it falls short of being a document with any teeth to compel state action. Instead of strong international obligations, the treaty shifts implementation and enforcement burdens to states and extends no jurisdiction by any international entity. By vesting right and obligation in the domestic system of the states, the Convention on Cybercrime reifies the central position of the state, and ignores the vastly different governance dimension that Cyberspace presents. In fact much of the scholarship on international law and Cyberspace seems imply that it is an ineffective mechanism.[219] Sofner et al suggest that cyber war, cyber

---

[214] *Id.* at Art 17
[215] *Id.* at Art 21
[216] Kulesza goes further noting that "it is still difficult to even talk about a common international forum competent" develop law in regards to cyberspace. Kulesza, *International Internet Law*, xiii-xiv.
[217] *Convention on Cybercrime* (entered into force July 1, 2004).
[218] The ITU and Cyberspace is taken up further in Chapter 7.
[219] Kulesza, *International Internet Law*, 29 (noting current regulations "are not sufficient to confront the electronic domain.") and *Id.* at 60 (" . . . developing treaties is time consuming and difficult . . .").

intelligence, content restrictions, human rights, and national security will all remain outside the scope of international agreements.[220] Notably, conflict and human rights are specifically within the scope of international agreements that do not involve cyberspace, which indicates a significant shift in power.

It is precisely the orientation to the national that has rendered international law ill equipped to deal with the global nature of cyberspace, as it uses a "silo-based" "regulatory paradigm" based on physical territory.[221] While scholars have looked to both customary international law[222] and soft law principles such as norms,[223] there is little consensus on how cyber should be treated by nation states. The terrain seems to be frozen in terms of international law making.[224] This is not to say that states could not negotiate a

---

[220] Abraham Sofner, David Clark, and Whitfield Diffie, "Cyber Security and International Agreements," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, ed. Committee on Deterring Cyberattacks: Informing Strategies and Developing Options; National Research Council (Washington, DC: National Academies Press, 2010), http://www.nap.edu/catalog.php?record_id=12997.

[221] Werbach, "Breaking the Ice," 78. It should be noted that the quoted text is conceptually appropriated, as it is used by Werbach to describe U.S. domestic telecommunications regulations. *Id.*

[222] Monika Zalnieriute, "An International Constitutional Moment," 99–133.

[223] *See generally*, Power & Tobin, "Soft Law for the Internet," 31–45; Panayotis A. Yannakogeorgos and Adam B. Lowther, "The Prospects for Cyber Deterrence: American Sponsorship of Global Norms," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton: Taylor & Francis, 2013), 49–77; and Roger Hurwitz, "A New Normal? The Cultivation of Global Norms as Part of a Cybersecurity Strategy," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton: Taylor & Francis, 2013), 233–64. On norms generally, see Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization* 52, no. 04 (1998): 887–917.

[224] Kulesza notes that other transborder issues are "based on frameworks of legal references," but that "[s]uch a mechanism is yet to be developed with respect to the Internet." Kulesza, *International Internet Law*, xiii-xiv and Hurwitz, "A New Normal?," 243. For instance, the council of Europe states that the "obligations of states under international human rights law" apply to Cyberspace communications. Council of the European Union, "EU Human Rights Guidelines," at I.D.36. While this is certainly a progressive perspective, it draws Cyberspace into an international space that has consistently failed to develop consensus as to the content of international human rights laws. Kulesza, *International Internet Law*, 44-45; Habermas, *The Postnational Constellation,* 119; and Daniel Bell, "The East Asian Challenge to Human Rights: Reflections on an East West Dialogue," *Human Rights Quarterly* 18, no. 3 (1996): 641–67.

treaty aimed at governing Cyberspace. They could do just that. The claim, instead, is that states are unable to deliver such a treaty, because they understand their own limitations effectuating control in a sphere marked by severe jurisdictional uncertainty.[225] The non-territoriality of Cyberspace disembowels the notion of jurisdiction as contained international law.[226]

A final distinction must be made. Chapter 2 posits a global location for Cyberspace, and it must be acknowledged that there are areas external to the state that exist within international space and are fully contemplated by international law. A group of areas known as global commons are defined within the bounds of international law, but outside the bounds of the national.[227] The high seas, Antarctica, and outer space are all territories delineated by international law as global in nature.[228] Cyberspace does not fit within this category, because it lacks a key common element with the global commons: Cyberspace is not a *res communis* in the sense contemplated by international law. Global commons share a core legal prohibition against appropriation by a state. Cyberspace though, throughout the layered model, is marked by a dispersion of ownership with some components being owned by

---

[225] One of the reasons scholars have resorted to soft law analyses is because "soft law offers an effective way to deal with uncertainty." Power & Oisín Tobin, "Soft Law for the Internet," 35. On uncertainty, *see generally*, Clark & Landau, "Untangling Attribution," 25; Martin C. Libicki, "Two Maybe Three Cheers for Ambiguity," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton: Taylor & Francis, 2013), 27–34; Lawrence Lessig, *Code 2.0* (Basic Books, 2006), 25; Rose McDermott, "Decision Making Under Uncertainty," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, by Committee on Deterring Cyberattacks: Informing Strategies and Developing Options; National Research Council (Washington, D.C.: National Academies Press, 2010), 227–41, http://www.nap.edu/openbook.php?record_id=12997&page=273.

[226] Kulesza, *International Internet Law*, 15 (" . . . application of the territoriality principle as the primary rule for cyberspace is destined for failure.")

[227] Betz and Stevens argue Cyberspace in terms of global commons. Betz & Stevens, *Cyberspace and the State,* 107.

[228] Kulesza, *International Internet Law*, 20.

states themselves. Cyberspace emerged appropriated and is therefore not a global commons within the legal sense of the word making it difficult to classify within the international system.[229]

II. Codes

The inability of national and international legal space to contain Cyberspace is rooted in the fact that users are "[s]eparated from doctrine tied to territorial borders."[230] In order to articulate a legal geography of Cyberspace, an inquiry into what regulatory mechanisms pick up when the territory of the state runs out must be made. Despite the fact that Cyberspace is sometimes compared to the Wild West[231] implying a degree of lawlessness, there are a number of sources of regulation in Cyberspace that exert control when and where the state cannot.[232]

---

[229] *But see,* Kulesza, *International Internet Law*, 69 (critical Internet resources "ought to be considered Common Heritage of Mankind and governed under international law."). Some commentators have argued that aspects of Cyberspace are global public goods, which is different than a commons which is understood in terms of spatial area. Though similar, the concept of global public goods does not attach to specific body of international law. *See generally,* Joseph E. Stiglitz, "Knowledge as a Global Public Good," in *Global Public Goods: International Cooperation in the 21st Century*, ed. Inge Kaul, Isabelle Grunberg, and Marc Stern (New York, Oxford: Oxford University Press, 1999), 308–25; Sy, "Global Communications for a More Equitable World," 326–43; Spar, "The Public Face of Cyberspace," 344–62; Tambini et al, *Codifying Cyberspace,* 10. This view "remains disputable" since most of the infrastructure is still owned by private and public entities. Kulesza, *International Internet Law*, xii.

[230] Johnson & Post, "Law and Borders," 1367; Kulesza, *International Internet Law*, 124 ("International organizations and states themselves are unable to execute the changes they consider appropriate in borderless cyberspace."); and McIntosh & Cates, "Hard Travelin'," 114 ("Transmissions over computer networks defy current understanding of jurisdictional communities based upon physical geography.")

[231] *See, for instance*, Lynn Mattice, "Taming the '21st Century's Wild West' of Cyberspace?," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton: Taylor & Francis, 2013), 9–12.

[232] Tambini et al, *Codifying Cyberspace,* 5 ("Of course, the Internet has always been regulated.")

As discussed in Chapter 2, Cyberspace has a technical architecture that sets its spatial boundaries and borders which also serve to constrain inhabitants of that space. In the same way that a mountain range can prevent migration, the geography of Cyberspace is such that individuals can be stopped from migrating to certain networks as the result of virtual walls. The major difference - aside from one being virtual and the other existing in "meatspace" - is that Cyberspace is an architected geography.[233]

Cybergeography - i.e. its mountains and valleys and other "natural" attributes - is a manifestation of the code and hardware deployed across the layered conceptual model.[234] To conceptualize how code restricts, consider a simple example of the early arcade game Pong. Pong was a simple game that was released for the Atari game system in 1972.[235] In Pong, two players control blocks on the screen that function as paddles. These paddles are used to hit a dot on the screen, which represents a ball. The paddles that the players use move across a single axis, up and down, on the lateral ends of the screen, and the ball bounces off the top and bottom of the screen. Game play continues until one player misses the dot allowing it to pass the paddle and touch the left or right edge of the screen.

In other, less convoluted terms, Pong is an electronic version of ping pong or table tennis. There is a critical difference, for the purposes at hand,

---

[233] Lessig, *Code 2.0*, 6. ("Code is never found; it is only ever made, and only ever made by us.") Meatspace is a common Internet term use to distinguish real space from cyberspace. The human in terms of "meat" exists in real space; and the human conscience exists in cyberspace.
[234] Tambini et al, *Codifying Cyberspace,* 5 (comparing cyberspace architecture to "gravity and other laws of motion" in real space.) and Michael V. Hayden, "The Future of Things Cyber," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton: Taylor & Francis, 2013), 4 ("Man can actually change his geography").
[235] "About Pong," www.ponggame.org (last visited February 11, 2016).

beyond just the equipment needed for each version: in ping pong a player can break the rules. It is a game with a set of rules, and though those rules constrain the players through threat of penalty, but there is possibility that the players can subvert and violate those rules.[236] In Pong, on the other hand, players are incapable of cheating. Pong's rules are enforced perfectly in the sense that players are compelled to obey them, not through threat of consequences for violation, but through compulsion of the games geography architected by the computer code which sets constraints on the player within the game space.[237] The rules are enforced perfectly, so the player need not be given a rulebook or even notice of the rules to avoid violating them.

This example is used to illustrate Lessig's "code is law" principle.[238] Lessig's principle states that when technology of any sort mediates transactions the code, or architecture, of that technology also regulates the possibilities for those transaction.[239] Regulation embedded into architecture can achieve near perfect enforcement because rules are compressed into the structure.[240] At the heart of Lessig's theory is the concept of regulability. He argues that individuals are "regulated" by a variety of forces including markets, law (in the

---

[236] International Table Tennis Federation, "The Laws of Table Tennis," http://www.ittf.com/ittf_handbook/2016/2016_EN_HBK_CHPT_2.pdf (last visited February 11, 2016).

[237] This simplistic account ignores the possibility of hacking the game and changing the geography of the code, which will be of central importance later in this work. For now however, this possibility will be ignored in order to convey the basic concepts.

[238] Lessig, *Code 2.0*, 5.

[239] *Id.* at 77-78. Code consists of the hardware and software that enable Cyberspace. *Id.* 124; Tambini et al, *Codifying Cyberspace*, 11; Cass R. Sunstein, *Republic. Com 2.0* (Princeton, NJ: Princeton University Press, 2007) at 95. Nor is code is exclusive to Cyberspace. Eppenstein & Aisenberg, "Radio Propaganda," 155-56 (noting a history of technological regulations through changes in radio hardware to limit reception).

[240] Lessig, *Code 2.0*, 110; Beth Simone Noveck, "Designing Deliberative Democracy in Cyberspace: The Role of the Cyber-Lawyer," *BUJ Sci. & Tech. L.* 9 (2003): 7.

formal sense), norms, and architecture or code.[241] Each of these forces exerts limitations on an individual's actions. Lessig posits that in Cyberspace "regulation is imposed primarily by code"[242]

Code regulates Cyberspace because it "defines the terms upon which cyberspace is offered."[243] The code is law principle requires analytic focus to be returned to the layered model wherein we can see the variety architectures through which code is deployed. The layered model reveals specifically that there is code running across the bottom three layers that, combined, influence the user experience at the content level. These layers "are the unacknowledged legislators of cyberspace."[244] A benign example is Netflix, a website that streams movies to subscribing customers.[245] Netflix licenses distribution rights for intellectual property and makes that intellectual property available to view by its customers. Netflix has several core concerns in making its business model operate effectively and profitably. The first is avoiding theft in the sense of nonsubscribers gaining access to the Netflix collection. Netflix does not rely on a notice forbidding non-subscribers from entering the website under force of prosecution. This would plainly be futile. Instead, Netflix uses code at the applications layer that requires a subscriber to verify their identity in the form of a login using a username and password. Netflix discourages widespread sharing of these credentials by deploying code that limits the

---

[241] On the four modalities of regulation, *see* Lessig, *Free Culture,* 123. Lessig uses the concept of "reguability" meaning "that a certain behaviour is capable of being regulated." Lessig, *Code 2.0*, 16. *See also*, Tambini et al, *Codifying Cyberspace,* 11-12.
[242] Lessig, *Code 2.0*, 24.
[243] Lessig, *Code 2.0*, 84.
[244] Greenberg, *This Machine Kills Secrets* , 148 (quoting Nick Mathewson)
[245] http://www.netflix.com.

number of IP addresses (and therefore devices) that can access the collection under through single account at a time. Second, Netflix is concerned with abiding by the terms of the distribution license it has with the owners of the intellectual property it streams. Netflix uses code at the applications layer to make movie files stream to user devices instead of downloading, which keeps Netflix from distributing an unauthorized copy of the file.[246] License agreements are also likely to contain geographic restrictions on distribution. Netflix uses the IP address, which is part of the code of the logical layer, to filter out devices logging in from outside the territory in which the distribution license applies. Finally, Netflix wants its service to work for its subscribers. To do this it analyzes the bandwidth of the subscriber's connection and adjusts the resolution of the display accordingly to ensure smooth streaming. Bandwidth is highly dependent on the architecture of the physical layer through which the subscriber connects to Netflix. Netflix's user experience is shaped by the layered architecture of of Cyberspace. Notably the user likely does not experience these codes as regulations or rules that command compliance. Instead, all of the regulatory mechanisms - save IP filtering, which maps to territorial concerns - are likely experienced as functionality of the service.

Netflix is a benign example, but it highlights one of Lessig's key insights. Coded regulations are hidden in the architecture of the space. This means that regulatory effects are often experienced as functionality rather than limitation, meaning that hidden regulations can be developed and imposed outside of

[246] Streaming technology allows services to send only parts of a media file being actively watched to a user's devices, and it avoids local caching, so that the user's device does not retain the data that is sent.

public scrutiny. Code hides from the user, and there is rarely conversation between the user and the developer as to how code is to function. Indeed, users may not have any notice at all of the rules or how they are being applied. In applications such as Pong and Netflix this can be of little importance to the user, but when considered in terms of a global network that interconnects individuals such hidden rules become problematic as machine mediated interactions proliferate. The code is law principle explains how the regulatory space is shaped, but opens the questions of the sources of code and how code is implemented.

III. Source Code: Software and Softlaw

Law comes from lawmakers. In a liberal democracy, it is, in theory, meant to be very easy to see where law comes from.[247] Transparency in law and regulation is a function of the liberal democratic system of governance. This system implements a standardized process for lawmaking, which creates openness in the public forums that law is made and adjudicated. The standardized procedure allows for individuals to access the law. The coupling of transparency and procedure allows citizens in a liberal democracy are able to peer in and see how the laws that govern them are constructed and applied. This process hinges on legitimacy in the substance of the law being confirmed through the legitimating act of proper procedure. It also opens political space by setting a framework for government action.

---

[247] The law in such systems is in a sense "open access."

Code comes from coders; that is, people who write code. Coders are everywhere. They can be employed by a government, contracted by a private entity, working as a collective for the public good, part of a criminal cartel, or working on their own for simple personal satisfaction. The motivations of coders are non uniform as are their goals. They can be writing code for economic gain or public benefit. The code they release can be proprietary and secret, or it can be open and transparent. Code can be deployed at any of the layers of the layered model. The implication being that there is no standardized procedure for developing code and there is no open and transparent forum in which code as a category of regulation is debated. This is because in Cyberspace code is ubiquitous and non monolithic.

Code, like the Internet itself, is rhizomatic in nature. It develops irregularly across space and time from multivariate, unpredictable sources, and it is deployed dynamically across networks that mediate interactions.. This is a function of the end-to-end network, which has already been demonstrated to facilitate innovation at the edges of the network. Coders working at the applications layer to proliferate transaction points through the development of innovative applications. The open architecture literally allows an individual to change the legal geography of Cyberspace by writing code. For example, the Silk Road, an online marketplace for blackmarket goods was programmed and operated primarily by a single individual.[248] The Silk Road changed the space of the online marketplace by facilitating anonymous transactions making

[248] Bearman, "The Untold Story of Silk Road."

transactions previously burdened by state regulation to take place in an online marketplace.

Code must be understood as dispersed: across layers, across actors, across motivations. At any given time, a user in on the Internet is being regulated by multiple layers of code functioning across the layers of the conceptual stack. Operationalized, the code is law principle means that it is difficult to discern applicable regulations when analyzing user level interactions. There is literally too much code for the user to evaluate, and the user must find ways to extend trust in code without needing to understand all code structuring interactions. Users can do using a variety of ways: user agreements, security certificates, trusted source, etc. What this reveals is that the legal geography of Cyberspace is dispersed across multivariate actors and technologies. The decentralized and distributed nature of Internet architecture, enabled by the logical layer, is the hallmark of its legal geography as well.

The practical result of this dispersion of code is that Cyberspace is embedded with a preference for self-regulation.[249] This result flows from the non-hierarchical architecture, addressed in Chapter 2, that pushes control points rhizomatically through technology and across global geographic space. States have significant power to oversee parts this architecture, but not enough to regulate Cyberspace as a whole, because the decentralized nature of the network gives "all actors . . . an equally strong position in defining its

---

[249] Tambini et al, *Codifying Cyberspace,* ("In the narrow engineering sense, much of the Internet is self-regulated."); Johnson & Post, "Law and Borders," 1388 ("Experience suggests that the community of online users and service providers is up to the task of developing a self-governance system."); Kulesza, *International Internet Law*, 60 (noting that self-regulation is more appropriate than treaty making)

nature."[250] It facilitates multiple entry points for co-regulators to deploy code. So, while states might use a device's IP address to reveal the identity of the individual using that device, Tor browser technology is deployed at the applications level to encrypt and obscure a device's IP address thereby diminishing the reach of state's regulatory power.[251] Self-regulation allows for the dispersion of governance over a complex system, and it "is the laboratory of law and regulation for the Internet."[252] Tor gives the individual the option of choosing rights inconsistent with those defined in the legal geography of the state.

The self-regulatory preference is salient because law has traditionally been an inefficient means of governing rapidly developing technology. Law moves slowly compared to technology, thus law can be slow to react to technological developments, and changes in technology can warp legal terms and entrench outmoded legal provisions.[253] This is one of the reasons that in the modern bureaucratic state lawmakers pass specificity down hierarchically to regulators, whose procedural rules make them more dexterous in rulemaking. These more dextorous means though are still burdened by formal procedure. Self-regulatory mechanisms perform a similar function, but are able

---

[250] Kulesza, *International Internet Law*, 125.
[251] Greenberg, *This Machine Kills Secrets*, 139-143.
[252] Tambini et al, *Codifying Cyberspace,* 4.
[253] For example, Gellman notes that the US Electronic Communications Protection Act is based on "assumptions about technology that are outmoded" and the law now "operate[s] inconsistently." Robert Gellman, "Civil Liberties and Privacy Implications of Policies to Prevent Cyberattacks," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, by Committee on Deterring Cyberattacks: Informing Strategies and Developing Options; National Research Council (Washington, D.C.: National Academies Press, 2010), 273–309, http://www.nap.edu/openbook.php?record_id=12997&page=273.

to implement standards (i.e. regulatory mechanisms) by stripping process to a minimum and focusing on narrowly defined problems.

Cyberspace is big, and its architecture is designed to handle its massive scale.[254] One of the ways that it does this is by dispersing governance across public, private, and civil society networks and devices. As noted, the state holds significant regulatory power over individuals and physical property. But Cyberspace governance is an assemblage, and the state is only one component of that assemblage. Similarly, international institutions such as the ITU and UN, despite their limitations, constitute another component of the assemblage as an expression of consensus, or lack thereof, of the member states. The rest of the assemblage is composed of a variety of actors that work across the Internets layers and exert different degrees of self-regulatory powers. For the purposes at hand, these non-state actors will be divided into three groups: commercial actors, civil society, and the individual. These groups are not discrete, and are chosen as representative points on a spectrum of actors.

i. Commercial Code

Commercial actors have long been considered to wield regulatory power, primarily through market forces. Indeed, Western European empires were built around private companies with the ability to extend regulatory authority through a *lex mercatoria*.[255] This is the sort of regulatory power that sits at the heart of most Marxist critiques. Commercial power has most recently been examined in in the context of neoliberalism and the rise of the multinational

[254] Post, *In Search of Jefferson's Moose,* 60-79.
[255] Burbank & Cooper, *Empires in World History,* 153-162.

corporation (MNC). One of the key lessons from the globalization literature is the embeddedness of the MNC throughout the world, and its ability to skew law and policy through the extension of economic power has been confirmed.[256]

Cyberspace is, of course, no different. Commercial interests pervade three layers of the Internet. Corporations own physical infrastructure; corporations develop software at the applications layer; and corporations own content at the content layer. Only the logical layer is free of corporate ownership and that is because the principle of interoperability requires the logical layer to be open, transparent, and the code free of proprietary claims. Corporations though are invested in the logical layer and are active in Internet Governance Communities (IGCs), discussed below.

Tambini et al show that corporate self regulation happens along industry divisions, and is rooted in the notion "that conventional regulation involving legislative lag and inexpert courts, would be inappropriate and would risk breaking the architectural principles of this new technology."[257] They show that different industry divisions deploy self-regulatory mechanisms to ensure compatibility, user trust, and accountability. These groups use devices such as codes of conduct, industry standards bodies, and interfaces that allow users to report norms violations in order to ensure compliance with the law as well as user satisfaction.[258] Self-regulatory activities by corporations are subject to the

---

[256] The actions of the oil industry to the Ogoni people of Nigeria serves as a salient example. *See* Ken Saro-Wiwa, "On Environmental Rights of the Ogoni People in Nigeria (1995)" in Micheline Ishay, *The Human Rights Reader: Major Political Writings, Essays, Speeches, and Documents from the Bible to the Present* (Routledge, 2007) 360-363.

[257] Tambini et al, *Codifying Cyberspace,* 30 and Jayakar, "Globalization and the Legitimacy," 726-29.

[258] *See generally*, Tambini et al, *Codifying Cyberspace.*

same critiques as self-regulatory bodies in other commercial areas. Questions of democratic deficits, the reification of power structures based on concentration of capital, and legitimacy are all raised for obvious reasons.[259] In Cyberspace, as Tambini et al observe, one of the central problems is that commercial bodies maintain control over information and how it flows, meaning that private interests become the arbiters of the "freedom of expression" as found in a variety of human rights documents.[260] Importantly, corporations that exist in the global space of Cyberspace at a sufficient scale become the arbiter of this right across global spaces not linked to territorial jurisdictional limitations.

A second analytical problem caused by corporate self regulation is that there are numerous different types of corporate actors. Phrases like "corporate interests" and "commercial interests" often indicate a unitary set of interests, but no such unitary interests can be identified for the 'Internet industry.' Self-regulation by commercial actors is architecturally dispersed across the layered model, and dependent on where a corporation functions within the layered model. Commercial actors innovating at the applications layer have an interest in maintaining open, end-to-end data transfers in the logical layer. This means that commercial interests owning physical infrastructure, like backbones and ICT networks are, due to market forces, required to maintain bandwidth sufficient to pass along the data required by the applications layer.

---

[259] *Id.* at 112.

[260] For instance, UN General Assembly, Res. 217 A(III). Universal Declaration of Human Rights, (December 10, 1948) at Arts. 18 & 19; International Covenant on Civil and Political Rights (entered into force Mar. 23, 1976) Art. 19; European Convention on Human Rights (entered into for June 1, 2010) Art. 10; and American Convention on Human Rights (entered into force July 18, 1978) Art. 13, among others.

The mismatch of interests, between content and bandwidth, can be seen in the net neutrality debate taking place in the US and Europe. The rise of streaming applications, such as Netflix, led to a steep rise in bandwidth requirements at the backbone level.[261] Due to the nature of agreements that arrange peering between backbones, the commercial owners were experiencing costs associated with increased bandwidth. The natural commercial solution to this problem is to pass those costs along to the entities using the bandwidth. ISPs in turn want to pass those costs on to users. From a commercial perspective this is exactly how a market economy works, but this means that the ISP is also incentivized to give preference to some types of bandwidth usage.[262] As a result, an ISP and an Internet Content Provider (ICP) might enter into a contract that gives that ICP's content a priority to bandwidth or even excludes bandwidth traffic from a competitor. This could prove to be a viable profit stream to an ISP as well as potentially fatal to an ICP that lacks sufficient market power. ICPs interest in providing content implicates free expression issues as well as the innovative architecture of the Internet itself. If the end-to-end architecture fails to connect ends, then the space created by the technological landscape is dramatically changed. The point here is not necessarily to discuss the merits of net neutrality, but to show how corporate interests at different points in the

---

[261] Osgood, "Net Neutrality and the FCC Hack," at 33-34 and Verizon v. FCC, at 5-6.

[262] Rick Osgood, "Net Neutrality and the FCC Hack," in *Hackaday Omnibus 2014*, ed. Mike Szczys, 2014 at 34; Verizon v. FCC, 740 F. 3d 623 SLIP (Court of Appeals, Dist. of Columbia Circuit 2014) at 6. *See also* Debora L. Spar, "The Public Face of Cyberspace," in *Global Public Goods: International Cooperation in the 21st Century*, ed. Inge Kaul, Isabelle Grunberg, and Marc Stern (New York, Oxford: Oxford University Press, 1999) at 352; Damian Tambini, Danilo Leonardi, and Christopher T. Marsden, *Codifying Cyberspace: Communications Self-Regulation in the Age of Internet Convergence* (Routledge, 2008) at 8-9; Kevin Werbach, "Breaking the Ice: Rethinking Telecommunications Law for the Digital Age," *J. on Telecomm. & High Tech. L.* 4 (2005): 78-9; Vera Ranieri, "EFFecting Digital Freedom," *2600: The Hacker Quarterly*, v. 31/4, 2014-2015, 52-53..

stack of layers diverge. Net neutrality shows how a simple supply and demand issue at the physical layer permutates across the other Internet layers and reveals deep governance issues concerning the nature of the network and core human rights.

The net neutrality example reveals divergence of corporate interests, but it also reveals a convergence as well, namely that as technologies converge, corporations often merge. Many ICPs are not owners of the intellectual property rights in the content that they provide.[263] The control of intellectual property has been key contestation in Cyberspace and has a pedigree that includes ICPs such as Napster and Pirate Bay. Successful ICPs such as YouTube, push content controls to users which has been a thorn in the side of content owners who want to be the sole arbiters of that property.[264] Net neutrality serves as a reminder that companies, such as Time Warner, are both content owners and ISPs.[265] Such corporate convergence without net neutrality would allow these companies to constrain ICPs from both directions in the layer stack. Such corporate convergence can create new sources of regulatory power as diversified companies seek to leverage different mechanisms to maximize profitability and filter out the competition.[266]

---

[263] Rick Osgood, "Net Neutrality and the FCC Hack," in *Hackaday Omnibus 2014*, ed. Mike Szczys, 2014 at 35.
[264] Notice and take down
[265] Such concerns were brought to light during the failed merger of Time-Warner and Comcast, *see* Hilary Stout, "Comcast-Time Warner Cable Deal's Collapse Leaves Frustrated Customers Out in the Cold," *The New York Times,* April 26, 2015, http://www.nytimes.com/2015/04/27/business/media/mergers-collapse-leaves-frustrated-cable-customers-out-in-the-cold.html. *See also*, kliq, "Xfinite Absurdity: True Confessions of a Former Comcast Tech Support Agent," *2600: The Hacker Quarterly*, 31/3, 2014, 51.
[266] These issues will be revisited in Chapter 7.

ii. Public Code

Public spaces are coded. As an example, Lessig cites the American with Disabilities Act, a law that recoded public space in order to increase access.[267] Similarly, newly constructed public and private places must be built "to code." Building codes ensure a number of different things: they ensure compatibility between structures and public utilities such as the electrical grid; they ensure safety by describing construction techniques that will give the building the required structural integrity, and these codes also enforce certain types of space. Helen, GA is an example. Helen, GA is a small tourist town in the Appalachian Mountains in Northeast Georgia. It has all the amenities of a vintage tourist town from an age when road trips were forced down windy highways. Its has restaurants, including fast food chains, mini-golf, wine shops serving local rotgut, and motels for weary travellers. Popular with bikers on long mountain drives and summer camp field trips to "tube the Hooch," Helen sounds like numerous other outposts across Appalachia, but Helen looks different. Specifically, Helen looks like a Bavarian village lifted out of Germany - even the McDonalds conforms to the aesthetic (see Fig. 2.1).[268] Helen uses its building code to transform itself into a particular type of public space, which is designed to structure an economic space built around tourism. The building code enforces architectural predictability in both the public space and the private commercial space.

---

[267] Lessig, *Code 2.0*, 127.

[268] More precisely Helen looks like a Bavarian Village taken out of Germany, transplanted into Destin Beach, Florida for several years, and the transplanted into the Appalachian Mountains. In other words, German charm and airbrushed t-shirts.

Fig. 3.1: Helen, GA is a quintessential Bavarian village in the Appalachian Mountains

ISPs and ICPs own and operate networks on the network of networks. To extend the 'information superhighway' metaphor, these are the private spaces that you see as you drive along the highway.[269] They consist of businesses with their doors open to the public, and businesses that are closed to all but those authorized to enter. Additionally, there are mom and pop stands, yard sales, and other roadside attractions. There are also private residences which remain closed to the public, and churches that are open to all. As you drive, though, you are in public space. You are on a road, that is maintained by a public authority for the public good, but this authority is not a government authority enforcing local zoning standards.

[269] *But see* Streck who argues that the information highway metaphor is reduces cyberspace to a "single, homogenous experience." John Streck, "Pulling the Plug on Electronic Town Meetings," 27.

Public space on the Internet is most visible at both the logical layer and the applications layer.[270] These layers are where interaction points proliferate, but those interaction points must be architected. This has led to an interesting assortment of entities that maintain this public space through standardization procedures that are meant to ensure many of the same things building codes accomplish, namely interoperability, stability, and maintenance of the public space. Standardization is the means through which these entities work to structure the parameters of online interactions, because standardization makes architecture predictable.

Standard setting bodies are by no means an innovation. Government and commercial standards settings bodies have always been a feature of market economies. Government interests in setting such standards is in the maintenance of public space. While commercial interests are often vocal in the standards adoption process, they can be met with skepticism when they become the arbiters of rights within the public space. As already established, states only have partial control of the public space of the Internet, so as the state's territory runs out, a different type of self-regulatory body has stepped in: Internet Governance Communities (IGCs).[271] These governance bodies are self-regulatory in nature, and are marked by various levels of open membership that allows anyone with an interest and sufficient technical skill to take part in their deliberations. IGCs have grown organically with the development of

---

[270] Openness can be observed at the physical layer as well, such as in the right to broadband access in Finland. "Finland Makes Broadband a 'Legal Right,'" *BBC News*, accessed December 2, 2015, http://www.bbc.com/news/10461048.

[271] IGCs is used to delineate these from IOs and to denote them as a distinct type of NGO (to the degree that they fit the definition of NGO).

Internet technology, and they constitute a community in which standard technical structures are negotiated.[272] Unlike the ITU which has been unable to extend its regulatory power over Internet protocols, IGCs routinely adopt standards that affect functionality across all layers of the Internet. IGCs will be central component to the analysis found in Chapter 7, but two brief examples are offered here as illustrations.

The heart of the protocol stack, the logical layer creates a public space through its open code. It facilitates the digital handshake between devices on the Internet; the standards allow entities to set up shop on the information superhighway. The standards that facilitate such interoperability must be open, nonproprietary, and accessible, and they must work well enough to ensure wide adoption which facilitates architectural predictability.[273] These standards are developed by the IETF. The Internet Engineering Task Force was established by the researchers that were architecting the Internet, and "probably has the largest influence on the technologies used to build the Internet" despite it lack of "formal authority."[274] Originally, a group of computer scientists hailing from universities and making contributions to the early network architecture, the IETF now allows anyone to join and take part in

---

[272] Leiner et al trace the historical development of these communities. They situate the community unit as core to these entities: "The Internet is as much a collection of communities as a collection of technologies and its success is largely attributable to both satisfying basic community needs as well as utilizing the community in an effective way to push infrastructure forward." Leiner et al., "A Brief History of the Internet."

[273] The idea of transparency in the code is comparable to Rawls' assertion that the "publicity of the rules of an institution insures those engaged in it know what limitations on conduct to expect of one another and what kind of action is permissible." Rawls, *A Theory of Justice*, 56.

[274] Harald Alvestrand and Hakon Wium Lie, "Development of Core Internet Standards: The Work of IETF and W3C," in *Internet Governance: Infrastructure and Institutions*, ed. Lee A. Bygrave and Jon Bing (Oxford: Oxford University Press, 2009), 126.

deliberations on its non-binding standards.[275] Though non-binding, these standards are adopted under a decision procedure that emphasizes "rough consensus and running code," a deliberative stance that values agreement and functionality equally.[276] The IETF places great emphasis on transparency in decision making, and it's essential "read me" document states explicitly a rejection of "kings and tyrants."[277]

A second example is the W3C. The innovation enabled at the logical layer means that other public spaces can be opened in Cyberspace through the use of the applications layer. As examined before, WWW is an applications layer code, and its basic language is HTML. Specifically, HTML enables the concept of hypertext, which allows connections to be made among digital documents, a function commonly called linking.[278] Hypertext is quite literally why Cyberspace is often characterized as a vast repository of information. In order to facilitate such hypertext linking, HTML needs to be standardized and open.[279] The World Wide Web Consortium (W3C) is the standards setting body that ensures the publicness of the WWW.[280] W3C describes itself not as an organization but as an "international community that develops open standards to ensure the long-term growth of the Web."[281] It too has open membership

---

[275] *Id.* at 129.
[276] Internet Engineering Task Force, "The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force" (2012) at https://www.ietf.org/tao.html.
[277] *Id.*
[278] Hypertext was first theorized by Vannever Bush. Brate, *Technomanifestos,* 33-52. WWW is not the only hypertext network, Xanadu was developed by Ted Nelson, but did not succeed. Brate notes Nelson's political ideology as "humanistic libertarianism." *Id.* at 220-225.
[279] Note here that it is HTML and not the browser itself that is the public space. The browser is a separate application that accesses the public space and is often proprietary.
[280] Alvestrand & Lie, "Development of Core Internet Standards," 138-139.
[281] World Wide Web Consortium, "About W3C," https://www.w3.org/Consortium/ (last visited Feb. 11, 2016).

allowing both organizations and individuals to join, and its decisions are taken by "community consensus."[282]

Both of these examples exhibit key characteristics that make IGCs difficult to characterize in organizational terms, making their evolution as a governance mechanism significant to understanding the legal geography of Cyberspace. First, IGCs are a reflection of the distributed, open nature of Internet architecture. Their open membership schemes potentially distribute of decision making globally, and their process is open in order to ensure goals of interoperability.[283] Second, as communities, rather than organizations their decisions impose community values into architectural design. In IGCs, the public, as a collective, creates and maintains the code of public space.

iii. Personal Code

The end-to-end network reduces barriers to innovation as does open code at the logical level. These innovative edges open up spaces in which individuals can act at a global level and change the nature of interactions in cyberspace at the applications level. Both PGP and the Silk Road, discussed above, are examples of coders rewriting state regulatory power. These application layer codes inscribe new rules on the state's ability to control information using cryptographic technologies, or as one commentator claims, the user is empowered to "[c]reate the digital world, and with it, [one's] own

---

[282] *Id.*

[283] *See* Lessig, *Code 2.0*, 148 ("What makes a system open is a commitment among its developers to keep its core code public - to keep the hood of the car unlocked.")

rules."[284] The individual is given direct access to implementing innovations that can reconstruct the legal geography the user inhabits. The implication that the individual can directly regulate in Cyberspace is controversial, at best, and many would outright reject such a notion. Alternate readings would likely suggest that the code deployed by these individuals will be the subject of criminal or commercial law. Such readings inscribe national jurisdiction around the individual as the subject of the law.

Such stances are rooted in territory and overlook is the way in which these technologies re-architect legal geography. Applications can extend to individual an ability to be the arbiter of their own rights in terms of informational freedoms, which are usually umbrellaed under the freedom of expression. They are an "arbiter" in the sense that they can effectively hide personal interactions and remove them from the legal geography of territory. The logical layer allows applications layer code to bypass the state jurisdiction. The user respatializes to a legal geography that exist outside of the state's territorial gaze. The user as coder chooses the values contained in the code that he or she writes. This means that some may use these technologies to assert a freedom of political expression, but others can imbue the right with more nefarious content such as child pornography or terrorism. Such uses will be the subject of Chapter 8.

Wikileaks serves as a good example.[285] Wikileaks is more than just a webpage. It is applications level code that allows for an individual to send

---

[284] Greenberg, *This Machine Kills Secrets* , 148.
[285] www.wikileaks.org (last visited Feb. 11, 2016)

information to Wikileaks while preserving anonymity.[286] Developed and deployed by Julian Assange with the help of a handful of other programmers, Wikileaks became a global actor after it published a number of prominent leaks. This media attention peaked with the publication of thousands of State Department cables leaked by Chelsea Manning.[287] Two things are important here, first Julian Assange's purposes for developing Wikileaks specifically invoke changes in world order and re-empowerment of the individual.[288] Wikileaks is "a platform, a tool, an instance of technology," but it has an explicit legal purpose of diminishing the State's enforcement jurisdiction by reducing "incalculable legal costs" by transporting leakers to a new legal geography.[289]

The second thing to note is the power of the code. Cablegate leaker, Manning was not caught as a result of the state following his digital trail. Instead, Manning revealed himself to a fellow coder, Adrian Lamo, who turned him in. Until that point, the United States had no evidence against Manning. Manning's own revelations returned his act to the interior of the the legal geography of the state. Only when Manning spoke the crime did it materialize in a territorial sense.

* * * * *

The legal landscape of Cyberspace, as described above, is a multidimensional geography that can rewrite the jurisdictional patterns

---

[286] *See generally*, Domscheit-Berg, *Inside Wikileaks*.
[287] *Id.*
[288] *See*, Domscheit-Berg, *Inside Wikileaks ,* 160 (quoting Julian Assange as stating "I'm off to end a war" in relation to the Collateral Murder leak from the U.S. occupation of Iraq.)
[289] *Id.* at 174-75, 137

established as accepted in international governance.. Multidimensionality is the result of the dual geography implicit in the layered architecture of the Internet. This reveals why the layered model carries force as an explanatory tool: through dissection of the network architecture, interconnected points of control can be identified and observed. The layered model facilitates "layered thinking," which can reveal how the spatial characteristics of Cyberspace can ripple across the conceptual stack and changes the lines of other geographies as has been shown in relation to the legal geography addressed above.[290]

The airport analogy that opened this chapter took us to an international frontier found in an airport's international arrivals hall. There is another aspect of this room that should be noted before moving to the final chapter in Part I. If you listen while in the arrivals hall, you can hear the muffled, a-rhythmic beat of stamps hitting passports. As observed above, jurisdiction, or legal geography, is usually mapped across space using state territorial borders as indicators. These borders represent another notion as well. In the airport arrivals hall, the border is as much about territory and law as it is about individual identity. The border is an expression of political identity, and passports are opened in order to check political identity. The next chapter will take up this notion through examination of political geography.

---

[290] Werbach, "Breaking the Ice," 69.

Chapter 4

Political Places

In *Midnight's Children,* Salman Rushdie interweaves his signature magical realism into the political geography of India surrounding the specific time, 12:00am August 15, 1947, that India came into existence as a nation state.[291] Rushdie identifies this moment of national political identity as inseparably linked to individual identity. In one of the many turns of the novel, the reader is presented with the sale of Methwold's Estate. In the story, William Methwold sells his estate to an Indian family with the contractual stipulation that the family must continue to live exactly as the English inhabitants before them had until the moment of Indian independence at which point the family could again live as Indians. The fictional contract imposes an English (read colonial/imperial/Western) geography over the estate being sold. The contract extends a political identity as well, the contract defines the identity of the inhabitants concurrently with the state's political borders. The family lacked the possibility to live as and be Indian until the stroke of midnight, because until that point there was no such place to bound such an identity. Borders are what Kamal Sadiq, borrowing Rushdie's phrase, calls "midnight's children." Decolonization led to "[n]ew borders," and "paths that were legal and customary became illegal overnight" forcing, through both inclusion and exclusion, new identities on the local inhabitants as the result of international

[291] Salman Rushdie, *Midnight's Children* (New York: Random House 2006).

geopolitical shifts.[292] In Rushdie's tale law enforces political identity congruent with state geography. At midnight, though, everything changes.

In this example, we can see that the law (i.e. the contract) is the expression of political identity across a territory, rendering a condition in which "[l]ocation equals identity."[293] Rushdie illustrates that an individual's location is a construct that can change without physical movement. In other words, the "space changes . . . meaning."[294] Political space is the space in which negotiations about how social rights and obligations will be allocated among the governed and the government. This negotiation itself gives identity to the participants in terms of membership, which legitimates their role in such negotiations. International borders, therefore, are expressions of legal geography mapped onto spatial geography through an expression of a political geography bounded by common community.[295] As a result, legal arguments "presuppose spatial knowledge," and human rights actions are "struggles for spatial normativity."[296] These values structure public space in which discourse and deliberation take place. Of course, such uniform identification of

---

[292] Kamal Sadiq, *Paper Citizens: How Illegal Immigrants Acquire Citizenship in Developing Countries* (Oxford: Oxford University Press 2010) 39. *See also*, Cooper, "What Is the Concept of Globalization Good For?," 206 ("To study colonization *is* to study the recognition of space, the forging and unforging of linkages . . .").

[293] Andy Greenberg, *This Machine Kills Secrets*, 141; see also, Clark & Landau, "Untangling Attribution," 25. Liste notes that

[294] Lessig, *Code 2.0*, 87.

[295] Coicaud, *Legitimacy and Politics,* 12 ("As the guarantors of the public space, political institutions are at once the instrument and expression of rights."). *See also* Streck, "Pulling the Plug on Electronic Town Meetings," 39. (". . . identity in cyberspace is cumulative . . . ")

[296] Philip Liste, "Transnational Human Rights Litigation and Territorialised Knowledge: Kiobel and the 'Politics of Space,'" *Transnational Legal Theory* 5, no. 1 (2014): 1–19.

individuals with political values compartmentalized by borders is a mythical construction, but it is the construction that underlies international space.[297]

Thus far in this research, Cyberspace has been described in terms of its spatial and legal geography. Legal space is not *sui generis*; it has origin and history. Specifically, law is the product of negotiations that occur within the constructed public space of the state. Law is a mechanism used to articulate the parameters of public space as a reflection of the values negotiated by the political membership of the space.[298] At the heart of the concept of legal jurisdiction are "fundamental questions of order and legitimacy," which describe the political geography.[299] This chapter turns its attention to the project of identifying how values that shape the political geography of Cyberspace through its code and architecture. If code is law then the coder made political "[c]hoices among values, choices about regulation, about control, choices about the definition of spaces of freedom."[300] This section argues that there are underlying values that organize Cyberspace as well as guide and legitimate power distribution in the governance of Cyberspace. First, this

---

[297] *For instance, see* James Ferguson's account of the Web Magazine *Chrysalis* which attempted to construct the idea of Zambianess into the political container drawn by imperial powers and titled Zambia. Ferguson's account shows that the author's felt compelled to link identity to the territorial imposition of political space. James Ferguson, *Global Shadows: Africa in the Neoliberal Global Order* (Durham: Duke University Press, 2006) 113-154. *See also,* Christopher Clapham, "Degrees of Statehood," 154 ("This claim to representation has been accepted under the rules of sovereignty, no matter how bitterly it has been contested by many of those citizens themselves."); Walzer, "The Moral Standing of States," 214 ("Hence states can be presumptively legitimate in international society and actually illegitimate at home."); and Armand Mattelart, *Networking the World,* 1 ("International communication emerged with modern nationalism which established the territory as the basis of sovereignty and of an imaginary community.").

[298] Coicaud, *Legitimacy and Politics,* 83. (" . . . rules of conduct are indissociable from a historical context wherein the economic, social, and cultural aspects - to cite only those ones - combine with power-related phenomena to produce a specific type of society.")

[299] Post, "Against 'Against Cyberanarchy,'" 1387.

[300] Lessig, *Code 2.0*, 78.

chapter will build a framework for understanding how constitutional values structure public space and legitimate action therein. Then, it will analyze how constitutional values were implemented into the open network architecture through a historical analysis of its design code across the technical layers of the Internet. The final section will then reflect on the value of interoperability and argue that it is the core organizing logic for the political geography of Cyberspace.

I. Code and Constitution

At the heart of modern governance is the idea of the constitution. Constitutions are legal documents that are foundational in scope. They serve as the blueprints for the construction of public space, and are distinct from the legal geography they deploy.[301] Effective constitutions organize and distribute power among the actors within a governance space in such a way that a tenable imbalance of power is created between citizen and state.[302] So for instance, Sajo argues that constitutions embody shared emotions and values of the political community that it organizes,[303] and as such, constitutions can be seen to organize the "communicative conditions for a reasonable political will

---

[301] Rawls refers to the "political constitution" as a "major institution" in the "structure of society." Rawls, *A Theory of Justice*, 7. *See also*, Habermas, *The Postnational Constellation,* 116. ("This idea of constitution-making practice links expression of popular sovereignty with the creation of a system of rights.") and Noveck, "Designing Deliberative Democracy in Cyberspace," 11 (". . . value choices turn in to design choices . . . ").

[302] Rawls, *A Theory of Justice*, 28 (". . .basic liberties are taken for granted and the rights secured are not subject to political bargaining or the the calculus of social interests.") and Ian Clark, *Legitimacy in International Society* (Oxford University Press, 2005) 19 (Constitutions create "expectations . . . about forms of political conduct").

[303] *See generally*, András Sajó, *Constitutional Sentiments* (New Haven [Conn.]: Yale University Press, 2011).

formation."[304] These value laden "communicative conditions" are a political geography that structures public discourse and deliberation. The flow of information and boundaries to its flow are connected build the "public sphere" within which political identity is formed.[305] Constitutions set the limits of jurisdiction, meaning that they extend communicative conditions across space, and demarcate the limits of community as defined by values embedded through founding political practices.[306] The constitution shapes the political geography in which "the process by which we reason about how things ought to be" takes place[307]

Political geography can be observed in the communicative conditions deployed by code. Code when observed in the layered model constitutes both the spatial geography of Cyberspace (i.e. its architecture) and the legal geography of Cyberspace (i.e. its architecture). This compression is important. In physical space law and politics are extended over and thus compressed with territory. In Cyberspace, space is extended by code, and code is law. It should be no surprise then that code imposes communicative conditions as well, which require probing the extent to which code functions as a constitutional force. In return this will reveal how values are architected directly into Cyberspace. Code is of course not the same as a formal constitution, but code does perform

---

[304] Habermas, *The Postnational Constellation,* 117.
[305] *See generally*, Douglas Kellner, "Intellectuals, the New Public Sphere, and Technopolitics," 147–86; Noveck, "Designing Deliberative Democracy in Cyberspace," 11; Clinton, "Internet Rights and Wrongs"; and Jayakar, "Globalization and the Legitimacy of International Telecommunications Standard-Setting Organizations," 713.
[306] See for example, Alfred North Whitehead, *Science and the Modern World* (Simon and Schuster, 1967), 13 ("Law is both the engine for government, and a condition restraining government.").
[307] Lessig, *Code 2.0*, 78.

many of the same functions as a constitution, which makes the analogy tenable.[308]

The concept of legitimacy will be helpful in articulating the constitutional values that define a political geography. Legitimacy addresses the "justification of power" within a governance structure, and is a "fundamental problem of politics."[309] It is a measure of the distribution of power that "concerns first and foremost the right to govern."[310] The right to govern is defined through a network of social values, laws, and founding principles that together define the critical "division that separates those individuals who command from those who obey."[311] In other words, legitimacy is articulated and observed at points that structure the division of power among entities that *govern* and entities that are *governed*.[312] Societies use constitutionally constructed political institutions "to settle conflicts that threaten the cohesiveness of the community."[313] These institutions are the "guarantors of the public space" in which communicative conditions foster a "network of sociability."[314] Constitutions construct a political geography by bounding "exchanges to unfold in a fixed framework and under the form of

---

[308] The relationship between code and constitutions is not foreign to the literature. *See, for example*, Lawrence Lessig, *Code 2.0* (Basic Books, 2006), 6-7, 275, 314 and C. Dianne Martin, "Using the US Constitution to Frame the Governance of Cyberspace," *ACM Inroads* 6, no. 1 (2015): 24–26.
[309] Martin Wight, *International Theory: The Three Traditions* (Holmes & Meier for the Royal Institute of International Affairs, 1992), 99.
[310] Coicaud, *Legitimacy and Politics,* 10.
[311] *Id.* at 26. (the "signification of the right to govern is connected in the first place with this division")
[312] *Id.* at 10.
[313] *Id.* at 21.
[314] *Id.* at 11.

reciprocity" that "tangl[es] together . . . rights and duties."[315] The constitution expresses what it means to be a member of of a political space by expressing the bounds of that space in terms of rights and obligations in an "unequal distribution of power."[316] The rights and obligations themselves, often expressed through law, institutionalize shared values of the community.[317]

Legitimacy, then, is fluid across space and time,[318] but actors within a given political community will often invoke foundational or constitutional values in order to legitimate contemporary actions by framing them in the communicative conditions.[319] Constitutional values shape "rules of conduct [that] are indissociable from a historical context."[320] Legitimacy is not a universal norm, so each political geography must be examined in the context "of social facts is set within the ongoing flow of history."[321] Legitimacy, as the link between the power and values, is an analytic for examining the political geography deployed by code in Cyberspace.[322]

II. Code is Politics

---

[315] *Id.*

[316] *Id.* at 31. The idea of imbalanced power should not be confused with raw, *de facto* power with also leads to imbalanced governance mechanisms. Instead using "legitimacy" to describe such power distribution assumes that consent plays a major role." *Id.* at 10

[317] *Id.* at 32; Lessig refers to these as "framing values." Lessig, *Code 2.0*, 316.

[318] Coicaud, *Legitimacy and Politics,* 207-08 (depicting society as a "field of possibilities.") and Power & Tobin, "Soft Law for the Internet," 39 (Legitimacy as dependent on the "context or society").

[319] Coicaud, *Legitimacy and Politics,* 23 (". . . the institutions that lay down and make the law must establish it in terms of the fundamental values of [a] group."); Clark, *Legitimacy in International Society*, 2 (actors are "engaged in endless strategies of *legitimation* in order to present certain activities or actions as *legitimate*").

[320] Coicaud, *Legitimacy and Politics,* 83.

[321] *Id.* at 192; Clark, *Legitimacy in International Society*, at 13.

[322] Tambini et al., *Codifying Cyberspace,* 13 ("The architectures of cyberspace are causing such re-examination of regulation and legitimacy.");Clark calls this "political terrain." *Id.* at 3.

Technology as it progresses through its technical life span, from development to operations, it is laden with politics.[323] Technology, which is often advertised as of the future, is always a product of history.[324] As a result, design decisions made in early stages of development entrench design values in a technology, and such decisions are often influenced by politics.[325] Cyberspace is no different, and this section will use history of its development as a tool to reveal foundational values embedded in its architecture that shape its political geography.[326]

This historical inquiry focuses on the source of code: coders. As with any discussion of values, the ability to articulate them with specificity that also applies with generality is limited.[327] This section will examine the political values that the coders designed into Cyberspace. In the same way that an American constitutional lawyer might consult the *Federalist Papers* to discern the values of the constitutional designers, this section will examine how these coders articulated the the values they held into the code they designed.

i. Making Space

---

[323] In Lessig's words, "architecture is politics." Lawrence Lessig, *Code 2.0*, 24.
[324] Coicaud, *Legitimacy and Politics,* 199 ("The rootedness of the study of social phenomena in its historical setting is irrepressible.")
[325] Kenneth R. Fleischmann et al., "Thematic Analysis of Words That Invoke Values in the Net Neutrality Debate," March 15, 2015, https://www.ideals.illinois.edu/handle/2142/73433 at 1 ("Values are tightly connected to how people use technology").
[326] Walzer, "The Moral Standing of States," 211 ("The moral understanding on which the community is founded takes shape over a long period of time."). *See also* fRonnie D. Lipschutz, "Environmental History, Political Economy and Change: Frameworks and Tools for Research and Analysis," *Global Environmental Politics* 1, no. 3 (2001): 72–91, 73 ("In other words, to understand, imagine and shape landscapes in the future, we need to know how they were created in the past.").
[327] Coicaud, *Legitimacy and Politics,* 138 ("The dimension of values is stubbornly resistant to the types of analysis that is used to account for natural phenomena.")

Cyberspace is a globally distributed phenomenon,[328] but this is a relatively new development in its history. Though the Internet went "public" in in the mid 1990s, it's first vestiges were established in 1965 when the TX-2 computer in Massachusetts was connected to the Q-32 creating the first "wide area computer network."[329] This was followed in 1969 by the establishment of the ARPANET, a US Department of Defense funded project to establish networked computer communications which eventually "grew into the Internet."[330] The first public demonstration of Internet technology was by Bob Kahn, one of the designers of the TCP, in 1972, and that same year, email was developed.[331]

Early Cyberspace was inhabited by the people that were constructing it, meaning that "networking research incorporated both work on the underlying network and work on how to utilize the network."[332] In other words, the first individuals to set foot in Cyberspace were neither natives or explorers, they were architects. Cyberspace was not territory to be claimed in an imperial sense; it was a territory springing from a community. These individuals were forming the very rules that would bind them as they interacted in Cyberspace, and they were developing these rules as a community as was seen with the IETF and the W3C in the previous chapter.

---

[328] Manuel Castells, "Communication, Power and Counter-Power in the Network Society," *International Journal of Communication* 1, no. 1 (2007): 247.
[329] Leiner et al., "A Brief History of the Internet."
[330] *Id.* Interestingly, many commentators state that ARPANET was established as a way to create a decentralized communication system that could survive a nuclear attack that destroyed nodes within that network. Leiner et al, though, refer to this as a "false rumor" that resulted from a RAND study. *Id. See also*, Tambini et al, *Codifying Cyberspace,* 1.
[331] Leiner et al., "A Brief History of the Internet."
[332] *Id.*

The Internet that they created "embodies a key underlying technical idea, namely that of open architecture networks."[333] As discussed in Chapter 2, this means that the overall network itself is not hindered by design choices of specific network operators as interoperability is facilitated through packet switching technologies. Packet switching is a design choice that results in there being "generally no constraints on the types of network that can be included or on their geographic scope."[334] Interoperability becomes a core communicative condition through the establishment of a common standardized language, the use of which is the only prerequisite for membership in the network of networks.

Bob Kahn, one of the inventors of the TCP/IP, articulated "four ground rules" for open architecture networking.[335] First, each network connecting to the Internet "would have to stand on its own" and there could be no requirement of "internal changes" to such a network for connection.[336] Second, the transmission of data packets would be on a "best efforts basis," meaning that if a node failed to transmit a packet it would have to be retransmitted from the source.[337] Third, the gateways and routers (i.e. the physical layer) would serve transmission purposes only and retain no information about the packets being transmitted.[338] And finally. "[t]here would be no global control at the

---

[333] *Id.*
[334] *Id.*
[335] *Id.*
[336] *Id.*
[337] *Id.*
[338] *Id.* This principle underlies the rhetoric of the Internet being "stupid." Post, *In Search of Jefferson's Moose,* 40.

operations level."[339] These four principles, and especially the fourth principle, construct the limits of the public space as articulation of core values of open network architecture. They also reveal an interesting aspect of the Internet, namely that it is not a singular entity, but instead is an assemblage of technologies working together based on common rules or protocols. This technical design stood in contrast to the traditional telecommunication monopolies that were the norm during its development. The values that were entrenched can be observed in two distinct traditions in Cyberpsace: in the populist code that structures the logical layer and in libertarian code developed at the applications layers.

ii. Rights Space

Open architecture networking is more than just a set of technical specifications. It is code that embodies a set of political values embedded by its designers and reflect their specific historical situation.[340] These designers were generally Americans working at research universities during the Cold War and the American Civil Rights Movement, among other historic events.[341] Their efforts established a particular type of network design that reflect the liberal values that pervaded the coding community at that time. In particular,

---

[339] Leiner et al, "A Brief History of the Internet."
[340] Betz & Stevens, *Cyberspace and the State,* 33 ("From its earliest days, cyberspace has been suffused by a latent ideology born of a mix of technical pragmatism and heartfelt desire to 'improve the world'")
[341] Brate, *Technomanifestos,* 85.

its Cold War origins shape this design in a uniquely American way - especially since it was DoD funded at its inception.[342]

As a result, the Internet is the product of a particular historical milieu that led its designers to seek to accompany the technology with "social conscience."[343] The designers saw that "we have the free will to either place human rights and virtues – better distribution of wealth, free speech, human rights – in lockstep with technological advances or else suffer the consequences."[344] These coders therefore incorporated a "rights culture" into the developing Internet. Information theorists, like Norbert Weiner, argued that distributed flows of information would lead to open discourse "unbounded by geography or politics."[345] Such flows would be made manifest as computer scientists began to design the Internet. Early Internet pioneer Doug Engelbart focused his work on empowering the individual user of computing systems to help the collective good.[346] Doug Englebart was a leader in the field of human computer interaction, and invented the computer mouse. Brate connects Engelbart's ideology specifically to American politics at the time, including the

---

[342] For example, in a speech on Internet freedom, Secretary of State Clinton repeatedly invokes core Cyberspace values like openness and correlates them to core American constitutional values. Clinton, "Internet Rights and Wrongs." *See also* U. S. Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," July 2011, http://library.blountsfolly.com/space/items/show/184 (cyberspace should "reflect our principles"); and Martin, "Using the US Constitution to Frame the Governance of Cyberspace," 24–26 (using the US Constitution to ground policy analysis of Cyberspace governance). This should not be surprising since communications technologies have routinely been argued to carry the values of Western liberalism. *See* Mattelart, *Networking the World,* 1, 4.

[343] Brate, *Technomanifestos,* 26-27.

[344] *Id.*

[345] *Id.* at 25. On Weiner generally *see Id.* at 10-32.

[346] *Id.* at 114-141.

Civil Right Movement, and goes on to say that "Engelbart's values and ethics would remain hardwired into the future of the technology."[347]

Weiner, Englebart, and others like them sought technological development that "intersected with efforts to promote and protect many human rights."[348] The open architecture reflects these values as "technologies are imperfect and incomplete physical manifestations of the current political order."[349] As Americans, these designers would be acutely influenced the First Amendment to the American Constitution and the public space that it formulates by delegitimizing government involvement in information exchanges. The five freedoms embodied in First Amendment are all freedoms directly related to information transfer among non-governmental individuals and entities.[350] Broadly, this can be referred to as the "freedom of expression." It should be noted that the freedoms enumerated in the First Amendment are constructs:

> When the claim to freedom of expression emerged, this presupposed that an originally small but critical mass shared their desire to express their views and receive information without censorship. This desire and need were conceived and felt as something due, which in the emerging rights culture became a matter of strong expectation. This expectation grew stronger, to the point where any disregard of the expectation triggers a sense of injustice.[351]

---

[347] *Id.* at 136.
[348] David P. Fidler, "The Internet, Human Rights, and U.S. Foreign Policy: The Global Online Freedom Act of 2012," *ASIL Insights* 16, no. 18 (May 24, 2012), http://www.asil.org/insights/volume/16/issue/18/internet-human-rights-and-us-foreign-policy-global-online-freedom-act.
[349] David Banks, "The Politics of Communications Technology," Cyborgology, May 5, 2013, http://thesocietypages.org/cyborgology/2013/05/04/the-politics-of-communications-technology/.
[350] U.S. Constitution, Amend. I.
[351] Sajo, *Constitutional Sentiments*, 27.

As a construct this freedom developed along with historical processes, and the rights culture embedded in Cyberspace reflects this historical context.[352] The design itself embeds a historically contextualized freedom of expression that the designers would likely characterize as "free information."[353] The political geography of Cyberspace is one that places minimal restriction on the transfer of information and the autonomy of the individual user.[354] The early Internet community maintained a "dominant ethos . . . [of] altruism" with a "spirit of mutual aid."[355] The code was engineered to be "vehemently public sphere."[356]

The value placed on free information would be heightened by the Internet's historical links to higher education.[357] Its use spread initially on college campuses and early Internet policy spread the Internet to all University users.[358] Infact, Yahoo! was founded by two researchers on Stanford's campus whose hobby was cataloging the websites in the quickly growing cyberspace. In the United States, higher education holds freedom of expression - in terms of information sharing and inquiry - as a core egalitarian value. The majority of

---

[352] *See generally*, Ronald J. Rychlak, "Compassion, Hatred, and Free Expression," *Miss. CL Rev.* 27 (2007): 407. There are no states with completely open content rules. The United States' formulation of the freedom of expression has limits to the types of information that can be expressed, so for instance the state can regulate fighting words, obscenity, and false advertising among other items. This differs from other Western nations such as Canada, which bans "racially offensive material." Adeno Addis, "The Thin State in Thick Globalism: Sovereignty in the Information Age," *Vanderbilt Journal of Transnational Law* 37, (2004): 1-107. The question becomes one of line drawing, and it exists on a spectrum with the United States on one end and states like North Korea (with a total control of information) on the other end.

[353] Brate, *Technomanifestos*, 29 and Betz & Stevens, *Cyberspace and the State*, 18.

[354] On autonomy, *see* David Held, *Democracy and the Global Order: From the Modern State to Cosmopolitan Governance* (Stanford: Stanford University Press 1995) 145-156 and Habermas, *The Postnational Constellation,* 118.

[355] David Resnick, "Politics on the Internet," 51.

[356] Tambini et al, *Codifying Cyberspace,* 11.

[357] University computer labs were instrumental in designing the Internet. Adam Brate, *Technomanifestos,* 98.

[358] Lawrence Lessig, *Code 2.0*, 2.

the population of Cyberspace for close to half of its technical life would be primarily found in higher education.[359] The connection of the Internet to research is important, because "the network's first role was sharing the information about its own design and operation."[360] This means that the information sharing values of the academic communities became part and parcel of the values being embedded in the political geography.

The historical context in which the Internet was being designed sheds light on how the values of open architecture networking emerged. The designers of the open architecture network were working in the midst of the Cold War threat of the USSR from abroad and the upheaval of the Civil Rights Movement domestically. These events give context to the communicative conditions that were developed to support the right of free information.

First, as a product of a specific time and place - and funded by the US DoD, Cyberspace reflects values shaped by the ideological conflict in the Cold War.[361] The United States at that time emphasized openness as a way of counteracting the closed, centralized Soviet model,[362] and as a result cyberspace is designed as a "highly decentralized" network that stands in contrast to the Soviet model.[363] The "iron curtain" was a descriptive term of a political geography

---

[359] In the 1980s, the National Science Foundation required as "a condition for a U.S. university to receive NSF funding, for an Internet connection" that "'the connection must be made available to ALL qualified users on campus.'" This would change as governmental policy pushed for commercialization of the network. Leiner et al., "A Brief History of the Internet."
[360] Leiner et al., "A Brief History of the Internet."
[361] Brate, *Technomanifestos,* 89-90.
[362] See, for instance, Bush who compares information flows in the American System with information flows in the Soviet system. Vannevar Bush, *Modern Arms and Free Men* (New York: Simon and Shuster 1949), 201, 223-4. *See also* Brate, *Technomanifestos*, 48.
[363] Spar, "The Public Face of Cyberspace," 345.

that was locked and therefore not free.[364] Vannevar Bush, head of the US Office for Scientific Research and Development during World War II - which oversaw the Manhattan Project, argued that freeing information would be a tools against totalitarianism.[365] We see this reflected in the open network architecture's underlying principle of "no global control at the operations level." The decentralized and nonhierarchical network counters the Soviet model by moving power over information to the individuals using the network.

At the same time, deep questions about political membership within the United States were being raised by the Civil Rights Movement. Images of the era show African-Americans claiming space in the political geography by invading the white only spaces of the legal and spatial geography with marches and sit ins. The Civil Rights Movement was pushing for identity in the political community for minorities. The severe inequalities displayed by the civil rights movement became part of a broader narrative of liberal activism throughout the 1960s and the 1970s.[366] Open network architecture through its emphasis on interoperability has the potential to "[enhance] the equal rights of participation for all members of society" by opening access to its political geography.[367] The interoperability envisioned in the network reflects a concern

---

[364] Bush, *Modern Arms and Free Men*, 168.

[365] Brate, *Technomanifestos*, 48, 33. Bush's work on the theoretical Memex device would introduce the concept of hyperlinking and be influential on the development of the WWW. *Id.* at 33-52.

[366] Brate, *Technomanifestos* ("The crusade to augment human intellect fits nicely into the 1960s wish list of revolutionary change."); *Id.* at 192-93

[367] Rawls, *A Theory of Justice*, 224; Betz and Stevens argue that Cyberspace "pioneers had an idea of it as a form of commons." Betz & Stevens, *Cyberspace and the State,* 103; Brate, *Technomanifestos,* 104 (early Internet researchers "knew that their technology could facilitate democracy and make the distribution of knowledge more effective than ever before.")

of the coders for equality of access.[368] This coding was "motivated by the drive to create a greater good through empowerment of the people."[369] The Internet is designed specifically not to discriminate among different types of information or users.

The coders working on the design of the open network architecture can be seen to has implemented a version of the freedom of expression that is consistent with the populist leanings of their particular historical context. These early designers were primarily concerned with the logical layer of the Internet. Their design was built on populist leanings that sought to extend rights to users by constructing a space in which to create interoperable communities. The notions underlying this structure rest in the ideal that the "more information is shared, the freer society is, the greater the potential is for cooperation."[370] It is the transfer of information for the public good that underlies their project, and as we will see below transfers power to the logical layer as a result. The network was designed to created an interoperable citizenry.

iii. Liberation Space

The populist bent of the open network architecture pushes power to the edges of the network as a way to incorporate individual power into the political geography. This has an interesting effect of not only facilitating communication, but giving users the ability to define the terms of their

[368] For instance, Alan Kay saw the potential for the computer to enrich human participation in the political process. Brate, *Technomanifestos,* 185-87.
[369] Brate, *Technomanifestos*, 132-133.
[370] Brate, *Technomanifestos,* 208.

communication. The political geography extended by the logical layer allows for the development of political geography at the applications layer. This means that diverse political groups are able to create their own spaces through the use of applications. Quite possibly the best example of this is the libertarian ideals which began to drive cryptographic code as a means of individual liberation.[371] The logical layer created an opening in political space that promised "freedom without anarchy, control without government, consensus without power."[372] Libertarians saw the Internet as a place where individual rights would triumph over states rights.

This libertarian turn in the design and culture of Cyberspace was a powerful one and has a strong and lasting pedigree, and libertarian philosophy to some extent is responsible for many of the applications that redefine borders.[373] The word hacker, today, is often used to describe criminals that wreak havoc in cyberspace by stealing valuable information or defacing websites. Media accounts refer to hackers as the bad guys in cyberspace that compromise networks and systems for fun and for profit.[374] However, this use is a far cry from its origins in the tech community, wherein hackers are

---

[371] This trend was not limited to cryptography. Brate notes that hypertext theorist Ted Nelson's political ideology was "humanistic libertarian," and that Tim Berners-Lee, creator of the WWW, was influenced by Nelson's "democratic, egalitarian ideals." Brate, *Technomanifestos,* 226, 227 and Lessig, *Code 2.0*, 2 (". . . cyberspace became a new target for libertarian utopianism.")

[372] Lessig, *Code 2.0*, 2. For example, WWW was developed with "no central control" to promote the broadest information sharing ability. Brate, *Technomanifestos,* 224. *See also* Betz & Stevens, *Cyberspace and the State,* 56.

[373] A prominent example is Bitcoin, which is an application that has no "central controlling person or entity." It is "*completely decentralized*, with all parts of the transaction performed by the user of the system." Craig K. Elwell, M. M. Murphy, and Michael V. Seitzinger, "Bitcoin: Questions, Answers, and Analysis of Legal Issues," Report (United States: Library of Congress. Congressional Research Service., December 20, 2013) 1. *See also*, DeNardis, *Global War for Internet Governance*, 8 (BiTorrent); and Bearman, "The Untold Story of Silk Road" (the Silk Road).

[374] Betz & Stevens, *Cyberspace and the State,* 16 (hackers are the "new digital outlaws")

individuals "who enjoy[] exploring the details of programmable systems and how to stretch their capabilities.[375] Hackers were driven by an "ethical code [that] was driven by the progress of computer code - it was wrong, almost *evil*, to keep code or programming resources to yourself."[376] Hackers, in the original sense, believe that "information sharing is a powerful-positive good," which echos the value of free information.[377] Though hackers often resist political categorization,[378] the hacker ethic of understanding how things work "is in one sense essentially apolitical and technically focused, while in another sense it is subversive and profoundly ideological."[379] Hacking is a "way of knowing things"[380] that emphasizes empowerment through knowledge of technical architecture, easily adapts itself to a libertarian rhetoric of mainstream society "being led" and "being fed."[381]

The hacking ideology was extremely influential in Internet culture and groups such as the Cypherpunks.[382] A cypherpunk is an individual "interested in the uses of encryption via electronic ciphers for enhancing personal privacy and guarding against tyranny by centralized, authoritarian power structures, especially government."[383] Their political views are best described as

---

[375] Eric S. Raymond, *The New Hacker's Dictionary*, 3d ed. (Cambridge, MA: MIT Press 1996) 233.
[376] Brate, *Technomanifestos,* 243.
[377] Raymond, *The New Hacker's Dictionary,* 234.
[378] "A Tale of Many Hackers," *2600: The Hacker Quarterly*, v.31/3, 2015, 5.
[379] Betz & Stevens, *Cyberspace and the State,* 18 and Brate, *Technomanifestos,* 243.
[380] James Kracht, "The Hacker Perspective," *2600: The Hacker Quarterly*, v. 31/3, 2014, 26 and Brate, *Technomanifestos,* 251-252.
[381] James Kracht, "The Hacker Perspective," 26 and Prisoner #6, "The 21st Century Hacker Manifesto," *2600: The Hacker Quarterly*, v. 31/4, 2014-2015, 50-51.
[382] Greenberg, *This Machine Kills Secrets*, 94-134 and Julian Assange et al., *Cypherpunks: Freedom and the Future of the Internet* (Or Books, 2012), 21-22. *See also* Domscheit-Berg, *Inside Wikileaks,* 174-75 ("Julian [Assange] was a hacker."
[383] Raymond, *The New Hacker's Dictionary,* 140

anarcho-libertarian.[384] Using the motto "privacy for the weak, transparency for the powerful," they recognized that the applications layer could give substantive meaning to their construction of freedom of expression.[385]

The central issue to the cryptographic community is that information flows unfettered by state interference, including chilling effects of extensive surveillance.[386] Cypherpunks cast communicative conditions in terms of "[w]hat is public, and what is private."[387] Freedom of expression in this political geography rests on freedom of speech as emphasized in Western liberal democracies.[388] So for instance, while giving a speech on Wikileaks, Tor activist Jacob Applebaum informs federal agents that the only thing in his pockets is the Bill of Rights.[389] This freedom is further linked to international human rights regimes which also endorses a freedom of expression.[390] Cypherpunks however redeploy the anti-totalitarian from the Cold War against all power structures.

As a result these coders deploy code that hides the individual from power structures, including the state. Cryptographic code facilitates an political

---

[384] Greenberg states that "[e]verywhere [Cypherpunks] saw authority, they attacked it." Greenberg, *This Machine Kills Secrets*. For other examples *see Id.* at 89-91, 122, 148, 150, 192-193, 227, 255; Domscheit-Berg, *Inside Wikileaks*, 4; Assange et al., *Cypherpunks*, 29, 70-1, 76; and Tambini et al., *Codifying Cyberspace* 11.

[385] Assange et al., *Cypherpunks*, 7 and McIntosh & Cates, "Hard Travelin'," 86 (noting three arguments for free speech, the first of which "grounds free speech in the deeprooted, fundamental libertarian ideal of *individual autonomy and dignity.")*

[386] *For instance*, Edward Snowden, "Testimony before the Parliament of the European Union," March 7, 2014, http://library.blountsfolly.com/space/items/show/171 at 1 (Surveillance programs "endanger a number of basic rights which, in aggregate, constitute the foundation of liberal societies.")

[387] Domscheit-Berg, *Inside Wikileaks,* 50.

[388] Rawls, *A Theory of Justice*, 197 and US Constitution, Amend. 1.

[389] Greenberg, *This Machine Kills Secrets*, 167. Greenberg refers to Appellbaum as a "young Anarchist." *Id.* at 150.

[390] The rights asserted by Cypherpunks are contained in documents such as Universal Declaration of Human Rights, Art. 18-19. Assange would call this type of activism "liberal radicalism." Greenberg, *This Machine Kills Secrets*, 127

geography with equal distribution of power over information as a way to reallocate power and wealth. To this end they work to reclaim information technology from being "the privileged technology of neoliberalism."[391] As an example, Applebaum endorses of dispersion of power "to people who are not simply the ones who make the decisions" through what Barlow would call a "renegotiation of power."[392] Similarly, Domscheit-Berg describes Wikileaks as a project to shift political geography:

> In the world we dreamed of there would be no more bosses or hierarchies, and no one could achieve power by withholding from the others the knowledge needed to act as an equal player. That was the idea for which we fought.[393]

To anarcho-libertarians, Cyberspace's open architecture reflects their own value in individual liberty through rights, which helps to explain pervasive libertarian tone in the tech world.[394] Libertarian code uses digital cryptography to recode communicative conditions imposed on the individual and rewrite political geography. They use their code "to prove that technology not pretension would define the nature of identity on the Internet."[395]

III. Interoperability

Cyberspace contains lots of values. Any visit to a social networking, such

---

[391] David Harvey, *A Brief History of Neoliberalism* (Oxford: Oxford Univ. Press, 2009) 159; Assange et al., *Cypherpunks*, 27; and Bearman, "The Untold Story of Silk Road."
[392] Greenberg, *This Machine Kills Secrets*, 176, 255
[393] Domsheit-Berg, *Inside Wikileaks*, 4
[394] Spar, "The Public Face of Cyberspace," 347 (" . . . the radical promise of the Internet was to dismantle existing chains of authority.") Tambini et al note that the there is also a strain of a "new type of radical free-market libertarianism," which is more concerned with "corporate and commercial freedom" from government economic regulation. Tambini et al., *Codifying Cyberspace,* 11; Sunstein, *Republic. Com 2.0,* 111-12; and Bearman, "The Untold Story of Silk Road."
[395] Andy Greenberg, *This Machine Kills Secrets,* 115.

as Facebook, website will quickly display numerous different value sets. These value sets are not the values *of* cyberspace, but the variety and scope of them is indicative of the political geography of Cyberspace. As Lessig observes that the space that is constructed "depends entirely on the values that guide development of that place."[396] As discussed above, the principles of open network architecture are constitutional values that express through packet switching technology. these principles and the code of packet switching create a political geography built around interoperability. The abundance of divergent views that are expressed in Cyberspace is a result of the interoperability value.

Interoperability pervades cyberspace and organizes its geography. More than just technical design, interoperability can be seen as the value given constitutional force in the code. It address the concerns about closed [political space and opens up space for further expansion of political space though the applications layer. Interoperability is the operalization of "information wants to be free." It recognizes that information freedom rests in the ability for information to be communicated among as many individuals as possible.

As the core value in Cyberspace, Interoperability facilitates direct communication by devices, and therefore it can be seen as facilitating interoperability among individuals as well. Interoperability uses three mechanisms to shape political geography. First, it decentralizes communications. Second, it creates free access through openness. Third, it creates equality on the network through peering. Critically these mechanisms shift the division between ruler and ruled, and fosters participation by opening

---

[396] Lessig, *Code 2.0*, 70.

up political membership. Interoperability means that participation is no longer subject to specific central authority; instead participation is self authenticating through the adoption of a standard protocol.

The networkification of the world pushes this principle to a world scale and makes geography interoperable. Networked geography is no longer bounded in terms of exclusion. Instead, its limits can be understood in terms of inclusion and accessibility. This means that the bounds of the political geography of Cyberspace are not territorial, rather the bounds are the digital divide between those with access and those without.

* * * * *

The layered model is a conceptual stack that a framework for understanding the complex technical architecture of Cyberspace. By delineating different functions, the layers model allows for categorization of technologies so that they can be understood for their discrete functions and features. The layered model though sometimes obscures the fact that these technologies are not always discrete, and that Cyberspace is an assemblage of these layers.

Similarly, thus far the *geography* of cyberspace has been described as layered: a spatial geography layered with a legal geography that is layered with a political geography. The problem is that all these geographies happen at once. When an individual looks at the state of their nationality on a map, they do not see the drawn borders and deconstruct the state into spatial, legal, and political

units. Instead, the borders represent a compression of those concepts into a single understandable geography. While one can not *see* Cyberspace in terms of borders, the experience of Cyberspace is such that individuals experience the same compression of concepts, possibly more so. In real space it is much easier to disaggregate physical geography, such as a mountain, from the other geographies of the state. In the geography of the state, the mountain stays the same while the legal and political geographies that encompass it can change, sometimes literally, at the stroke of midnight. In Cyberspace the geography can change at a keystroke.

The geographic compression in code, is a natural extension of Lessig's principle: code is geography. Cyberspace does not have nature; it only has code and as such code is central to its organization. Part I has described Cyberspace in insular terms. This is a view of Cyberspace from within Cyberspace, which is not without its limitations. This exercise will prove essential in examining how Cyberspace as an alternative geography interacts with international space.

Interlude

“Obviously, when an old world sees a new world arise beside it, it is challenged dialectically and is no longer old in the same sense.”

- David Berlinski

Chapter 5

The Nomos of Cyberspace

In 1543 Copernicus first published his theory of a heliocentric universe, a theologically controversial idea that would play out in the early 1600s when the Catholic Church placed Galileo on trial for supporting such views. The Church, in 1616, banned books that supported a Copernican map of the solar system and only recently recanted its position in the Galileo matter.[397] Scientifically, the work of these two scholars can not be overstated as the heliocentric model is integrated in human understanding of the solar system and the universe. It is the Church's reaction to the Copernican map that shows the true impact of Copernican thinking. The Catholic Church at the time was trying to maintain dominance in Western Europe, and its claim to legitimacy and power was rooted in the space of Christendom. This sphere of Christ, oriented towards the central divine authority of the Pope, was experiencing growing pains as kings and princes making claims to similar authority. In the wake of the English Reformation and on the eve of Westphalia, the Copernican map literally changed Western human orientation within the geography of the universe.[398] The map presented by the Catholic Church was one that depended on the Church being at the center of the Universe making it the natural focal

---

[397] Alan Cowell, "After 350 Years, Vatican Says Galileo Was Right: It Moves," *The New York Times*, October 31, 1992, sec. World, http://www.nytimes.com/1992/10/31/world/after-350-years-vatican-says-galileo-was-right-it-moves.html.

[398] Schmitt, The Nomos of the Earth, 86 ("The new global image . . . required a new spatial order.").

point for the heavenly gaze. The legitimating principle of divine right depended on the centralization of that right of a single point importance.[399] Copernican thinking destroyed "a world in which the spatial structure embodied a hierarchy of values" and replaced it with "a universe of indefinite proportions."[400] This fragmented the map of Christendom by diminishing the importance of its chief spatial indicators: the Rome and the Pope were no longer the literal center of the Universe. Indeed, the human race itself had been moved to the periphery.

Now, move the clock forward 400 years to 2016 and transport to a New York City street (or any street in any big city or medium sized city or, quite possibly, any street, anywhere). If you look around you will likely see someone looking at a map on a digital device. A map that conveniently centers on that individual's location at the touch of a button. The power in Copernicus' idea, has in a sense been lost. Humans have found their way back to the center of the map. More precisely, the digital device has found its way to the center of the map which reveals the user's location, and the gap between device and user is shrinking.[401] These maps choose their centers dynamically imparting importance on the device and the user as they both move through space and

---

[399] *Id.* at 112. (". . . the distinction between the territory of Christian and non-Christian princes and peoples remained fundamental to and characteristic of that spatial order.")

[400] Coicaud, *Legitimacy and Politics,* 98

[401] *For example see* Lessig, *Code 2.0* ("Your hard drive is you."); Riley v. California, No. 13-132 (2014) 18 (noting that modern cell phones contain data from which "the sum of an individual's private life can be reconstructed."); and Streck, "Pulling the Plug on Electronic Town Meetings," 25 ("Paradoxical though it may seem, with a device-driven conception of cyberspace the device slips away leaving an empty vessel to be filled with whatever meaning those who control the discourse might choose to assign it."). *See also*, the literature on transhumanism, for example George S. Robinson, "Addressing the Legal Status of Evolving 'Envoys of Mankind,'" *Annals of Air and Space Law* 36 (2011): 470-475.

time, and as a result the user experience is such that they become part of the map as space extends out from them both virtually and physically.

This idea that humans are at the center of the map again, is more than just a quippy metaphor. Maps, at their most basic, display the relative location of various geographic epistemic units. As a representation of the world, maps are human constructions of orientation, and as such maps construct how humans experience the world.[402] The lesson from Galileo is that the choice of where to center a map is a choice relative importance.[403] As a result, a world map made for a U.S. middle school social studies class during the Cold War might center the United States thereby dividing Soviet Union into two parts thereby reinforcing national identity. Even the seemingly neutral choice to place the Prime Meridian at the center of some world maps embeds Western primacy by entrenching the Atlantic Worldview. Buckminster Fuller's Dymaxion map serves as a counter narrative to maps that show division by reprojecting the world as one continuous landmass, which allows for a different conceptualization of how the world is connected.[404] Fuller's projection was meant to challenge specifically the boilerplate nature of the traditional world map, by diminishing the importance of its center and taking away conceived notions of up and down produced by cardinal directions. The Dymaxion Map projects the world on an icosahedron, which can be unfolded in multiple ways

---

[402] Schmitt connects cartography with displaying a need for "a substantive spatial order of the Earth." Schmitt, *The Nomos of the Earth,* 86.

[403] Schmitt tells us that "great power complexes" have always conceptualized themselves as "the world" or the "center of the world." *Id.* at 51.

[404] Buckminster Fuller Institute, "The Dymaxion Map," https://bfi.org/about-fuller/big-ideas/dymaxion-world/dymaxion-map (last visited Feb. 15, 2016).

to reveal the connections and disconnections in the world (see Fig. 5.1). Fuller's map also embraced the idea that geographic understandings can and do change, and these understandings change how individuals and societies understand the world.

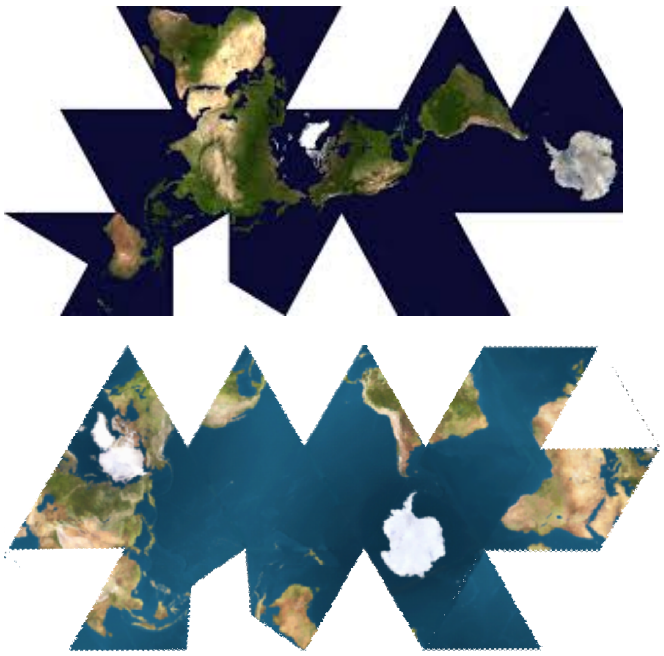

Fig. 5.1: Buckminster Fuller's Dymaxion Map, showing the Earth's territory as one landmass at top and showing the Earth's seas as a single ocean at bottom.

Since maps signify space, then control of maps is linked to control of space. As a result, many states have strict mapping laws. For example, China's State Secrets Law places geographic information under the control of the

Central Government.[405] Such control of space by the state is not without its complications. The Google Maps tool has repeatedly been at the center of controversies on how borders are drawn in its mapping software.[406] Borders are important because they set limits: spatial, legal, and political. The center of the map, chosen for importance, is limited by borders, which show the limits of the central power. In terms of the state, for instance, the map shows a star as the central capital, and solid dividing lines as the borders of both the values and law that flows from the star.

Chapters 2-4 describe the geography of Cyberspace from within Cyberspace. This choice of perspective purposely centers Cyberspace in terms of importance and diminishes territory in terms of borders.[407] It would of course to be disingenuous to argue that Cyberspace is not linked to territory, as the physical layer clearly reveals the territorial links. Thus, Goldsmith's claim still rings true, Cyberspace only exists as a result of human enterprise in a physical world, therefore Cyberspace cannot be separated from the physical world in any real sense. Virtual reality is, after all, still virtual.[408] This chapter takes the presented geography of Cyberspace and argues that it presents social

---

[405] Kathrin Hille, "China Cracks Down on Online Maps," *Financial Times*, May 21, 2010, http://www.ft.com/cms/s/0/9569b59e-64f3-11df-aa4d-00144feab49a.html#axzz40FUFCz8W. *See also* Kulesza, *International Internet Law*, 114-15..

[406] *See generally* Wesley Fenlon, "Did Google Maps Cause an International Border Dispute?," *HowStuffWorks*, October 3, 2011, http://computer.howstuffworks.com/google-maps-international-border-dispute.htm; "India Google Maps Controversy Is Modern Drama," *Democracy Chronicles*, July 29, 2014, https://democracychronicles.com/india-google-maps-controversy-modern-drama/, and Adam Taylor, "The Simple Way Google Maps Could Side-Step Its Crimea Controversy," *The Washington Post*, April 1, 2014, https://www.washingtonpost.com/news/worldviews/wp/2014/04/01/the-simple-way-google-maps-could-side-step-its-crimea-controversy/..

[407] *See* Kulesza, *International Internet Law*, xii (" . . . the world perceived through the prism of the Internet is opposed to traditional geography.").

[408] *But see* Ferguson & Mansbach, *Globalization,* 136 ("spatial reality can be virtual reality") +

actors with an alternative geography that "detach[es] social and political reality from the world of sovereign states."[409] The alternate geography is not a separate place as envisaged by Barlow, instead it is a way of knowing and conceptualizing space that rewires the way we experience the primary geography of the world. It follows then that cyberspace changes the way in which individuals experience and approach the space in which they inhabit. This shift in geography does not nullify borders, but it changes their content and meaning, which in turn causes shifts in the underlying governance structures that support such borders. In essence the argument here is that Cyberspace transforms geography and governance from the international into the interoperable global. The first section will explore the concept of borders and their changing meanings. The second section, will argue that Cyberspace re-codes borders and changes their geographic content. The final section will use the concept of *nomos* to argue the re-coding of borders is changing world order.

I. Borderless Worlds

The spatial narrative introduced in Chapter 2 is based on lingual cliches that have rooted themselves into the descriptions of Cyberspace. One of the most popular of these cliches references the Internet and Cyberspace as "borderless" in scope.[410] As part of the spatial narrative, borderlessness is

---

[409] Kulesza, *International Internet Law*, xi-xii; and Bowman, "Thinking Outside the Border," 221-22 ("noting the "evolutionary" nature of borders")

[410] *See generally* Lessig, *Code 2.0*, 71 (". . . bits have no borders."); Kulesza, *International Internet Law*, 45 ("an age of borderless cyberspace"); and Martin, "Using the US Constitution to Frame the Governance of Cyberspace," 24 ("borderless virtual place")

associated with the free transfer of information across national frontiers. Designating a space without containment or limits, borderless is used specifically to invoke a counter narrative to international space in terms of spatial, legal, and political geography.[411]

A realist response to assertions of borderlessness is obvious: each physical component and user has location within territory and is subject to the *lex loci* of that place.[412] There is ample evidence to support such claims. China controls the Internet at nine physical locations where where it allows the Internet to travel across its border.[413] North Korea also keeps tight control over physical entry points for the Internet, and sharply controls individuals' access within its physical geography.[414] Iran has plans to create a "halal Internet" that exists exclusively within its borders.[415] The US and UK's ability to engage in mass surveillance is based on the physical location of infrastructure in the United States and the United Kingdom.[416] Egypt turned the Internet off during

---

[411] "[E]xclusiveness of power over state territory and citizens" is one of the key "indicators of state sovereignty." Kulesza, *International Internet Law*, 2. Borderlessness is connected to lawlessness, so for instance Hobbes' state of nature is located "in the new world." Schmitt, *The Nomos of the Earth,* 96.

[412] Goldsmith, "Against Cyberanarchy," at 7; *see also* Sofner et al., "Cyber Security and International Agreements," 190; and Yannakogeorgos & Lowther, "The Prospects for Cyber Deterrence," 50.

[413] Kulesza, *International Internet Law*, 109-10.

[414] Matthew Sparkes, "Internet in North Korea: Everything You Need to Know," December 23, 2014, sec. Technology, http://www.telegraph.co.uk/technology/11309882/Internet-in-North-Korea-everything-you-need-to-know.html.

[415] Doug Bernard, "Iran's Next Step in Building a 'Halal' Internet," *Voice of America*, March 9, 2015, http://www.voanews.com/content/irans-next-step-in-building-a-halal-internet/2672948.html.

[416] Glenn Greenwald and Ewen MacAskill, "NSA PRISM Program Taps in to User Data of Apple, Google and Others," *The Guardian*, June 7, 2013, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data and Barton Gellman and Laura Poitras, "U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program," *The Washington Post*, June 7, 2013, http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-in

the Arab Spring.[417] Realists, both legal and political, have a plethora of evidence to support the claim that the Internet exists within state borders, and that states pursue their national interests in that arena just as they did when steamships were the transformative technology. To some extent the realist is correct: borders remain an important feature of our experience of the world and they remain important in the organization of law and politics at a global level.

Both the "borderless" rhetoric and the realist argument have a central flaw. They both attempt to describe Cyberspace in terms of the state. The rhetoric miscalculates the level of integration of Cyberspace into the fiber of the state, and the realest miscalculates the lack of control that the state has over that integration. The realist view tends to engage with Cyberspace as counterfactual to the state system by focusing on discrete layers of functionality as a reaction to positions such as Barlow's, which also adopts Cyberspace as a counterfactual to the state system. In the realist critique Cyberspace is a thing, and things are the subject of the territorial authority. This externalization of Cyberspace is natural for a variety of reasons, but it insufficiently theorizes Cyberspace and ignores the endogenous nature of Cyberspace that shapes the space in which law and politics unfold.

Cyberspace is not a counterfactual to the state. Cyberspace is a part of everyday human life in almost every aspect: leisure, business, commercial,

---

ternet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

[417] Matt Richtel, "Egypt Cuts Off Most Internet and Cellphone Service," *The New York Times*, January 28, 2011, http://www.nytimes.com/2011/01/29/technology/internet/29cutoff.html.

political, even romantic.[418] Cyberspace is no longer exogenous to social interaction, it has become an "endogenous and political"[419] factor "embedded in the material condition" of the world.[420] Geographically speaking, Cyberspace is more river than highway. It is a part of the landscape, and it is difficult to control. Maybe one of the best examples of this can be found in one of the central realist institutions: the military. Militaries around the globe now include Cyberspace as one of the domains in which they operate.[421] By joining Cyberspace with land, sea, air, and space, there is an explicit spatial recognition of Cyberspace as a space *in* which military operations can take *place*.[422] This is more than just rhetorical, it is acknowledgement that Cyberspace constitutes a new locus for borders.[423] National defense is an act of protecting borders and Cyberspace as a domain of military operations spatializes Cyberspace as another place that intersects and influences the space of the state.[424] Military doctrine adopts Cyberspace not as a thing to be controlled, but instead as an endogenous medium with a geography that shapes the most realist of activities.

What then is to be made of the map which is still inscribed with the borders of international space? The borderless rhetoric seems empty in the

---

[418] It is "inextricably intertwined with daily life." Edward C. Liu et al., "Cybersecurity: Selected Legal Issues," Report (Congressional Research Service, Library of Congress, April 20, 2012) 1. *See also* Council of the European Union, "EU Human Rights Guidelines on Freedom of Expression Online and Offline," I.D.33 and Kulesza, *International Internet Law*, ix.
[419] Fritsch, "Technology and Global Affairs,"28.
[420] Luke, "The Politics of Digital Inequality," 120.
[421] Kulesza, *International Internet Law*, 67 (". . . cyberspace is the fifth battlefield . . . "); US Department of Defense, "Department of Defense Strategy for Operating in Cyberspace"; and Hayden, "The Future of Things Cyber," 3–8.
[422] Betz and Stevens note that an important difference from other domains is that Cyberspace is "entirely manmade." Betz & Stevens, *Cyberspace and the State,* 33.
[423] US Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," 8 (Cyberspace crosses "national boundaries").
[424] *Id.* at 5 (Cyberspace as a domain is a "critical organizational concept for DoDs national security missions.")

face of a clearly depicted international system, because borderlessness asserts an anarchic counterfactual that is not experienced by the user.[425] A better term would be re-bordered which implicates not just the location of borders, but their content as well. Users still experience the borders that appear on a political map of the world. These borders represent national frontiers many of which, if visited, might even be demarcated by walls, fences, or other physical divisions. Physical borders are often, quite literally, legal lines drawn in the sand. They demarcate jurisdiction as deployed across space by political processes. National borders demarcate people into discrete political units of difference, at least in theory. Borders are then inscribed on maps, and, as Wendy Brown notes, are often inscribed physically on the Earth's surface as states build physical barriers along lines the lines of political demarcation.[426] These barriers "draw on the easy legitimacy of sovereign border control even as they aim to function more as prophylactics against postnational, transnational, or subnational forces that do not align neatly with nation-states or their boundaries."[427] To states, and thus to realists, borders still matter.

As Brown observes, these physical landmarks are not fortifications against other states, but against the ideas of other space.[428] The fortifications

---

[425] Johnson & Post, "Law and Borders," 1389 ("Cyberspace is anything but anarchic . . .")
[426] Wendy Brown, *Walled States, Waning Sovereignty* (New York; Cambridge, Mass.: Zone Books ; Distributed by the MIT Press, 2010) 7-20; *Compare with* Schmitt, *The Nomos of the Earth* (" . . . the solid ground of the earth is delineated by fences, enclosures, boundaries, walls, houses, and other constructs.").
[427] Brown, *Walled States, Waning Sovereignty*, 32. *See also* Habermas, *The Postnational Constellation* 80-81 ("This defensive rhetoric invokes the political will to close the floodgates against uncontrolled waves breaking in from the outside.").
[428] Bigo echoes such notion in his "globalization of insecurity" which "makes national borders effectively obsolete as they no longer operate as effective barriers, fences, or fortresses behind which the population feels safe." Bigo, "The Emergence of a Consensus," 76–94. Compare to

are attempts to construct the meaning and content of national borders in the public mind, but "[s]tate borders are certainly not comparable to fortifications" despite this physical architecture.[429] This function of borders is not new and has historically been implicated with information technologies. Vannever Bush in 1949 wrote that "[i]ron curtains are not new inventions; yet they are now harder to maintain."[430] Bush's evaluation in the wake of WWII taps into a familiar logic of transparency and liberation driven by free flow of information. Bush though, pushes this narrative further by observing that the "same technical advances that sustain in mystery the distant emperor . . . also tend to penetrate the barriers to ideas that he must maintain for his continued sway."[431] This observation places technology as central to the transformation of space through social experience. Thus while borders maintain a "physical obdurate premodern signature," the power they contain "is networked virtually" and the people they contain are "hybridized."[432] Interoperability renders standards as "non-tariff barrier[s]" which eases interaction across these fortifications.[433]

Domscheit-Berg's rhetoric of Wikileaks as an "unassailable fortress" to underscore its liberty from state power. Domscheit-Berg, *Inside Wikileaks,* 131.

[429] Habermas, *The Postnational Constellation,* 66.

[430] Bush, *Modern Arms & Free Men*, 168.

[431] *Id*. Such sentiments can be traced through to documents such as Assange's "Conspiracy as Governance" which characterizes "authoritarian regimes as collections of nodes connected by lines of communication that depend on technology for their survival." Greenberg, *This Machine Kills Secrets* 128 and Julian Assange, "Conspiracy as Governance," *IQ. Org*, 2006, http://library.blountsfolly.com/space/items/show/172. This should be juxtaposed to views such as Morozov's which read cyberspace as empowering authoritarian governments. Morozov, "Political Repression 2.0." *See also* Lessig, *Code 2.0*, 53 (". . . cryptography is Janus-faced."); and Benjamin Wittes, "The Intelligence Legitimacy Paradox," blog, *Lawfare*, (May 15, 2014), http://www.lawfareblog.com/2014/05/the-intelligence-legitimacy-paradox/ ("Technology . . . is a coin with two sides - or maybe a die with many sides . . . ").

[432] Brown, *Walled States, Waning Sovereignty*, 80.

[433] Jayakar, "Globalization and the Legitimacy of International Telecommunications Standard-Setting Organizations," 716.

Just as Copernicus started a process of changing the way in which humans orient themselves to the world, the technology of Cyberspace is causing shifts in human orientation to the world. Copernicus did not change the borders of the territories he was describing, he simply reoriented those territories drawing into question the content of their borders. Cyberspace does the same. As a decentralized, interoperable network, Cyberspace presents an alternate geography that is increasingly networked into the social consciousness. It is this non-Copernican conception of the world that allows for the social construction and experience of global space by "destroying notions of traditional borders."[434] Such construction and experience happens on the other side of "a legally significant border between Cyberspace and the 'real world.'"[435] The technical design of Cyberspace, the architecture itself, is reprogramming the content layer of geography by recoding borders.

II. Re-coding Borders

To understand this process of re-coding borders, it would be helpful to have a map of Cyberspace.[436] As such, a map would help to uphold the claim of cybergeography made throughout this study. There is rich work on mapping cyberspace which reveal a variety of aspects. These maps show the world as a disaggregated networks. Borders in the traditional sense are not indicated

---

[434] Spar, "The Public Face of Cyberspace," 347.
[435] Johnson & Post, "Law and Borders," 1378.
[436] Post, *In Search of Jefferson's Moose*, 24 ("A good map of cyberspace, then, will help us get started.")

despite the state's claim to the physical layer (See Fig. 5.2).[437] One of the reasons for this separation is that the "cost and speed of message transmission on the Net is almost entirely independent of physical location."[438] Instead, these often beautiful maps reveal network connections in the shape of a decentralized and distributed network and display the vast opportunities for interoperability.[439] Cyberspace is depicted as the sum of its endpoints, making its true external border the digital divide.[440] Indeed, in most maps of the Internet, geographic features - the traditional features represented on maps - are the exact feature that are obscured.[441] Instead, these maps show the configuration of the network from a variety of different perspectives.

---

[437] *See generally*, Martin Dodge and Rob Kitchin, "Ways to Map Cyberspace," *Directions Magazine*, November 7, 2001, http://www.directionsmag.com/entry/ways-to-map-cyberspace/124119 and Post, *In Search of Jefferson's Moose*, 23-30.

[438] Johnson & Post, "Law and Borders," 1370.

[439] Post, *In Search of Jefferson's Moose,* 23-28. Leiner et al. refer to Internet as "a network in name and geography." Leiner et al., "A Brief History of the Internet."

[440] In other words, where the territory of digitization runs out. Luke, "The Politics of Digital Inequality," 133 ("Not having access in the Global Network, then, is as important a dividing line as territorial borders or ethnic cultures once were."); and Cooper, "What Is the Concept of Globalization Good For?" *African Affairs* 100, no. 399 (2001): 190 ("Structures and networks penetrate certain places and do certain things with great intensity, but their effects tail off elsewhere.").

[441] Post notes the lack of utility in a "you are here" sticker on a network map. Post, *In Search of Jefferson's Moose,* 28.

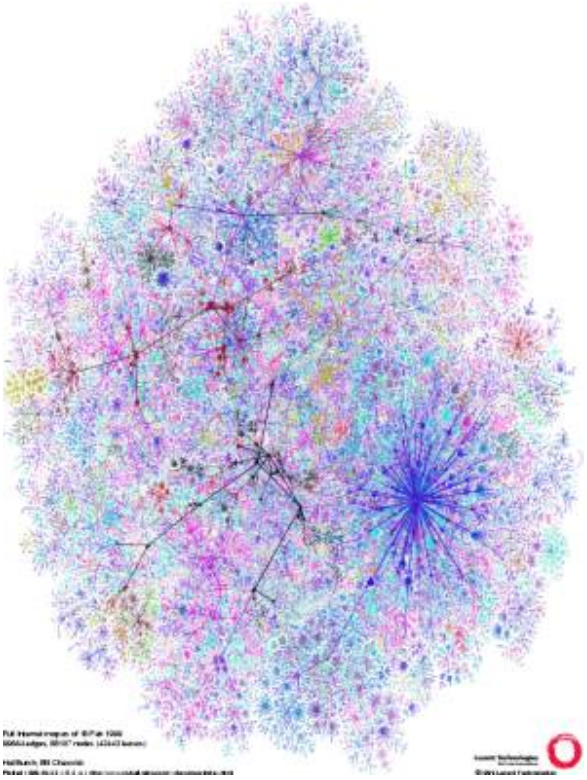

Fig. 5.2: A router level map of Cyberspace.[442]

Maps of Cyberspace are not Copernican maps, with humans at the edges circling around a central power source. These maps show the connections among humans at a global scale, and these connections are strikingly decentralized.[443] In fact there is often no discernible center at all, meaning that these maps are dynamically configurable to allow for understanding of the interactions they chart. Cyberspace maps reflect spatial characteristics in terms of devices and users, placing devices and users as the external boundaries of its legal and political geography and reflecting the

---

[442] Martin Dodge, "An Atlas of Cyberspace," https://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/topology.html (last visited February 15, 2016).
[443] Post, *In Search of Jefferson's Moose,* 28.

interoperability of open architecture networking.[444] These visualization depict an alternative geography in which the "power to control activity in Cyberspace has only the most tenuous connections to physical geography."[445] The idea of the border is unhinged from territory, which calls for reconsideration of spatial, legal, and political geography.[446]

What we are left with is a dual geography which the conceptual separation of Cyberspace from real space becomes increasingly untenable as there is dissonance between an observed physical reality of borders and an experienced spatial reality in which these borders do not exist.[447] This can be seen in the sociological debate between "digital dualism" and "augmented reality." These two sociological concepts are used to describe the effect of the human absorption of Cyberspace. Digital dualism suggests two selves: one online and one offline. Whereas augmented reality posits a cyber-experience that augments the perception in the real world.[448] Digital dualism keeps separate the "virtual" and the "real," and augmented reality on the other hand argues that "the digital and the physical are increasingly meshed" as

---

444 Leiner et al., "A Brief History of the Internet." ("There are generally no constraints on the types of networks that can be included or on their geographic scope . . .").
445 Johnson & Post, "Law and Borders," 1371.
446 Leiner et al., "A Brief History of the Internet." (The Internet is "a medium for collaboration and interaction between individuals and their computers without regard for geographic location.").Cooper notes, in his critique of globalization, that history is marked by a "back-and-forth varied combination of territorializing and deterritorializing tendencies." Cooper, "What Is the Concept of Globalization Good For?," 191.
447 Stephen K. Gourley, "Cyber Sovereignty," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton: Taylor & Francis, 2013), 277-78.
448 Nathan Jurgenson, "Digital Dualism versus Augmented Reality," *Cyborgology*, February 24, 2011,
http://thesocietypages.org/cyborgology/2011/02/24/digital-dualism-versus-augmented-reality/.

Cyberspace "implodes atoms and bits."[449] This debate centers on how the social mind reconciles two different maps of the world. Augmented reality allows such a reconciliation to be achieved through the development of new understandings of geography.

This need for reconciliation is important in broader terms as well since it requires a reconciliation of the international with the global. International governance is structured around territorial, international assumptions as opposed to global assumptions.[450] At the root of the international is the assumption of national space as a stack of spatial, legal, and political geography compressed into the concurrent borders.[451] Changes in the international system are generally understood in terms of changes in borders. It is along these lines of geographic understandings that serve as focal points for scholars of world order. This is why Westphalia is a central inquiry for many scholars, as it serves as a fulcrum point for observing transitions in the variety of geographic compressions.[452] There is recognition that changes in how territory is divided is critical to understanding the structure of the international system. Territory is *the* threshold question of all international legal and political issues.

---

[449] *Id.*

[450] *See* Kulesza, *International Internet Law*, 30 (" . . . the Internet in virtue of its limitless nature may not be described using principles mainly based on criterion of territorial sovereignty.")

[451] *See* Habermas, *The Postnational Constellation,* 60 ("The phenomena of the territorial state, the nation, and popular economy constituted within national borders formed a constellation in which democratic process assumed a more or less convincing institutional form."); *Id.* at 63 ("the conditions for a successful compulsory law require that the social delimitation of political community has to be combined with the territorial delimitation of the geographical area that will be under control of a state."); Sassen, *Territory, Authority, Rights*, 40 ("Today, we think of the question of exclusive state authority as imbricated with territory and nation-states as constituting equal jurisdictions."). This compression not necessarily "arbitrary" as "geographic borders for law make sense in the real world." Johnson & Post, "Law and Borders: The Rise of Law in Cyberspace," 1369 and Sassen, *Territory, Authority, Rights*, 20.

[452] Clark, *Legitimacy in International Society*, at 35

This link between law and spatial organization is what Schmitt refers to as *nomos,* which explicitly ties the subdivision of the Earth's land territory to the development of law.[453] *Nomos*, as used by Schmitt, naturalizes law in the sense that law flows from *terra firma due* to a human need to divide the Earth with lines ranging from furrows in a field to national frontiers.[454] He claims that "the great primeval acts of law [are] terrestrial orientations: appropriating land, founding cities, and establishing colonies."[455] International law then is the result of *how* humans draw lines on the Earth, and Schmitt's analysis focuses on transitions that reconstitute those borders and, importantly, how understandings of space changes. In other words, Schmitt's account is tied to the land.[456] Schmitt's central observation that spatial conceptualization is inherently linked to governance is salient, but in a networked world it must be understood as being linked not to land but to geography as mapped by human understanding of the spatial condition.

Schmitt's analysis thus falls short in that it fails to contemplate the opening of new space with any real depth.[457] His idea that "[l]aw is bound to the land" recenters the Earth's territory in terms of legal geography with the Earth "contain[ing] law," "manifest[ing] law upon" itself, and "sustain[ing] law above itself."[458] He flirts with alternative geographies when he discusses how technology can push forward a "global image," but his analysis is always

---

[453] " . . . *nomos* is the immediate form in which the political and social order of a people becomes spatially visible." Schmitt, *The Nomos of the Earth,* 70.
[454] *Id.* at 42
[455] *Id.* at 44.
[456] Quite literally: "Law is bound to the land." Schmitt, *The Nomos of the Earth,* 42.
[457] He notes the Airspace at the end of the volume, but his conception of airspace is still tied directly to physical territory. Schmitt, *The Nomos of the Earth*, 351-355.
[458] *Id.* at 42

constrained by the ends of the earth.[459] Specifically, he argues that his idea of *nomos* is not applicable to the sea, because it is not divisible in the same way that territory in the form of land is. There is, in his estimation, no *nomos* of the sea, because the seas defies subdivision, and can only be understood as an adjacency to the land. Any law applicable to the sea flows from its adjacency to land. The sea is a global commons except in its liminal spaces where it is sufficiently attached to territory.[460] For Schmitt, non-land can only be defined through its proximity to land.

This ignores the idea that the experience of territory itself is shaped by non-land areas. The ocean can rise up and take territory, thus individuals living on an island likely understand territory differently from individuals in a land locked area.[461] Schmitt's theoretical limitations are exposed by the contemporaneous dawning of the space age in which humans were first able to see the planet Earth as a globe.[462] Pictures from the early days of space exploration reflect a concurrent changes in the spatialization of the Earth's surface. The ability to visualize the Earth not as a map but as a photographic image, literalizing Schmitt's "global image," coincided with major shifts in international governance that began the process of reconstructing international space in the wake of World War II. This reorganization, though

---

[459] *Id.* at 86.
[460] This is a "land-bound perspective of the sea." Schmitt, *The Nomos of the Earth,* 183
[461] For examples, the Maldives concern environmental governance is based on a different orientation to territory than a continental state. Damian Carrington, "The Maldives Is the Extreme Test Case for Climate Change Action," *The Guardian*, September 26, 2013, sec. Environment, http://www.theguardian.com/environment/damian-carrington-blog/2013/sep/26/maldives-test-case-climate-change-action.
[462] The first image of the Earth from outer space was taken in 1947. Jason Major, "This Is the Very First Photo of Earth From Space," *Universe Today*, October 24, 2014, http://www.universetoday.com/115641/this-is-the-very-first-photo-of-earth-from-space/ .

ultimately based on the "territorial integrity and political independence" of the state, would for the first time include human rights as part of the organizing logic for international society.[463] Images of Earth from outer space, such as the Blue Marble, allow for and necessitate reflection on assumptions about the meaning of borders.[464] The photographic medium itself can be seen as closer to experience, than a map which encodes experience and embeds design choice.

Cyberspace has a similar, arguably, stronger effect. Cyberspace architecture allows users to experience borders differently thereby reconstituting the social understanding of those borders.[465] It "cut[s] across territorial borders" and "[undermines] the feasibility - and legitimacy - of laws based on geographic boundaries."[466] While individuals may still feel physically contained by those borders, they are no longer metaphysically contained as well. They instead can import ideas and communications at will across those borders.[467] The human conscience is extended into a global domain.[468] Tied to the values embedded by the coders of Cyberspace, this means that nations are "now wired . . . with an architecture of communication that builds a far

---

[463] UN Charter, Art. 1-2.

[464] NASA, "Blue Marble - Image of the Earth from Apollo 17," *NASA*, (July 31, 2015), http://www.nasa.gov/content/blue-marble-image-of-the-earth-from-apollo-17. *See also* Mike Featherstone, "Genealogies of the Global," *Theory, Culture & Society* 23, no. 2/3 (March 2006): 387.

[465] Similarly, Habermas notes that in the 1830s "travellers on the earliest railways described a new mode of perception of space and time." Habermas, *The Postnational Constellation,* 42.

[466] Johnson & Post, "Law and Borders, 1367.

[467] *Id.* at 1372 ("Individual electrons can easily, and without and realistic prospect of deflection 'enter' any sovereign's territory.")

[468] Habermas, *The Postnational Constellation,* 39 ("Since mid-century . . . the physiognomy of persons in great numbers has itself undergone change, The presence of bodies - collected, herded together, set in motion - has given way to the symbolic inclusion of the consciousness of the many into even wider networks of communication: the concentrated masses have been transformed into a broadly dispersed public of mass media."). *See also* Coicaud, *Legitimacy and Politics,* 136 (placing importance on the "role of individuals in the historical production of reality.") and Betz & Stevens, *Cyberspace and the State,* 106 (placing the edge of Cyberspace "in the cerebral cortex of the human brain, where . . . sense of consciousness resides.")

stronger First Amendment than [American] ideology ever advanced."[469] As argued in Chapter 4, this "stronger First Amendment" is really a freedom of expression as envisioned by the designers of the Internet and its applications.

Cyberspace is not like the global commons as portrayed by Schmitt. Schmitt claims that the "sea is free" and that "[o]n the open sea there were no limits, no boundaries, no consecrated sites, no sacred orientations, no law, and no property."[470] Schmitt is asserting that the governance structure of global commons excludes these spaces for their lack of geography.[471] This is why the 'borderless world' rhetoric is a poor description of Cyberspace. It deprives it of geography. Cyberspace though does not lack "sacred orientations." Quite the opposite, Cyberspace is increasingly becoming a waymarker for individuals moving in real space. Such waymarkers include phrases like "Google it"; the use of twitter as a locus for action in traditional new coverage; and, possibly most starkly, the proliferation of printed QR codes that serves as physical doors to places in Cyberspace (see Fig 5.3).

---

[469] Lessig, *Code 2.0*, 236.
[470] Schmitt, *Nomos of the Earth*, 43.
[471] United Nations Convention on the Law of the Sea (December 10, 1982) Art. 2; Antarctic Treaty (December 1, 1959) art. IV(2); and Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (January 27, 1967) art. II.

Fig. 5.3: QR codes are images that users can scan with a device such as a phone in order to gain informations. Such codes can be printed and placed in real space to give users entry into Cyberspace. The QR code pictured opens a hyperlink to http://space.blountsfolly.com

Another reason to distinguish Cyberspace from the global commons is that the sea, like other global commons (namely Antarctica and Outer Space), is uninhabitable.[472] While there is vocabulary for transient seafarers, there is no corresponding concept of a permanent seakind.[473] As was argued in Chapter 2, Cyberspace has population. It has transitory surfers,[474] but it also has permanent netizens, many of whom are digital natives. Schmitt's thesis requires inhabitability, because spatial division is entangled with the demarcation of inhabitation. Implicit to Schmitt's theory is the idea that there

---

[472] Uninhabitability, here is meant in the a historical sense. Technology can change the inhabitability of an area and as a result there small populations that do exist in global commons (e.g. science outposts in Antarctica, the *International Space Station*, or Sealand and other ocean platforms).

[473] A Google search returned no pages discussing any notion of seakind. There is a corresponding notion of spacekind however. *See generally* George Robinson, "Astronauts and a Unique Jurisprudence: A Treaty for Spacekind," 7 *Hastings Int'l & Comp. L. Rev.* 483 (1983-1984).

[474] The use of an ocean metaphor here should not be overlooked as it certainly indicates the non-permanence that Schmitt is addressing in his assessment of the high seas.

is a community of inhabitants that inscribe borders onto land.[475] However the digital native represents "a more mobile kind of legal person."[476]

Cyberspace on the other hand has inhabitants and communities that exist within its borders.[477] This forces consideration of legal concepts such as self determination and human rights, because "for there to be principles and practices of legitimacy, there needs to be a community/society."[478] The important implication of a group of "digital natives" is that the world's population will be increasingly dominated by users who have always understood space as shaped by Cyberspace. Digital natives will not experience Cyberspace as an alternate geography any more that Native Americans experienced the the Americas as "new world." Digital natives understand Cyberspace as part and parcel of their geography.[479] The implication is that there is a shift happening in how the world is spatialized; a shift that is deeply implicated with interoperability.

III. Nomos

Schmitt's object is to prove that international law itself is based on the basic question of spatial division. It is "a primary criterion embodying all

---

[475] Schmitt, *Nomos of the Earth*, 42 ("human toil and trouble"; "worked by human hands"; "orientations of human social life")
[476] Johnson & Post, "Law and Borders," 1400.
[477] Julian Assange et al., *Cypherpunks,* 155 (". . . but we don't understand ourselves as living in Germany, we understand ourselves as living on the internet, which is perhaps a big part of our self-understanding . . .").
[478] Clark, *Legitimacy in International Society*, 6, 149.
[479] In other words, digital natives "describe [themselves and their relationships] in ways that fit the preordained limitations" of the network architecture. Power & Tobin, "Soft Law for the Internet," 43 (quoted text in original used to describe social construction within social media software).

subsequent criteria,"[480] and "*nomos"* is the immediate form in which the political and social order of a people becomes spatially visible."[481] Schmitt compresses spatial and legal geography into a single layer.[482] In conjunction with his *Concept of the Political*, which compresses legal geography and political geography, Schmitt reads territory as an essential agent of law and politics. Schmitt's analysis is chosen for critique specifically due to this essentialness, because it is the question of territory that sits at the heart of the debate on the nature of Cyberspace. Schmitt's "terrestrial fundament" presents a fulcrum point from which to base conceptualization, because to understand Cyberspace as an alternative geography, we must first accept the enduring and historically constructed nature of our own physical boundedness.[483] The task is not necessarily one of debunking Schmitt or of supporting Schmitt, but instead seeking an understanding of Cyberspace that resolves the dissonance in the perceptions of geography and alternate geography and, instead, understanding them as a single networked geography. This requires investigation into how the *nomos* of Cyberspace shapes the *nomos* of the Earth. Or, in other words, how does Cyberspace reinscribe borders and transform geography on a world scale. If *nomos* is to be understood as the "form in which the political and social order of a people becomes spatially visible," then a *nomos* of Cyberspace should be visible.[484]

---

[480] Schmitt, *The Nomos of the Earth,* 45.
[481] *Id.* at 70.
[482] *Id.* at 45 (arguing that land appropriation has a "categorical character" and is "the primary legal title that underlies all subsequent law.") and *Id.* at 70.
[483] *Id.* at 47.
[484] *Id.* at 70

The analysis in the *The Nomos of the Earth* is one that is concerned with change. While Schmitt ties territory to law, he recognizes that a diversity of spatial orders can orient that space. The essential link between territory and law is not to be confused with an argument that the state is the natural unit for global organization. Schmitt clearly recognizes that "new spatial phenomenon" can change the spatial order, and he notes that human extension into airspace means that "firm land and the free sea are being altered drastically, both in and of themselves and in relation to each other."[485] He observes that this technology is not just changing the "efficacy and velocity of the means of human power, transport, and information" but the "content of this *effectivity*."[486] Technology in his account can have a transformative effect on the organization of law, and not as an external factor. Technology becomes an endogenous factor that shapes the content of the spatial order itself.

Schmitt exposes that spatial understandings are deployed by technology. Observing this phenomenon proves more elusive as Cyberspace is complex and expansive. Its networked nature means that it is a system with no exact size or shape. Additionally, it pervades social interaction at a scale that makes generalizations about transactions in Cyberspace severely limited. A natural place to observe border re-coding is at the geographic borders: spatial, legal, and political. Those borders can reveal how Cyberspace pushes up against the international as its territorial geography thins and runs out, and it is these

---

[485] *Id.* at 48. Despite Schmitt's recognition of "new spatial phenomenon," he still considered "land-appropriation of the Earth's soil to be "fundamentally significant." *Id.* at 80.
[486] Schmitt, *The Nomos of the Earth,* 48.

places of abutment and intersection that exhibit the fault lines from which global space is emerging.

The geographic categories used in Part I correlate to the components that Sassen argues are "assembled" into governance structures. She argues that world organizing logic can be understood through the assemblage of territory, authority, and rights, and that across history global systems are constructed and reconstructed as assemblages of these three components.[487] These components serve as points of analysis from which to observe the particular conditions within a world scale system of governance.[488] While Schmitt and Sassen would likely not see eye-to-eye in substance, their arguments both embrace a an understanding that international space is capable of being reconceptualized.

International space is constructed around a myth of Copernican-esque systems: territories with a centralized governments that hold authority are the building blocks of international space. States are actors and subjects within this space and they are given rights based on an organizing logic that aligns high degrees of legitimacy with the occupation of territorial space. Pre-1945 states were the rights bearers in International law. Post Nuremberg and the Universal Declaration of Human Rights, individuals became limited rights bearers in the international order.[489] This reallocation of rights is reflected in the noble mission of the UN, but events such as the Rwandan genocide serves as grim reminders of the concentration of state power over territory despite the

---

[487] Sassen, *Territory, Authority, Rights,* 18.
[488] *Id.* at 32.
[489] *See* Donnelly, "Human Rights," 14.

1945 reallocation of rights. Scholarship in international legitimacy portrays these allocations in terms of rightful membership.[490] This scholarship has traced a growing trend in international legitimacy of placing increasing emphasis on rightful action by the state. This shifts the gaze of international governance from the border to the interior of the state by allocating international right to citizens. Despite this re-allocation the state remains the primary arbiter of human rights as a result of low degrees of enforcement despite strong international rhetoric."[491]

If Cyberspace is indeed opening up global geography then it should be observable in international space through the reallocation of territory, authority, and rights in the international assemblage. There should be observable points where the geography of the international runs out and borders Cyberspace. When the geography of Cyberspace is layered onto the geography of international space it should reveal a networked space which "[runs] in many dimensions."[492] As Habermas observes, "'[n]etwork' has emerged as a key term."[493] Space ordered through the network constitutes a "new spatial phenomenon," which should be observable in the key institutions of the international order. To continue the cartographic metaphor adopted in the beginning of this chapter, by layering cybergeography onto international

---

[490] Jean-Marc Coicaud, "Deconstructing International Legitimacy," in *Fault Lines of International Legitimacy*, ed. Hilary Charlesworth and Jean-Marc Coicaud (Cambridge University Press, 2009), 37, Donnelly, "Human Rights," 2; Clark, *Legitimacy in International Society*, 2; and Rajan Menon, "Pious Words, Puny Deeds: The 'International Community' and Mass Atrocities," *Ethics & International Affairs* 23, no. 3 (September 1, 2009) 237.
[491] "never again"
[492] Habermas, *The Postnational Constellation,* 66.
[493] *Id.* at 66.

geography, we should be able to observe the distortions in the projection of the world.

New assemblages often incorporate aspects of historical predecessors embedding these into the construction of new assemblages.[494] Cyberspace is a paradigm shift, but despite this, much of the international system remains in tact and will continue to remain in tact. Cyberspace, as an alternative geography, is still "filtered through local languages and meaning systems."[495] This means that the international will remain a powerful forcedespite the spatial shift. International space, as a geography, can also be understood to be "filtered" through the languages and meaning systems of Cyberspace.

Part II of this research will take the geography described in Part I, and use it as conceptual map that can be juxtaposed to the map offered by the international. These maps will be layered together to explain observable points where Cyberspace changes the geography of the International. Using Sassen's vocabulary of territory, authority, and rights, the thematic case studies presented in the following chapters will analyze how geographies in real space are warping as they come into contact with Cyberspace. Chapter 6, will approach territory from the perspective of transnational cyber conflict, and will examine the idea of "territorial integrity" in terms of the cyber use of force. Chapter 7 will investigate how Cyberspace redistributes authority through an examination of IOs, IGCs, and corporations that make architecture decisions in Cyberspace. This chapter will show that the concept of global

---

[494] Sassen, *Territory, Authority, Rights,* 3-6; *see also* Ferguson & Mansbach, *Globalization,* 69 ("embedded past") and Burbank & Cooper, *Empires*, 8 ("memory of power").
[495] Ferguson & Mansbach, *Globalization,* 205.

multi-stakeholder governance shifts a great deal of authority to outside of the borders of the international. Finally, Chapter 8 will explore how Cyberspace transforms the individual's rights in relation to the state. This chapter will use the cryptography and surveillance to illustrate how rights have been reallocated in the context of Cyberspace. These three case studies taken together will show the contours of re-coded borders as they unfold in Cyberspace.

Part II
Encountering with the Digital

"I think I never before quite realized the place of the fence in civilization."

- W.E.B. Du Bois

Chapter 6

Conflicting Territories

In May of 2013, Cody Wilson printed a working gun with a 3d printer and fired it.[496] Shortly thereafter he made the computer file, a set of instructions allowing and 3D printer to print what he called the Liberator, available online for download. It was downloaded more than 100,000 times before Wilson removed the file.[497] Little did Wilson know that he was running afoul of the United States' International Traffic in Arms Regulations (ITAR). These regulations prohibit the export of "defense items" - in other words: weapons - found on the United States Munitions List (USML) without authorization from the government.[498] It also, significantly, prohibits the export of "technical data" on these items, which is data that would assist in allowing someone to manufacture the prohibited item.[499] Wilson's file was in a standard language that would allow anyone with an Internet connection to download it and use a 3D printer to manufacture a gun. The file, since it was on the Internet was downloadable anywhere in the world, and as a result Wilson removed the file from his website.[500]

---

[496] Jacob Silverman, "A Gun, a Printer, an Ideology," *The New Yorker*, May 7, 2013, http://www.newyorker.com/tech/elements/a-gun-a-printer-an-ideology.
[497] Carole Cadwalladr, "Meet Cody Wilson, Creator of the 3D-Gun, Anarchist, Libertarian," *The Guardian*, February 10, 2014, sec. Technology, http://www.theguardian.com/technology/2014/feb/10/cody-wilson-3d-gun-anarchist.
[498] 22 C.F.R. 120.
[499] 22. C.F.R. 120.6.
[500] Carole Cadwalladr, "Meet Cody Wilson, Creator of the 3D-Gun, Anarchist, Libertarian," In May of 2015, he sued the United States Government for impinging on his freedom of Speech. Alan Feuer, "Cody Wilson, Who Posted Gun Instructions Online, Sues State Department," *The New York Times*, May 6, 2015,

Three years later Wilson's file is still online and freely available through sources like the Pitrate Bay to those that want to download it.[501] Wilson started a company called Defense Distributed, which now manufactures a product called the Ghost Gunner.[502] This desktop CNC mill will take a block of aluminum and mill a lower receiver for an AR-15.[503] Wilson's product cannot be exported, and the computer file is sold on the website so that only United States citizens can buy it, so this product does not run afoul of ITAR. It does on the other hand effectively digitize a gun, which lowers the barriers to access. The gun that it creates is of high quality, and is a gun that is outside of the regulatory loop; it is an untraceable "ghost gun."[504] And while Wilson is keeping tight control over the "technical data" in the .cad files that allow the machine to manufacture the part, he has opened source the machine itself so that the plans for the hardware and the software that runs it are freely downloadable.[505] Anyone with these files can develop new design files for the Ghost Gunner, and enable it to make a various guns as well as a variety of other things. Defense has been distributed, digitally..

The Ghost Gunner is interesting because it shows the capacity of the state to lose control over violence in two ways. First, it lowers the barriers to the production of the means of violence, which weakens government control

---

http://www.nytimes.com/2015/05/07/us/cody-wilson-who-posted-gun-instructions-online-sues-state-department.html.

[501] Andy Greenberg, "I Made an Untraceable AR-15 'Ghost Gun' in My Office—And It Was Easy," *WIRED*, June 3, 2015, http://www.wired.com/2015/06/i-made-an-untraceable-ar-15-ghost-gun/.

[502] *Id.*

[503] Guns are made up of many parts. The lower receiver is the component that is regulated under the US law. *Id.*

[504] *Id.*

[505] CNC mills are not on the USML. Defense Distributed, "Downloads," https://defdist.org/downloads/ (last visted Feb. 17, 2016).

over violence. It is legal under federal law for an individual to manufacture a lower reciever, but it was a time consuming process and required a high level of skill.[506] The Ghost Gunner makes gunmaking a plug-and-play venture. Second, and important to the discussion below, it shows that the state no longer has control over the spread of violence at its borders. ITAR is specifically meant to help maintain international peace and security by restricting the export of munitions to countries or persons that might use them for ill. ITAR is directly related to the international project of bracketing war, by cutting off the supply of armaments. The ITAR correlates to regimes such as the Wassenar Arrangement[507] and the Arms Trade Treaty.[508] These initiatives are mechanisms used to stop the flow of armaments across their borders, which was easy when armaments needed to be carried on trucks. Ghost guns are digitized, just as lethal, and save on the shipping cost.

This chapter investigates how Cyberspace changes the nature of territory by examining how Cyberspace changes international conflict. Schmitt's claim "that law and peace originally rested on *enclosures in the spatial sense*" is particularly salient here as it highlights the role of borders in conflict prevention.[509] In Schmitt's territory-centric conception of international law, war is "bracketed" to locations such it does not "disturb" the spatial order.[510] This chapter will probe this bracketing war, and illustrate the diminished importance of the border in constructing the the space of conflict.

---

[506] Andy Greenberg, "I Made an Untraceable AR-15 'Ghost Gun' in My Office."
[507] Wassenaar Arrangement, "About Us," http://www.wassenaar.org/about-us/ (last visited Feb. 17. 2016)
[508] Arms Trade Treaty (entered into force Dec. 24, 2014).
[509] Schmitt, *Nomos of the Earth*.
[510] *Id.* at 186.

The argument here is not meant to be a "dethroning of Clausewitz," but it does argue that Cyberspace dramatically changes the context of international conflict through the subversion of territorial borders.[511] In short, it argues that armed conflict as conceived in the international system is tied to territorial geographies, and that international governance mechanisms that are meant to minimize international armed conflict are structured around this link. The chapter will then shows how the concept of cyberwar dislodges conflict the territorial link, which makes the application of norms meant to control international violence unable to effectively bracket it. Section one of this Chapter will use Stuxnet attack on Iran's centrifuges to analyze how international law has traditionally dealt with war as well as some of the observable gaps in that regime. This section will show how Cybebrspace dislodges territory from the governance of international armed conflict. The second section will analyze the role of the international concepts of disarmament and deterrence in limiting cyber conflicts, and it will show that these mechanisms are ill equipped for placing substantive limitations on cyberweapons. Finally, it will use the the North Korea-Sony hack to show how international politics become deterritorialized and distributed in Cyberspace, which means that international conflicts processed through Cyberspace become deterritorialized as well.

I. Territorial Integrity

---

[511] David J. Betz, "Clausewitz and Connectivity," *Infinity Journal* 3, no. 1 (March 2013), https://www.infinityjournal.com/article/84/Clausewitz_and_Connectivity/. *See also* Betz & Stevens, *Cyberspace and the State,* 12.

At the heart of the post-1945 settlement is the UN charter's Article 2(4), which prohibits "the threat or use of force against the territorial integrity or political independence of any state."[512] This article sought to for the first time to create a legal prohibition against interstate armed conflict.[513] Article 2(4) and the UN Charter in general were transformative for international law as it enshrined the state as "the arena within which self-determination is worked out and from which, therefore, foreign armies have to be excluded."[514] For the first time the resort to war, characterized in the Charter as the "use of force," was generally prohibited outside of a few exceptions.[515] Article 2(4) compartmentalizes violence within the borders of a state and gives the state sovereignty over violence within its borders. This compartmentalization, or "bracketing" as Schmitt would call, it not a new process. The bracketing of war was an act of recognizing order from chaos, and Schmitt's project is to show how the international spatial order emerged the externalization of war. So for instance, he notes that during the age of European empires violence was pushed to the peripheries of empires by conceptualizing newly found territories as existing outside of the Western-centric international legal system.[516] Article 2(4) represents a new bracketing of war by conceptualizing every state as an inviolate territory of order. States in this new spatialization were connected to

---

[512] UN Charter 2(4).
[513] Previous attempts had been more political in nature. *See generally*, Cornelis Arnold Pompe, *Aggressive War - An International Crime* (Martinus Nijhoff, 1953) 12, 160-64.
[514] Walzer, "The Moral Standing of States," 210.
[515] For those exceptions see UN Charter Art. 42, 51.
[516] Schmitt, *The Nomos of the Earth,* 101-125.

law both internally and, importantly, externally in a legal dynamic between de facto control and external recognition.[517]

Art. 2(4) did not change extant borders in a way that was perceptible on a map. Nonetheless, Art. 2(4) did change the content of those borders, and in a very dramatic way. By giving all states an obligation to contain violence within their borders, it also gave all states the right to be free of chaos from outside their borders. Article 2(4) underpins the entire international legal regime meant to contain international armed conflict. The Art. 2(4) prohibition on force is central to *jus ad bellum,* and its goals are further advanced through the *jus in bello* and international disarmament efforts. While the core goal of "international peace and security" found in the UN Charter could be said to hinge on Art. 2(4),[518] when Art. 2(4) is understood as a spatial order to bracket war and silo it into territories of disorder there are important implications across a large swath of international governance mechanisms. Cyberspace by recoding borders changes their ability to bracket digitized war.

The best place to start to unravel this problem is Stuxnet. Stuxnet presents a clear case for the application and analysis of International Law. In 2010, researchers uncovered a computer virus that was propagating itself on computers in Iran.[519] The virus, which came to be known as Stuxnet, was a carefully developed computer program which wound its way into computers in the Natanz nuclear facility in Iran. Once there the malware attacked industrial control systems and executed a program that sped up uranium enrichment

---

[517] *See generally* Coicaud, "Deconstructing International Legitimacy," 29–86.
[518] UN Charter 1(1).
[519] *See generally* Kim Zetter, *Countdown to Zero Day : Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown Publishers, 2014) Chap. 1.

centrifuges to damage and destroy them before the end of their expected limetime. The program itself "displayed a level of technical sophistication and integration never before seen in malware,"[520] and it has been referred to as the"world's first digital weapon."[521] The sophistication of Stuxnet was such that it incorporated four zero days, and was able to jump an air gap that separated Nantanz from the Internet.[522] The program was reportedly developed and released by the United States and Israel as a way to slow the Iranian nuclear program down.[523] For the purposes of the discussion below, it is assumed that this is a state on state act, placing it firmly within the realm of the international system, making international law the controlling governance mechanism. This raises the "principle intellectual challenge in the law of information conflict . . . deciding which areas can be covered by a mere extension of conventional legal principles to cyberspace by analogy, and which require whole new methodologies."[524]

The first question to be asked is whether there has been a violation of Article 2(4). If the United States or Israel had flown a plane across the border and bombed the plant, as Israel did to a Syrian facility in 2007, then we can see

---

[520] Eric P. Oliver, "Stuxnet: A Case Study in Cyber Warfare," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton: Taylor & Francis, 2013) 129.
[521] Kim Zetter, *Countdown to Zero Day : Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown Publishers, 2014) 3
[522] Eric P. Oliver, "Stuxnet: A Case Study in Cyber Warfare," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton: Taylor & Francis, 2013), 143.
[523] William J. Broad, John Markoff, and David E. Sanger, "Stuxnet Worm Used Against Iran Was Tested in Israel," *The New York Times*, January 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.
[524] Thomas C. Wingfield, "Legal Aspects of Offensive Information Operations in Space," 1998, http://www.au.af.mil/au/awc/awcgate/dod-io-legal/wingfield.pdf 1.

that there has clearly been a violation of article 2(4).[525] In this case however, there was no physical violence in a ballistic sense, however, violence was achieved in a kinetic sense in that the centrifuges themselves were physically manipulated in order to destroy them. The centrifuges were attacked, but it is unclear whether this amounts to a use of force under article 2(4).[526] The *Tallinn Manual on the International Law Applicable to Cyber Warfare*'s Rule 11 states that "[a] cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."[527] The *Tallin Manual* is an attempt by a NATO group of experts to identify "the law currently governing cyber conflict,"[528] but it notes that "the lack of agreed-upon definitions, criteria, and thresholds for application creates uncertainty when applying the *jus ad* bellum."[529] When compared to a statement by US defense official on the United States Cyber Strategy, who stated "If you shut down our power grid, maybe we will put a missile down one of your smokestacks," it seems as if one of the parties has characterized attacks such as Stuxnet as a use of force.[530] The *Tallin* manual experts themselves

---

[525] Zetter, *Countdown to Zero Day,* 192, 215-216.

[526] Kallberg and Burk argue that an attack on industrial control systems, such as those attacked by Stuxnet, to achieve environmental damage would arise to an "act of war." Jan Kallberg and Rosemary A. Burk, "Cyberdefense as Environmental Protection - The Broader Potential Impact of Failed Defensive Counter Cyber Operations," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton: Taylor & Francis, 2013), 265–75.

[527] Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013) 45.

[528] *Id.* at 5.

[529] *Id.* at 42. *See also* Libicki who calls this "indeterminism." Libicki, "Two Maybe Three Cheers for Ambiguity," 30. Dipert suggests the development of an "ontology for cyberwarfare." Randall R. Dipert, "The Essential Features of an Ontology for Cyberwarfare," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton: Taylor & Francis, 2013), 35–48.

[530] Siobahn Gorman and Siobhan Gorman And Julian E. Barnes, "Cyber Combat: Act of War," *Wall Street Journal*, May 31, 2011,

agreed unanimously that Stuxnet was a use of force that violated international law, but they "split . . . on whether it constituted an armed attack."[531] This split illustrates the disjunctures that occur when international law is deterritorialized. The separation of "use of force" from "armed attack," categories that were previously substantially concurrent due to the nature of violence, is indicative of the encounter between international and cyber geographies.

Interestingly, Iran never made any complaint to the UN General Assembly nor the United Nations Security Council, instead opting to maintain a high degree of silence on the matter. Iran's silence is related to its own interests in keeping its nuclear program secret, but it also points to one of the key lesson from Natanz: everyone knows that the United States and Israel were responsible for Stuxnet, but no one can prove it definitively. This is dissimilar from United States covert involvement in Nicaragua which the ICJ deemed a use of force.[532] In that case there were physical border crossings by the United States and its warfighting capacity that were observed by witnesses to physical attacks.[533] In the case of Stuxnet, no one saw the attack There is ample evidence pointing the finger at the United States and Israel: the complexity of

---

http://www.wsj.com/articles/SB10001424052702304563104576355623135782718., *See also* David E. Sanger and Elisabeth Bumiller, "Pentagon to Consider Cyberattacks Acts of War," *The New York Times*, May 31, 2011, http://www.nytimes.com/2011/06/01/us/politics/01cyber.html. *See also* Benjamin H. Friedman and Christopher A. Preble, "A Military Response to Cyberattacks Is Preposterous," *Cato Institute*, June 2, 2011, http://www.cato.org/publications/commentary/military-response-cyberattacks-is-preposterous.

[531] Zetter, *Countdown to Zero Day* , 402.

[532] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986, p. 14.

[533] *Id.* at para. 22.

programming, the target of the attack, the use of high value zero day vulnerabilities, and anonymous sources to journalist all point to the US and Israel. There is, however, no definitive evidence of that fact, and the United States has officially made no statement confirming its involvement resting on the plausible deniability that Cyberspace provides.[534] Digital computing enables the ability to encrypt communications and to hide the source of cyberattacks. Even if a cyberattack were to be traced to an IP address within a state, that state can claim that it is the victim of a hacker using it as a digital hiding spot or that one of its own citizens is the malefactor for which there carry limited responsibility. US DoD acknowledges this potential by noting that "low barriers of entry . . . means that an individual or small groups of determined cyber actors can potentially cause significant damage."[535] In the case of Stuxnet, the virus was feeding information back to servers located around the world.[536] Attribution is a core concept in International law. This is because for a wrongful act to also be an internationally wrongful act it must be an act of the state or attributable to the state.[537] The Draft Articles on State Responsibility state that "conduct directed or controlled" by a state is attributable to it, but this requires the establishment of a definitive link that proves such. In Cyberspace such links are hidden by veils of government secrecy, including secrecy classification systems and digital veils of encryption, and making it difficult to attribute an act to the territory of a state much less to

---

[534] McDermott, "Decision Making Under Uncertainty," 234. Edward Snowden, "Testimony before the Parliament of the European Union," 4.
[535] US DoD, "Department of Defense Strategy for Operating in Cyberspace," 3.
[536] Zetter, *Countdown to Zero Day,* 27.
[537] Draft Articles on the Responsibility of States for Internationally Wrongful Acts 53 UN GAOR Supp. (No. 10) at 43, U.N. Doc. A/56/10 (2001) Art. 2.

the state itself.[538] Attribution is a necessary precondition for an international response, but it "is an enduring problem" in Cyberspace.[539] The attack, though initiated from some specific geographic point, is experienced as coming from Cyberspace. Cyberspace as an origin for an attack is supported by the military adoption of Cyberspace as a fifth domain.[540]

This fifth domain remains outside of international space, and it obscures the geographic links to force, which borders are meant to prevent.[541] This creates an obvious problem for stability built around the centrality of a sovereign's territorial integrity in the international system, since International borders no longer separate order from chaos when anonymized weapons can pierce pierce borders and affect physical infrastructure. The plausible deniability enabled by Cyberspace means that states are, in part, relying on the prevalence of non-state actors dispersed around the globe to create noise that covers their tracks. National defense is distributed among a network of indistinguishable actors.

Before moving on from Stuxnet, it is worth noting how this incident reflects on the *jus ad bellum*'s counterpart the *jus in bello*.[542] *Jus in bello*, or international humanitarian law (IHL), is not without problems of application,

---

[538] On the problem of attribution in Cyberspace see Clark & Landau, "Untangling Attribution."
[539] Zetter, *Countdown to Zero Day,* 64. *See generally* Collin S. Allan, "Attribution Issues in Cyberspace," *Chi.-Kent J. Int'l & Comp. L.* 13 (2013): 55–201.
[540] US DoD, "Department of Defense Strategy for Operating in Cyberspace," 5.
[541] *Id.* at 8 (challenges caused by Cyberspace "extend across national boundaries") and Department of the Army, "FM 3-38: Cyber Electromagnetic Activities," February 12, 2014, http://library.blountsfolly.com/space/items/show/194 1-4.
[542] It should be noted that there is also a concept of *jus post bellum* that is also implicated in unattributable cyberattacks, but at present this area is more moral than normative. O'Meara, Richard M. "Jus Post Bellum: War Closure in the 21st Century." In *Routledge Handbook of Ethics and War: Just War Theory in the 21st Century*, edited by Fritz Allhoff, Nicholas G. Evans, and Adam Henschke, 105–19. Routledge, 2013.

but it does seem that it is more adaptable to cyber conflicts.[543] This is primarily because IHL is not centered on questions of territory. Instead, IHL focuses on humanitarian concerns such as the limitation of pain and suffering for civilians and combatants. It is a *lex specialis* that only applies within the space and time of an international armed conflict.[544] As such, IHL principles are a bit more adaptable to Cyberspace, but they are not without gaps.

For instance, in the case of Stuxnet, it is unclear whether there was an ongoing state of armed conflict that would trigger IHL. Though the attacks occurred over the course of several months, Iran was unaware, and when it became aware it did not respond with force nor through any official channels. Despite the lack of clarity as to whether the rules had been triggered, there is evidence that the programmers of Stuxnet worked hard to make sure that it fell within the legal limits of a weapon. States when developing new weapons technologies are required to give the weapon a legal review to ensure that it is a weapon that can be used legally.[545] This review must assess whether the weapon is capable of being targeted at a specific target such that its effects, in terms of collateral damage to civilians, are limited in proportion with the military advantage gained[546] as well as whether the weapon causes unnecessary

---

[543] Dunlap, "Perspectives for Cyberstrategists on Cyberlaw for Cyberwar," 212 ("the tenets of LOAC are sufficient to address the most important issues of cyberwar."). *See also* Department of the Army, "FM 3-38: Cyber Electromagnetic Activities," (noting throughout the role of military lawyers in cyber electromagnetic operations).

[544] Yoram Dinstein, *The Conduct of Hostilities Under the Law of International Armed Conflict* (Cambridge University Press, 2004) 1-16.

[545] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) (June 8, 1977) Art. 36. *See also* P. J. Blount, "The Preoperational Legal Review of Cyber Capabilities: Ensuring the Legality of Cyber Weapons," *Northern Kentucky Law Review* 39, no. 2 (2012) 11–20.

[546] Gompert and Saunders refer to this as a critical question. Gompert & Saunders, *Paradox of Power,* 126

suffering.[547] The first thing to note is that this review cannot be done in terms of "cyber weapons" as a class any more than it can be done of "ballistic weapons" as a class. Instead, the analysis is capability by capability which is confirmed by a US Air Force Instruction on the legal review of cyber capabilities.[548] What Stuxnet's code revealed is that the programmers went to great lengths to infect only specific computers. Stuxnet was equipped with a kill switch that deleted it if the computer did not match very specific conditions.[549] The "missile" portion of the program replicated itself across computers, but was designed to only release its payload, which targeted industrial control boxes, in the Natanz facility.[550] Though the weapon was released through attacks on networks of private Iranian companies, the damage caused minimal threat to human life or civilian property.[551] The weapon itself was designed to work with precision, but it must be remembered that generally "[c]ollateral damage in Cyberspace has a longer reach than in the physical realm."[552] There are other complications with the application of IHL, many of these are simply that: complications. They change the context of humanitarian principles and make the issues more complicated, but IHL would have means of filling the gaps since the regulatory focus in on human lives. For

---

[547] *See generally* Dinstein, *The Conduct of Hostilities Under the Law of International Armed Conflict*, 80-82.
[548] United States Air Force, Legal Reviews of Weapons and Cyber Capabilities, A.F. Instruction 51-402 (July 27, 2011).
[549] Kim Zetter, *Countdown to Zero Day,* 59.
[550] *Id.* at 52.
[551] *Id.* at 388.
[552] *Id,* at 382. Zetter does note that the "only limitation Stuxnet had were on where it ignited its payload, not where it spread." *Id.* at 352. On targeting in cyberspace see Department of the Army, "FM 3-38: Cyber Electromagnetic Activities," 3-11 - 3-12.

instance, the issue of who constitutes a combatant becomes more complicated, but is a problem that it solvable within the imagination of the IHL framework.

Others rifts are deeper. A critical concern for IHL is the military use of civilian objects. All Cyberspace attacks will depend on the use of civilian infrastructure, but Stuxnet illustrates state cyber attacks will often do more than just transit commercial networks. In order for Stuxnet to work it had to take advantage of zero days. These are vulnerabilities in software that are unknown to the programmer and as a result are not patched.[553] Zero days are unknown vulnerabilities. When an individual discovers a zero day, he or she has a few choices of what to do with that information. Some companies have a bounty system in place to buy zero days; there is a healthy black market for zero days; and Governments will also buy them.[554] Stuxnet had an unprecedented number of zero days in its programming.[555] This means that a government left open vulnerabilities in commercial software with the potential to put a multitude of devices at risk. Stuxnet also used fake security certificates that marked it as genuine so it would be accepted by the systems on which it installed itself.[556] These digital certificates are issued by companies that rely on strong encryption in order to verify that a piece of software is from where it says its is from. Stuxnet and its kin exploited these mechanisms thereby damaging the trust system used to verify software across the internet.[557] This means that these weapons rely on the maintenance and exploitation of

---

[553] Zero days are "the hacking world's most prized possession. Zetter, *Countdown to Zero Day,* 6.
[554] *Id.* at 13.
[555] Eric P. Oliver, "Stuxnet," 129.
[556] Zetter, *Countdown to Zero Day,* 13.
[557] *Id.* and DeNardis, *The Global War for Internet Governance*, 95.

vulnerabilities in the commercial infrastructure that underpins the Cyberspace at a global level.[558] While Stuxnet limited the effects of its attack, another state or entity using similar vulnerabilities might not limit such an attack, a point sharpened when it is recognized that computers similar to those found in Natanz are used to run a great deal of critical infrastructure such as power grids and dams.[559]

Stuxnet is a powerful portent for the international system,[560] and, though some authors wisely note the limitations of cyberwar,[561] Stuxnet is a well documented example of a computer attack that was used to manipulate and destroy a physical object from afar. What is striking about Stuxnet is the difficulty of placing it squarely within the international legal system. This is because weapons like Stuxnet defy the spatial geography of states. These weapons instead allows states to project force through the alternate geography of Cyberspace, allowing them to skirt around borders as well as the legal regime that supports those borders.

Stuxnet displays vulnerabilities in the Cyberspace infrastructure that individuals rely on globally. With other weapons of this sort (i.e. those that are

---

[558] Gompert & Saunders, *Paradox of Power,* 142; Fred Taylor, Jr. and Jerry Carter, "Cyberspace Superiority Considerations," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton: Taylor & Francis, 2013), 13–25, 14

[559] Zetter notes that Stuxnet used an "extensive checklist" to ensure it was infecting the proper computers. Zetter, *Countdown to Zero Day,* 61-62

[560] Eric P. Oliver, "Stuxnet," 128 ("Stuxnet served as an existence proof for the theory that malicious software . . . can strategically important, physically destructive effects"). Indeed, the progeny of Stuxnet appeared in early 2016 when a Ukrainian power plant was shut down with malware. *See* Kim Zetter, "Everything We Know About Ukraine's Power Plant Hack," *WIRED*, January 20, 2016, http://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/.

[561] Robert M. Lee and Thomas Rid, "OMG Cyber! Thirteen Reasons Why Hype Makes for Bad Policy," *The RUSI Journal* 159, no. 5 (2014): 4–12.

legal but have global implications such as strategic nuclear weapons) states have turned to methods of disarmament and deterrence as a way to manage international peace and security. These mechanisms, which are meant to lower the risk of an article 2(4) violation, are the subject of the next section.

II. Ghost Guns

The atomic bomb dropped on Hiroshima near the end of WWII ushered in a new age of warfare driven by technological advances that far outpaced previous technology blooms. Nuclear weapons, intercontinental ballistic missile delivery systems, long range stealth bombers, and military satellite systems all widened the ability of states to project force into the territory of other states. States found themselves in a classic security paradox in which the only way to be more secure is to have more and better weapons than one's adversary, leading both parties to actively incentivize their own insecurity.[562] To decrease the risk caused by such paradoxes, states turned to disarmament and deterrence mechanisms in order to implement systems of "reciprocal restraint."[563] As discussed above, ITAR is a domestic implementation of such measures.

Disarmament mechanisms usually come in the form of international agreements that ban the development and use of certain weapons, or limit the number of a particular type of weapon that a state may have.[564] Disarmament

---

[562] Gompert & Saunders, *Paradox of Power*, 1-12..
[563] *Id.* at 115.
[564] Disarmament mechanisms are not always necessarily "legal" documents. Transparency and confidence building measures (TCBMs) that facilitate information sharing among states, such as the Hague Code of Conduct on Ballistic Missile Activities, also serve the project of

mechanisms are underpinned by verification. Verification is the act of verifying whether or not a party is complying with the agreement. The importance of verification to disarmament can be seen in Reagan's signature quip: "trust, but verify."[565] Without verification disarmament agreements tend to be weak and difficult to negotiate. States have traditionally relied on national technical means (NTM) in these agreements as a form of verification, which consist of satellite observation in addition to other types of remote sensing.[566] NTM was an excellent way to verify nuclear disarmament agreements, and the US and the USSR were able to rely on satellite observation as a mechanism for verification since nuclear armaments were by their nature quite large. As a result, NTM worked well in forging compromises between the two states as they sought to securely reduce their nuclear stockpiles. It should be noted that "[b]ecause disarmament treaties go to the heart of national and international security, states are wary of frivolously embarking on new ones that might constrain their options."[567]

Deterrence is a companion to disarmament. Whereas disarmament seeks to reduce the munitions through reciprocal restraint, deterrence is a method of reducing the risk that a state might use those weapons. [568] It is a policy designed to "discourag[e] an adversary from doing something it might

---

disarmament. *See generally* Hague Code of Conduct against Ballistic Missile Proliferation (November 25, 2002).

[565] Roger Harrison, *Space and Verification, Volume I: Policy Implications* (Eisenhower Center for Space and Defence Studies 2007) .

[566] Forrest E. Morgan, "Deterrence and First-Strike Stability in Space: A Preliminary Assessment" (DTIC Document, 2010) 9-11.

[567] Trevor Findlay, "Why Treaties Work, Don't Work and What to Do About It?" (Canadian Institute of International Affairs, January 25, 2006), http://carleton.ca/npsia/wp-content/uploads/ciia_present_06.pdf.

[568] Morgan, "Deterrence and First-Strike Stability in Space," 23 ("Deterrence was the central pillar of U.S. Strategic thought from the late 1940s until the end of the Cold War.")

otherwise choose to do by manipulating its calculation of cost and benefit."[569] For example, China's current policy of no first use of nuclear weapons is coupled with a stockpile of weapons that would not assure success in a nuclear conflict, but would be able to survive first strike and inflict unacceptable losses on an adversary thereby deterring an attack.[570] Deterrence can also be attained through international agreements. The Anti-ballistic Missiles Treaty (ABM Treaty) is an example of such an agreement.[571] The US and the USSR, unable to compromise on the reduction of strategic nuclear weapon agreed on a disarmament treaty that reduced the deployment of defensive systems. The ABM Treaty ensured mutually assured destruction (MAD), a concept that restrains states from engaging in an attack because any such attack will result in their own demise. Thus, the ABM Treaty is an agreement that imposes disarmament in order to achieve mutual deterrence.

Traditionally, disarmament and deterrence have been the go to mechanisms for stemming armed conflict before it happens by placing limits on a state's recourse to force. Naturally, numerous commentators have turned to these concepts as a way to reduce the threat posed by cyber-attacks and cyber weapons. Gompert and Saunders argue that there are lessons from nuclear deterrence that could be deployed to foster "mutual restraint" in Cyberspace.[572] Yannakogeorgos and Lowther argue that US policy "suffers from a misperception that cyberspace is a virtual environment and as such,

---

[569] *Id.* at 24.
[570] Gompert & Saunders, *Paradox of Power*, 39-67.
[571] Treaty Between The United States of America and The Union of Soviet Socialist Republics on The Limitation of Anti-Ballistic Missile Systems (ABM Treaty) (May 26, 1972).
[572] Gompert & Saunders, *Paradox of Power*, 115-150.

eliminates discussion of territory and sovereignty."[573] They argue that international norms can be developed to solve the attribution problem by holding states culpable for cyberattacks "originating in or transiting information systems within their borders," but they give no indication of why states would agree to such an extraordinary norm.[574]

The problem with these approaches is that they ignore the inherently ambiguous nature of Cyberspace in which weapons are "in essence an algorithm."[575] As an anonymous hacker put it: "The new global arms race is no longer about who controls the most atomic bombs. It is about who controls/owns the most hackers, botnets, and exploits."[576] Zetter claims that just such a "digital arms race" was launched by Stuxnet.[577] Modern disarmament and deterrence were developed by states to deal with weapons of great magnitude, which have traditionally been rather large. NTM, thus was an acceptable form of verification, because it gave states a tool through which they could peer into the borders of another state and literally *see* what that state was doing.[578]

---

[573] Yannakogeorgos & Lowther, "The Prospects for Cyber Deterrence," 50

[574] *Id.* at 51. The only place such a norm exists in International Law is the Outer Space Treaty which holds state internationally responsible for activities by nongovernmental actors. Outer Space Treaty Art. VI.

[575] Dipert, "The Essential Features of an Ontology for Cyberwarfare," 36. *See also* Neil C. Rowe et al., "Challenges in Monitoring Cyberarms Compliance," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton: Taylor & Francis, 2013) 81 ("Cyberweapons are digital objects").

[576] Prisoner #6, "The 21st Century Hacker Manifesto," 50. *See also* Department of the Army, "FM 3-38: Cyber Electromagnetic Activities," 3-11

[577] Zetter, *Countdown to Zero Day,* 370.

[578] Sanger & Bumiller, "Pentagon to Consider Cyberattacks Acts of War." ("Cold War deterrence worked because there was little doubt the Pentagon could quickly determine whaere an attack was coming from")

NTM was an effective tool when addressing physical weapons, because it allowed states to maintain their borders, but it is useless in Cyberspace arms control.[579] Cyberspace diminishes "the horrors and costs of war . . . tempting" countries to resort to the anonymity of of a Cyberattack.[580] The weapons, if designed properly, are meant to invisible and non-detectable so that "the origins of the attack is almost always unclear."[581] In the case of Stuxnet, discussed above, the programmers went to great lengths to make the program hide itself from the users of the targeted systems. This undermines verification, which is a reason for treaty failure."[582] The immaterial nature of cyberweapons means that states can avoid having an attack attributed to them, which is a significant reason that states would resort to cyberweapons. The attribution problem is further complicated by the trend of "privatised intelligence and information warfare."[583] As former Director of the NSA, Michael Hayden notes "applying well-known concepts of physical space like deterrence, where attribution is assumed, to cyberspace where attribution is frequently the problem, is recipe for failure."[584]

---

[579] Zetter, *Countdown to Zero Day,* 400.
[580] Zetter, *Countdown to Zero Day,* 375.
[581] Sanger & Bumiller, "Pentagon to Consider Cyberattacks Acts of War."
[582] Findlay, "Why Treaties Work, Don't Work and What to Do About It?", 4.
[583] Peter Warren Singer, *Corporate Warriors: The Rise of the Privatized Military Industry* (Ithaca, NY: Cornell University Press, 2011) 99, 101. *See also* Jeremy Scahill, *Blackwater: The Rise of the World's Most Powerful Mercenary Army* (New York: Nation Books, 2007) 415 (As the U.S. finds itself in the midst of the most radical privatization agenda in the nation's history, few areas have seen as dramatic a transformation to privatised services as the world of intelligence.").
[584] Hayden, "The Future of Things Cyber," 4. *But see* Thomas M. Chen, "An Assessment of the Department of Defense Strategy for Operating in Cyberspace" (DTIC Document, 2013) http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA586430 6 (arguing that deterrence is dealt with "subtly" in the DoD Cyber Strategy)

Cyber-weapons are by nature covert. They are designed to take advantage of unknown vulnerabilities in computer software, and are meant to be deniable by the country that uses them. Stuxnet used security certificates from Taiwanese countries and the virus reported back the data that it had collected to servers located in a variety of global locations.[585] In fact, it may not have been discovered except for the fact that it caused a malfunction in some non-targeted computers in Iran.[586] As a result, the United States and Israel have never acknowledged their involvement in the attack. For all useful purposes, Iran was struck by a ghost gun - an untraceable weapon that lacks materiality.

The problem with these digital ghost guns, is that they defy location, and as a result they defy control. For example, cyberweapons make use of botnets, which are geographically distributed computers known as bots that are under the control of a single "bot master."[587] Botnets can not be understood to exist within the bounds of a single state, despite the fact that they act as a unitary whole. International governance, a system structured around the national border, is ill equipped to develop disarmament and deterrence mechanisms to control weapons and activities that ignore these borders. Because Cyberspace is everywhere, cyber-weapons "transform[] a limited physical battlefield to a global battlefield."[588] Disarmament and deterrence, as mechanisms are meant to create less ambiguity in international security by creating information about

---

[585] Zetter, *Countdown to Zero Day,* 28.
[586] Zetter, *Countdown to Zero Day,* 7-8.
[587] Generally, the bots are private computers that have been infected with a computer virus. *See generally*, Alana Maurashat, "Zombie Botnets," *SCRIPTed* 7, no. 2 (2010): 370–83, http://www2.law.ed.ac.uk/ahrc/script-ed/vol7-2/maurushat.asp.
[588] Department of the Army, "FM 3-38: Cyber Electromagnetic Activities," 1-5.

armaments that states can act on. As Gompert and Saunders note, "the complexity of computer networks, their myriad, uses, and the many ways of interfering with them could make reciprocal restraint in cyberspace markedly more difficult than in the nuclear and space domain."[589] Cyber-weapons simply do not fit into these mechanisms for a number of reasons.

First, these weapons are immaterial making any sort of verification system difficult and any sort of deterrence ineffective. These weapons can fit on a thumb drive, and can spread through the Internet easily. This make verification virtually impossible as the weapon itself is not tied to any sort of infrastructure and is freely portable. Deterrence on the other hand, which often works on the availability of data about a state's weapons systems, is also precluded. Cyber-weapons rely on vulnerabilities in systems that have not been patched. While disclosing the number and nature of nuclear munitions can have an effect on the strategic maneuvers of other states, the disclosure of a cyber weapon would lead to a software patch that could render the weapon useless. States developing these weapons are only incentivized to keep them covert due to the nature of the technology, and this means that international disarmament and deterrence are not capable of encompassing such technologies.

Second, the plausible deniability that accompanies cyber attacks is an important limitation on a state's ability to comply with disarmament agreements. The nature of the technology that underlies previous disarmament and deterrence mechanisms is such that the state could

---

[589] Gompert & Saunders, *Paradox of Power,* 115

effectively maintain control over those technologies. While history is not without examples of individuals attempting to build nuclear reactors in their garages,[590] the technology was of such complexity and scope that state's were able to detect such operations and maintain control over the development and deployment of these technologies. Cyberspace is a technological space that is built around fostering innovation. As a result, this means that "lone hackers" are empowered to develop new technologies built on the logical layer making it "largely the realm of nonstate entities."[591] Innovation is not always a good thing; it has made the "network attack . . . literally a cottage industry."[592] The same innovative open door that has pushed numerous startups, boosts "the power potential of non-state actors."[593] Indeed, one might argue that the only difference between a computer virus and a cyber weapon is the intent of the user. While commentators have argued that states should be responsible for curbing the activities of their own citizens, this gives little answer to the plausible deniability problem.[594]

Last and certainly not least, cyber weapons are weapons that subvert territory in a way that other weapons do not. Other weapons, must physically cross an international border and exert force or violence after having crossed that border. Cyber weapons can enter from anywhere and attack physical

---

[590] *For example* Xavier Aaronson, "The DIY Engineer Who Built a Nuclear Reactor in His Basement," *Motherboard*, August 27, 2014, http://motherboard.vice.com/read/the-diy-engineer-who-built-a-nuclear-reactor-in-his-basement.
[591] Gompert & Saunders, *Paradox of Power,* 131, 117.
[592] *Id.* at 133.
[593] Betz & Stevens, *Cyberspace and the State,* 11.
[594] *See for example* Gompert & Saunders, *Paradox of Power,* 117 and Sofner et al., "Cyber Security and International Agreements," 190

infrastructure far outside the territory of the attacking state. This was seen in the Stuxnet attack, as it was an attack that was introduced in Iran and the virus reported back to servers in global locations. States do not have legal mechanisms for restricting armaments that are ephemeral and locationless, and as a result disarmament and deterrence as mechanisms for slowing the spread of armaments to are ineffectual because they are dependent on the assumption that States have control over their borders and the mechanisms of physical violence within those borders.

Cyber weapons create uncertainty, and uncertainty stands in contrast to verification. Indeed, as seen above with Stuxnet, "the very point of a cyberattack, at least in part, is to increase uncertainty."[595] These weapons render the border ineffectual as a geographic indicator both in their control, as seen here, and there use, as seen with Stuxnet. This means that states are able to exceed their own geography through Cyberspace, giving them more options through which to pursue politics and conflict. The final section of this chapter will address how cyber conflict functions to dislodge international politics from their terrestrial bonds.

III. Conflict in Black

In May of 2014. the United States Department of Justice (USDoJ) filed an indictment against what it alleged were five cybercriminals. This in and of itself was not a necessarily novel event, but the individuals charged were novel. The indictment was against five members of the Chinese People's Liberation

---

[595] McDermott, "Decision Making Under Uncertainty," 229.

Army (PLA) who notably operated and resided in China.[596] The USDoJ asserted that these individuals were guilty of economic espionage in Cyberspace. The indictment itself marked a fever pitch in the bickering between the United States and China over the limits of online espionage. In this diplomatic impasse, the United States argued that China was violating international law by spying on companies for economic advantage and stealing intellectual property.[597] While the United States was pressing its concerns, though, Edward Snowden leaked a multitude of documents that revealed the United States own espionage efforts.[598] When China cried foul, the United States drew a line between diplomatic espionage and economic espionage.[599] The indictment from USDoJ was meant to reinforce the international norm that the United States was pushing.

Contrary to the intentions of the United States, the indictment served to reinforce the vast uncertainties about state action in the Cyberspace. The criminal sanctions, first and foremost, show the inability that the United States has to stop such actions. While certainly meant more as a diplomatic exclamation point, it must be noted that unless one of the indicted individuals

---

[596] U.S. v. Wang et al. - Indictment (W.D. Penn. 2014).

[597] *See also*, Joel Brenner, "Gray Matter," *Foreign Policy*, March 8, 2013, http://www.foreignpolicy.com/articles/2013/03/08/gray_matter and U.S. v. Wang, para. 5.

[598]Indeed the initial Snowden leak was a presidential order on Cyberwar the release of which coincided with a meeting between the leaders of the US and China. Rory Carroll, "Barack Obama and Xi Jinping Meet as Cyber-Scandals Swirl," *The Guardian*, June 8, 2013, sec. US news, http://www.theguardian.com/world/2013/jun/08/obama-xi-jinping-meet-cyberscandals and White House, "PPD-20: U.S. Cyber Operations," January 2013. The United States' complaints were also complicated by the Stuxnet operation. Zetter, *Countdown to Zero Day,* 369.

[599] Spying for national security reasons is generally considered legal under international law. Gompert & Saunders, *Paradox of Power,* 140-141. *But see* Snowden, "Testimony before the Parliament of the European Union," 8 (claiming that economic espionage is a "major goal of the US.").

sets foot into the United States is powerless to enforce the law it is invoking. Indeed, the indictment, far from emphasizing a point, seems to reveal the anxiety of the United States inability to ebb the flow of information to Chinese hackers. It also revealed the morphing nature of diplomacy, espionage, and conflict.[600] Were these military operations? Espionage? Or were they simply criminal acts?

The murkiness caused by state action online results a great deal from the attribution issues noted above. The ability of states to effectively conceal their cyber operations gives them great leeway to act in that realm, which is coupled with low cost of entry.[601] This is important to contemplate because it changes the space in which international politics unfold by changing the territory of war. In simplified terms, states may pursue their goals in international fora through diplomacy (here meant to mean anything that is not war including things like sanctions) or armed conflict. International law serves as a mechanism to keep states pursuing their interests within the confines of diplomatic action, which is why Art. 2(4) strikes the balance at the heart of international law by focusing on violence that crosses internationally agreed upon boundaries. Cyberspace short circuits that balance by removing the obstacle of the border and the corresponding risk of identification. States now have a third option of engaging through the geography of Cyberspace to achieve their goals. This third option is marked by the possibility of at once using force and refraining

---

[600] George R. Lucas Jr., "Can There Be an Ethical Cyber War?," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton: Taylor & Francis, 2013), 201

[601] US DoD, "Department of Defense Strategy for Operating in Cyberspace," 3.

from armed conflict. International politics, as a result, can now be mediated through geography Cyberspace.

This can be seen in the hack of Sony Pictures that was first revealed in November 2014.[602] The sophisticated hack affected most of Sony Pictures internal network and the company's internal information (including items such personnel records, e-mails, and unreleased movies) began to be leaked to the public.[603] The attack was soon linked to the upcoming release of the movie *The Interview*, a comedic parody about two Americans assassinating Kim Jung-Un, and it was assumed to have North Korean ties. When Sony was defiant about releasing *The Interview*, the hack was coupled with threats of terrorism that resulted in Sony pulling the release, though it was subsequently released online and in several theaters.[604] Two days later, on December 19, the FBI announced that it was attributing the attack to North Korea, though there has been great speculation as to the validity of this attribution.[605] President Obama, on

---

[602] Aly Weisman, "A Timeline of the Crazy Events in the Sony Hacking Scandal," *Business Insider,* December 9, 2014, http://www.businessinsider.com/sony-cyber-hack-timeline-2014-12.

[603] *Id.*

[604] Valerie Richardson, "Sony kills 'The Interview' after North Korea hack, terror threat," *The Washington Times*, Dec. 17, 2014, http://www.washingtontimes.com/news/2014/dec/17/sony-kills-the-interview-after-north-korea-hack-te/?page=all

[605] FBI Press Office, "Update on the Sony Investigation," Dec. 19, 2014, http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation. *But see* Robert M. Lee, "The Feds Got the Sony Hack Right, But the Way They're Framing It Is Dangerous," *Wired,* January 10, 2015, http://www.wired.com/2015/01/feds-got-sony-hack-right-way-theyre-framing-dangerous/; Bruce Schneier, "Attributing the Sony Attack," *Schneier on Security*, Jan. 7, 2015, https://www.schneier.com/blog/archives/2015/01/attributing_the.html; Jack L. Goldsmith, "The Sony Hack: Attribution Problems, and the Connection to Domestic Surveillance," *Lawfare*, December 19, 2014, https://www.lawfareblog.com/sony-hack-attribution-problems-and-connection-domestic-surveillance; Michael Sexton, "Accurately Attributing the Sony Hack Is More Important than Retaliating," *Georgetown Security Studies Review*, January 13, 2015, http://georgetownsecuritystudiesreview.org/2015/01/13/accurately-attributing-the-sony-hac

January 2, 2015, imposed sanctions on North Korea, which is the first times sanctions have been used in response to a cyber-attack.[606] Throughout this ordeal, the nature and scope of the attack made it a multidimensional threat that challenged the accepted nature of coercive action within the realm of the international.

The initial hack was credited to The Guardians of Peace (GOP) hacker group.[607] This hack was initially seen as a cybercrime against a corporation meaning that the core security concern was the security of Sony's network.[608] As a crime, the criminal is answerable to the state, but the focus is on the private network itself. At first, the hack of Sony did look criminal in nature as the hackers attempted to extort individual employees to keep their personal information from becoming public.[609] However, soon after this, security researchers began to find hints such as Korean language packs that linked the hack to North Korea. In a somewhat controversial move by the United States government, and specifically the FBI, to attribute the attack to North Korea thus moving the hack into center state of the national security narrative. It also moves the act out of the spectrum of a crime and into the spectrum of international relations, and as a result the United States issued sanction against the North Korean regime.

---

k-is-more-important-than-retaliating/. To highlight the controversy see the Sony Hack Attribution Generator at http://sony.attributed.to/.

[606] White House, Executive Order -- Imposing Additional Sanctions with Respect to North Korea (Jan. 2, 2015), http://www.whitehouse.gov/the-press-office/2015/01/02/executive-order-imposing-additional-sanctions-respect-north-korea

[607] Weisman, "A Timeline of the Crazy Events in the Sony Hacking Scandal."

[608] *Id.*. The initial reporting used the word "blackmailed."

[609] *Id.* Weisman notes that threats were made directly to Sony employees.

Superficially, US action in this incident may seem like business as usual in the context of international governance, but a close reading reveals a number of the uncertainties that show how borders are being recoded with new content. As noted above the FBI's attribution was hotly contested by security researchers, but a number of revelations show that even if North Korea was the master puppeteer, the cast of characters taking part in the hack was a globally distributed group of non-state actors. For instance, the Lizard Squad hacker organisation may have been involved in the hack as North Korean hired cyber contractors or, possibly, mercenaries.[610] The attribution question leads into a maze where the source of international conflict can no longer be pinpointed to a single site in terms of territory. The capabilities or weapons used are distributed, digital ghost guns making response difficult when the geographic source of the attack is territorially different from the attack, in this case North Korea and Cyberspace, respectively.

A second ambiguity is the nature of the attack. The attack on its facts is novel in terms of an "international incident," making it an interesting touchpoint for understanding how Cyberspace changes international space. North Korea bought technology that allowed it to attack a private US entertainment company in an attempt to halt the release of a film within the territory of the United States, and the attack garnered a response at the presidential level in the United States. In terms of international governance, the attack on Sony raises difficult questions of classification. If the source of

[610] Adrian Diaconescu, "Inside Job: Lizard Squad and Ex-Sony Employees Likely Aided North Korea's Hack Attack," *Digital Trends*, December 14, 2014, http://www.digitaltrends.com/computing/lizard-squad-and-ex-sony-employees-likely-involved-in-hack/.

the attack was indeed North Korea, it is safe to say that their military was involved, so one might think that this case would resemble the PLA case noted above. Personal information of employees and corporate information and intellectual property were stolen and released online. This has all the trappings of the economic espionage charged in the PLA indictment. The United States however chose a different response, which indicates that they intend to classify this cyber incident in a different category that goes beyond that of domestic criminal law which is usually the recourse that states have to espionage within their territorial borders. The use of a presidential order for sanctions against North Korea indicates a heightened concern with United States national security. Indeed, the president's order statesthat

> provocative, destabilizing, and repressive actions and policies of the Government of North Korea, including its destructive, coercive cyber-related actions during November and December 2014, actions in violation of UNSCRs 1718, 1874, 2087, and 2094, and commission of serious human rights abuses, constitute a continuing threat to the national security, foreign policy, and economy of the United States[611]

There are, of course, two factors that heightened the US response in this incident. The first is that the North Korean actions were targeted at denying the freedom of speech, a fundamental human right in the view of the US, and the second is the additional threats of acts of physical terrorism against theaters that show the movie.[612]

---

[611]White House, Executive Order -- Imposing Additional Sanctions with Respect to North Korea.

[612] Tierney Sneed, "Sony Hack Takes Darker Turn," *US News & World Report*, December 17, 2014, http://www.usnews.com/news/articles/2014/12/17/sony-hack-takes-darker-turn-with-interview-terror-threat.

What might be an even more interesting question though, would be how the North Korean authorities envisioned their actions. The regime is notoriously opaque, so ever having a full understanding of the logic that went into these actions is unlikely. North Korea's actions do show how Cyberspace changes the content of international action. Without cyber, North Korea's options would have been to choose diplomacy or conflict. If they choose diplomacy, they have a variety of peaceful options including negotiate with the US, place sanctions on the US, or place sanctions on Sony the company. These options seek to coerce change in another country through indirect action that stays outside of that country's territorial borders. In this case, North Korea can see that these options are either non-starters or ineffectual due to its relative power in the international community. It can also see that taking action in the form of direct action, i.e. conflict, within the borders of the United States is also not an available option due to its relative military power.[613] Cyberspace allowed North Korea to bypass this decision, by giving it the power to take a third path through the geography of Cyberspace. The similarities to Stuxnet as a coercive action should not be ignored. The Sony hack illustrates a second situation wherein a state was able to take direct actions that interfere with a state's "political independence" without the tell tale violations of its "territorial integrity."[614]

---

[613] *For example* Isaac Fish, "Could North Koreans Ever Really Invade America?," *Foreign Policy*, November 21, 2012, https://foreignpolicy.com/2012/11/21/could-north-koreans-ever-really-invade-america/.

[614] UN Charter Art. 2(4). Of course the drafters viewed these two phrases as disjunctive, but it is hard to imagine a use of force that threatened political independence without violating the territorial integrity of the state before Cyber. Of course article 2(4), also codes as illegal "threats of force," meaning that illegality is not dependent upon a simple penetration of

Similar to Stuxnet, the Sony hack raises questions about thresholds for self defense under of Article 51 and the application of International Humanitarian Law.[615] All of these structures meant to limit state action to the realm of diplomacy are dependent on the inherent territoriality seen in past conflict. The third path of action allows states the option to exceed their territory and directly encounter the space of an adversary state without geographic movement. The Sony-North Korea hack is one of a growing number of examples that demonstrate how the spatial context in which the international unfolds is being transformed by the imposition of alternate geographies, and it highlights how the nature of Cyberspace challenges underlying assumptions that shape the international space.

* * * * *

This chapter has shown how the governance system built around the physical territorial space of the state is being reshaped through the introduction of Cyberspace. This argument is built on illustrating how territorial borders no longer "bracket war" as envisioned in Art. 2(4). The international system, in other words, is ill equipped to create regulatory mechanisms that inhibit and control state action Cyberspace, much less the myriad other actors that can wield such violence.

---

another state's territory. However, because as noted above, for cyber weapons to be useful, they must be secret and as a result a threat of cyberforce is also unlikely.

[615] *See generally*, David D. Schmitt, "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflict," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, 2010, 151.

This theme of shifting international space will be extended in the next two chapters which address legal and political space. A number of subthemes will become evident as well and are worth noting as the analysis moves forward. First, the role of US action will be used as an explanatory mechanism through these chapters. The reason for this is twofold. First, the United States was where the Internet originated, and it harbors a bulk of the physical, application, and content layers of the Internet. As such it is of particular value in examining norm creation, or lack thereof, in Cyberspace. Second, it is hoped that the comparison of various US actions reveals a certain schizophrenia in US policy that indicates an understanding of Cyberspace as something extraterritorial, but an inability to coherently develop an international policy due to its own territoriality.

A second theme is that of attribution. The ability to trace an action back to an actor, will recur throughout these chapters. The technology that allows for the concealment of identity will be addressed specifically in chapter 8's exploration of encryption technologies. Attribution or lack thereof is critical in understanding how Cyberspace allows individuals and entities to transcend their own geographies and take part in other geographies.

Finally, a theme hinted at here that will become more evident in the next two chapters is the role and variety of non-state actors and their ability to contend directly with states within the geography of cyberspace. This chapter highlighted a state's ability to blend in with the noise of non-state actors, moving forward this theme will be addressed in terms of non-state actors ability to engage globally outside the strictures of the international arena.

Chapter 7

Standardizing Authority

In 1975, the United States and the USSR launched a mission to dock an *Apollo* module with a *Soyuz* module.[616] The mission was a carefully orchestrated scientific mission that was meant to show how science for peaceful purposes could bridge ideological gaps, and was meant to further detente between the two nations. The effectiveness of mission in political terms is a story for another day. The object here is to draw a point from a small sidebar of the narrative surrounding the mission. The two states both had their own docking systems, which both relied on, technically speaking, a female side which received the male side of the docking apparatus, much like a headphone jack. In the tense political atmosphere, neither side wanted to become the female side of the others docking system. As a result, the two countries developed an androgynous docking system that was interoperable with itself.[617]

The point here is not to highlight the misogyny inherent in these terms and Cold War politics, which is a continuation of an international relations discourse that often characterizes dominance as male.[618] Instead, it is to point out that the standardized docking mechanism, which is purely a technical specification, holds a great deal of political content. The standard creates

---

[616] *See* Debbora Battaglia, "Arresting Hospitality: the Case of the 'Handshake in Space'," *Journal of the Royal Anthropological Institute,* v. 18/1 (June 2012) S76-S89.
[617] *Id*. at S82.
[618] *See generally* Charlotte Hooper, *Manly States: Masculinities, International Relations, and Gender Politics* (New York: Columbia University Press 2001).

technical interoperability, but the technical standard is loaded with political content as it becomes the mediator of state to state communication. In the *Apollo-Soyuz* mission, it was a question of technical connection that defined the parity of the states involved as they brought their quasi-territories into proximity.[619]

Usually, questions of standardization occur when states are already in proximity, and international telecommunication has a long history of international governance mechanisms to develop such standards.[620] The ITU as the world's oldest international organization represents a legacy of international cooperation and coordination on telecommunications standards.[621] It also charts a unique history through which international law was developed in such a way that it avoided sticky issues of content by favoring interconnection over interoperability. States' ongoing ability to negotiate and adopt law in the realm of telecommunications would arguably make the international governance regime well prepared to regulate the Internet and Cyberspace, but this has not been the case. This chapter will investigate this phenomenon and argue that the development of Cyberspace has served to delegitimize the state as the central governance actor within its sphere. It will

---

[619] It should be noted that the androgynous system developed for *Apollo-Soyuz* would prove to be a significant development that would influence later systems. Significantly, the International Docking System Standard is an androgynous system. International Docking System Standard, Interface Definition Document, Revision D (April 30, 2015) http://www.internationaldockingstandard.com/download/IDSS_IDD_Revision_D_043015.pdf. Arguably, such systems are an important innovation that allows states to better fulfill obligations under the *Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space* (December 3, 1968).

[620] On standardization *see generally* Jayakar, "Globalization and the Legitimacy," 721-722.

[621] Another example of an international standards body would International Civil Aviation Authority. *See generally* *Convention on Civil Aviation* (Dec. 7, 1944).

also argue that an important part of this delegitimization is the undermining of consent as envisioned in international law.

To construct these arguments, this chapter will proceed first by examining the nature of the ITU's power to make law and regulation concerning international telecommunications. This section will give a historical overview of the ITU and then investigate the most recent effort by states to extend the ITUs authority over the Internet. The next section will examine the development of global multistakeholder governance through an examination of the Internet Engineering Task Force (IETF) and the Internet Corporation for Assigned Names and Numbers (ICANN). The final section will examine the trend of corporate intermediaries in Cyberspace and their capacity as governance bodies.

I. Harmful Interference

The need to facilitate interconnection among states through telecommunication is as old as the telegraph, and the ITU dates to this period having first been established as the International Telegraph Union.[622] The utility of telegraph technology was immediately apparent, but states wanted to ensure that they controlled the technology as it crossed their borders. As a result, the ITU developed as an organization that developed standards and rules for cross border telecommunications, which allowed for interconnection among countries. This regime gave states primary control over telecommunications at the nodes where physical infrastructure crossed their

[622] Codding, "The International Telecommunications Union," 501.

borders. The ITU's goal is to "facilitating peaceful relations, international cooperation among peoples and economic and social development by means of efficient telecommunications services," which echoes many of the core concerns of International Governance.[623]

This strategy worked well with lined communications such as telegraph and telephone, but broadcast brought on new challenges, because radio waves do not conform to state borders. There was, as a result, much debate in the international community on the nature of international responsibility for content crossing borders on radio waves. This can be seen in the Soviet complaints about radio propaganda during the Cold War[624] as well as in the UN General Assembly's controversial adoption of the Direct Broadcasting Principles.[625] The ITU again avoided coming into contact with the issue of content by adopting a policy of coordinating international usage of electromagnetic frequencies by nations so as to prevent harmful interference between broadcasts.[626] More recently, there was a movement in the ITU to give developing states more access to international telecommunications development resources.[627] Of course, in the realm of international relations a state's disbursement of aid is highly attenuated by a state's political goals. The ITU again avoided questions of content by developing a division that advocated for such development but left the legal substance to bilateral or regional

---

[623] *Constitution of the International Telecommunication Union*, preamble.
[624] Eppenstein & Aisenberg, "Radio Propaganda," 154.
[625] *See* Lyall & Larsen, *Space Law,* 256-269 and UNGA, "DBS Principles."
[626] *Constitution of the International Telecommunication Union*, Art. 1.2(b), Art. 45; Eppenstein & Aisenberg, "Radio Propaganda," 154.
[627] Codding, "The International Telecommunications Union," *Denver Journal International Law & Policy* 505.

agreements.[628] Held argues that technical IOs such as the ITU "have been sharply delimited" in order to make them "politically unexceptionable."[629] In the case of the ITU, its actions have been delimited to facilitating interconnection and coordinating usage.

Two key observations need to be made here. First, the ITU is a body made up of states as the basic unit of the body politic,[630] and the ITUs legitimacy, like that of other international organizations, springs from "state sovereignty."[631] Votes in the ITU are allocated one to one, and while non-governmental actors are given access to participate in deliberations,[632] the state is the primary power holder in the ITU forum for international coordination, meaning that the international norms that it adopts come through the "filter of domestic structures and domestic norms."[633] The ITU is a treaty based organization, and as such it springs from within the logic of international governance, which reifies international conceptualization of the world.

Second, the ITU makes international law and policy. The ITUs outputs consist of a variety of documents, and among these are law and policy documents. As the international body that adopts the rules of international telecommunication, the ITU adopts resolutions that charts its own course in addressing the issues raised by telecommunication technologies. More importantly, the ITU meets regularly to update the rules that make up the

---

[628] *See Constitution of the International Telecommunication Union*, Art. 21.
[629] Held, *Democracy and the Global Order*, 109.
[630] *Constitution of the International Telecommunication Union*, Art. 2
[631] Jayakar, "Globalization and the Legitimacy," 717.
[632] *Id.* at 728-729. DeNardis, *The Global War for Internet Governance*, 33.
[633] Finnemore & Sikkink, "International Norm Dynamics and Political Change," 893.

Radio Regulations. The Radio Regulations are a treaty of technical standards that is negotiated among members and sets out the regime for coordination of international broadcast telecommunication. The rules adopted by the ITU are binding international obligations that apply to states, not telecommunication providers, directly. In effect, the ITU depends on the member states to make its rules operable through national regulation binding upon domestic actors. Regulation as a result relies on consent of the state parties to the adopted rules.

As an international lawmaking body with the competency and a proven record for coordinating international telecommunication activities, it would seem that the ITU would be well situated to extend its hand of governance over the Internet which seems to easily fit within the definition of international telecommunication, which is "[a]ny transmission, emission or reception of signs, signals, writings, images and sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems."[634] The technology involved is exactly the type of technology that the ITU was developed to coordinate across borders, but the ITU has been unable to exert direct control within the sphere of Cyberspace. It has, instead, taken on a role more akin to a stakeholder within Cyberspace governance. This is in part to the historical conditions would saw the governance of information technologies "dominated" by other organizations.[635]

This inability of the ITU to effectively extend its competency can be seen in the results from proceedings that at the most recent Plenipotentiary

---

[634] *Radio Regulations* (2012) Art. 1.3
[635] Jayakar, "Globalization and the Legitimacy," 719.

Conference held in Busan, Korea in 2014 (PP-14). This meeting was preluded by media chatter warning of an ITU takeover over the Internet, which taps into an established "media narrative . . . about a possible Internet governance takeover" by the UN.[636] These headlines were prompted by the position being taken by the Russian Federation and other states that the ITU should have more control over the Internet.[637] This position of this bloc of states was widely interpreted as a threat to a free and open Internet. For instance, the United States characterized the proposals as mechanisms "that could have provided a mandate for the ITU in surveillance or privacy issues; inhibited the free flow of data; regulated Internet content and service companies; undermined the multi-stakeholder process; or called on the ITU to develop international regulations on these issues."[638] There was more though than just rote suspicion of the UN. As a product of international law, the ITU would need to extend the logic of international governance to Cyberspace to effectively regulate its mechanisms. This would mean adopting measures that allow for cross border interconnection while avoiding embroiling itself into disputes over the content of communications. This would give states the ability to adopt, through the ITU forum, technical standards that facilitate national content controls. Such standards would increase state power to censor, monitor, or treat with deference communications entering their borders.

---

[636] DeNardis, *The Global War for Internet Governance*, 33.
[637] Samantha Dickinson, "How Will Internet Governance Change after the ITU Conference?," *The Guardian*, November 7, 2014, sec. Technology, http://www.theguardian.com/technology/2014/nov/07/how-will-internet-governance-change-after-the-itu-conference.
[638] United States Department Of State, "Outcomes from the International Telecommunication Union 2014 Plenipotentiary Conference in Busan, Republic of Korea," Press Release|Media Note, *U.S. Department of State*, (November 11, 2014), http://www.state.gov/r/pa/prs/ps/2014/11/233914.htm.

In Busan, the moves to extend the ITUs competency were defeated through the work of the United States, which "built a broad consensus that led to success on Internet and cybersecurity issues keeping the ITU's work focused on its current mandate."[639] These efforts served "to mitigate and remove proposed language from resolutions that would have improperly expanded the scope of ITU,"[640] and the results of the negotiations are a handful of nonbinding resolutions that resemble policy statements.[641] So for instance Resolution 2 calls for a global framework to exchange information on such technologies to "support the harmonious development of telecommunication services."[642] More strikingly, Resolution 101 gives direct recognition to IGCs by "requesting" the Standardization Sector to continue "collaborative activities on IP-based networks with ISOC/IETF and other relevant recognized organizations."[643] The ITU further adopted Resolution 102, which states that "management of the Internet is a subject of valid international interest and must flow from full international and multistakeholder cooperation."[644] This resolution seemingly cedes power to an ambiguously defined

---

[639] *Id*. *See also* Dickinson, "How Will Internet Governance Change after the ITU Conference?,"
[640] United States Department Of State, "Outcomes."
[641] In addition to the resolutions addressed in text see ITU, "Resolution 133 (Rev. Busan, 2014) Role of Administrations of Member States in the Management of Internationalized (Multilingual Domain Names," 2014; ITU, "Resolution 140 (Rev. Buan, 2014) ITU's Role in Implementing the Outcomes of the World Summit on the Information Society and in the Overall Review by United Nations General Assembly of Their Implementation," 2014; and ITU, "Resolution 180 (Rev. Busan, 2014) Facilitating the Transition from IPv4 to IPv6," 2014.
[642] ITU, "Resolution 2 (Rev. Busan, 2014) World Telecommunication/Information and Communication Technology Policy Forum," 2014.
[643] ITU, "Resolution 101 (Rev. Busan, 2014) Internet Protocol-Based Networks," 2014.
[644] ITU, "Resolution 102 (Rev. Busan, 2014) ITU's Role with Regard to International Public Policy Issues Pertaining to the Internet and the Management of Internet Resources, Including Domain Names and Addresses," 2014.

"multistakeholder" system that will be argued below to exist outside the bounds of the international legal geography.

Trading off coordination for content is, of course, the status quo of international telecommunications regulations,[645] which raises the question of why Internet technology has resisted the encroachment of international law from the exact international body charged with regulating that type of technology. A simple answer would be that states do not want to extend international law to govern Cyberspace, and to some extent this is true. However, it seems odd that Cyberspace has such a prominent role in social life at the global level, and that international law remains largely silent on the matter. To be clear it is not that states are disinterested in the Internet, it is clearly an item on the agenda of the international, but it is one that international governance is at a loss to comprehensively address. A more satisfying answer can be found in the geography of Cyberspace that exists outside the logic of international geography. Critically, the legal geography of Cyberspace is built around code which is both content and medium. As a result, the "sharply delimited" functions of the ITU are ill equipped to expand to control a medium that is at the same time content. The legal geography of Cyberspace, as a result, has been peeled away from territorial borders. The state is not deprived of jurisdiction completely, as should be obvious from existing laws in the domestic legislation, but those laws can only extend to the layers of Cyberspace that intersect national space. As a result, international

---

[645] The only "right" recognized in the ITU Constitution is the "right of the public to correspond by means of international service of public correspondence," which has no expressive content. *Constitution of the International Telecommunication Union*, Art. 33

governance has lost significant control over transnational communication, which no longer conform to the bordered assumptions that underlie international governance.

This does not mean that Cyberspace is without authority. It means that the state becomes one of many stakeholders in a multistakeholder legal geography. The next to section will investigate the trend of global multistakeholder governance by examining the technical bodies that govern the logical layer of the Internet, and then through a look at the corporate and commercial interests that extend governance over the Internet. These sections together reveal a world scale legal geography that is not dominated by the state. It is most certainly not devoid of the state, but the state is no longer the central node of authority. This is a critical problem for international governance since it is based on a model in which the state is the primary authority.

II. Rejecting Kings

"We reject kings, presidents and voting" is a phrase worthy of most fringe political manifestos. Though dripping with anti-authoritarian angst, the phrase is not from an anarchists screed. Instead it is found in the central document, "The Tao of the IETF," that explains the workings of the Internet Engineering Task Force (IETF).[646] This is the technical body that adopts standards that govern the logical layer of the Internet. The statement is more than one of personal rejection of the authority; it is a community rejection of

[646] IETF, "Tao of the IETF."

state authority over the methods and means of communication and specifically within the geography of Cyberspace.

The rejection of kings has a strong roots in the anarcho-libertarian tradition of many coders who were instrumental in developing the Internet as discussed in Chapter 4. While the rhetoric used is anarcho libertarian, this statement is not a simple denial of state authority. It is in practice an assertion of authority over states, which is consistent with the ITU's inability to extend its own mandate. Multistakeholder governance structures remove the state's ability to dominate regulatory decisions by removing the state's ability to consent to governance. Consent to the law by states is a bedrock principle in the international governance system. States, however, do not have the ability to consent to new standards in Cyberspace. In the multistakeholder model "[t]here is no geographically localized set of constituents" with a claim to legitimacy to deploy power.[647] Legitimacy, as a function of consent, has been redistributed from communities defined by borders to "the participants themselves," and they could be anywhere.[648] The borders of the state do not define the political community Cyberspace, which disaggregates the core unit of international geography.[649] The legal geography of Cyberspace is not bordered. It is coded, and code is law.[650]

The IGCs discussed in Chapter 2 are representative of the multistakeholder governance that diminishes a state's power to consent to law.

---

[647] Johnson & Post, "Law and Borders," 1375.
[648] Johnson & Post, "Law and Borders," 1375.
[649] Walzer, "The Moral Standing of States," 1980, 211; Clark, *Legitimacy and International Society*, 6.
[650] Power & Tobin, "Soft Law for the Internet," 41 (IETF decisions are never "turned into hard law by statutory definition").

The IETF serves as a perfect example and its actions can be seen to push its authority over states. This multistakeholder body adopts and maintains the standards that make the Internet work, including the TCP/IP, and it has the "largest influence on the technologies used to build the Internet."[651] TCP/IP is exactly the the type of code that rejects kings, and it gives the IETF "a powerful seat of authority."[652] These protocols are meant to move activity to devices at the edges of the networks, which gives the user any freedom that he or she can program into Cyberspace. The state's bordered control point becomes null when data can move through any connection, thereby jumping those borders. Importantly, State's never consented to this state of affairs. States consent to telephone lines crossing their borders, and to the standards for the interconnection promulgated by the ITU. They consent to the frequency allocations governing terrestrial and spaced based broadcast technologies. They even agree to how the post will be exchanged between them. However, they never agreed on the TCP/IP which transforms other telecommunication technologies. The natural choke point found at the border fragments when information itself fragments through packet switching. Even physical gaps are becoming less effective as can be seen by Stuxnet, which jumped an air gap, as well as in projects that seek to get electronic devices across the border of states like North Korea.[653]

---

[651] Alvestrand & Lie, "Development of Core Internet Standards," 126. Denardis notes that "increasingly multistakeholder institutions" control Internet resources. DeNardis, *The Global War for Internet Governance*, 36.
[652] DeNardis, *The Global War for Internet Governance*, 65-66.
[653] Halvorssen & Lloyd, "We Hacked North Korea With Balloons and USB Drives."

The IETF evolved out of the historical development of the Internet in which the engineers that were constructing the Internet were also making the decision about how that space would be constructed.[654] As a result, decision making evolved from group conversations among the coders. The IETF evolved from these conversations which were extraneous to the state, and thus states were never admitted to the decision making process. As the Internet grew, so to did the IETF. It eventually opened its membership to anyone that wanted to join and take part in that decision making process. It was community governance built on "rough consensus and running code."[655] This form of decision making added decisional value to the functionality of code in addition to the value of consensus. This is important because for standards to be effective they must be widely accepted."[656] State may have agents join to represent their respective interests, but these individuals are on equal footing with a variety of others including corporate agents and civic minded netizens, removing the state from the dominant position it holds in international governance. The IETF's open and transparent process creates interoperability standards that shape the "modern public sphere and broader conditions of political speech."[657] This means that the IETF structures the discursive space within states and without their consent.

The IETF makes decisions on how data will travel across borders outside the scope of the state, but significantly, it "has no formal authority over

---

[654] *See* Leiner et al., "A Brief History of the Internet." and Power & Tobin, "Soft Law for the Internet," 41.
[655] IETF, "Tao of the IETF."
[656] Jayakar, "Globalization and the Legitimacy," 736.
[657] DeNardis, *The Global War for Internet Governance*, 77.

anything but its own publishing process,"[658] and its status is further complicated by the fact that it has "no formal membership."[659] The decisions that it takes construct the logical layer of the Internet, and state power in that decision process is limited to the ability to send representatives. The state, in the formal sense, is never consulted on IETF decisions, which erodes the state's ability to consent to rules governing transnational communications. This is a significant development in governance at a world scale and should not be downplayed. The spatial settlement premised on sovereign equality is, in essence, challenged by a set of rules that recode borders in such a way that states lose significant control of the flow of information across them. This is further confirmed by the IETF's lack of legal personality.[660] It therefore exists outside of the jurisdiction of any state and since states do not make up its membership it is not an IO founded upon international logic. The IETF's organizational nebulousness resists clear classification within the space of international legal geography.

The IETF is not the only entity that exerts this type of multistakeholder control over the Cyberspace and thus over states. Both the ISOC and the W3C (see Chapter 3) as Internet governance communities share attributes with the IETF, though the IETF is the most extreme in is extra-stateness. While these are both interesting cases, the warping of international legal geography is observed better in a case with different attributes. Such a case can be found in

---

[658] Alvestrand & Lie, "Development of Core Internet Standards," 126.
[659] DeNardis, *The Global War for Internet Governance*, 69.
[660] Alvestrand & Lie, "Development of Core Internet Standards," 126.

the Internet Corporation for Assigned Names and Numbers (ICANN), which currently exists as a non-profit corporation under the laws of the United States.

ICANN too was a product of the ad hoc historical processes through which computer scientists pieced together Internet governance. In the 1970s, Jon Postel began the work that would later be known as the Internet Assigned Names and Numbers Authority (IANA). Postel's work would eventually develop into a regime for managing the DNS, described above in Chapter 2. At this point the Internet was largely made up of US government and University networks. The US National Science Foundation (NSF) was the lead government agency it left governance of Internet architecture up to the coders and engineers that were making the technical decisions on how to best foster interoperability on the network. Postel emerged as the one man show at the University of Southern California, and he managed the root file of the DNS through an NSF contract.[661] The US government's policy during the 1990s was to leave the development of the Internet to "private sector leadership" in hopes of privatising the network of networks.[662] The US federal government, though, soon stepped in as a reaction to various proposals for privatization of the IANA function that began to arise in 1994.[663] This action resulted in ICANN "[a]s an alternative to government."[664] ICANN created by Postel to to take over the IANA function, and it signed its first Memorandum of Understanding with the

---

[661] Milton Mueller and Dale Thompson, "ICANN and INTELSAT: Global Communication Technologies and Their Incorporation into International Regimes," in *The Emergent Global Information Policy Regime*, ed. Sandra Braman (Palgrave Macmillan, 2004), 66-67.
[662] *Id.* at 63.
[663] *Id.* at 67-68.
[664] *Id.* at 63.

Department of Commerce in November of 1998.[665] ICANN is "a private nonprofit corporation created to manage policy and technical features" of the DNS.[666] The corporation itself functions with oversight by the National Telecommunications and Information Administration (NTIA),[667] which maintains a "back door authority"[668] that it uses to "very rarely reject" ICANN action.[669] This oversight does play an "important role in ensuring that proper processes are followed."[670]

Three things of significance should be noted here. First, is that ICANN has personality over US law that makes it subject to the law of the United States. The second, is that, despite the fact that ICANN extends from US government involvement in the development of the Internet, there was never any sort of lawmaking procedure that gave ICANN its authority.[671] It administers a significant governance regime that developed outside the realm of lawmaking in the domestic and international arenas.[672] Third, despite this extra legality, ICANN is subject to special government intervention through NTIA oversight

---

[665] *Id.* at 68.
[666] Paul Rosenzweig et al., "Protecting Internet Freedom and American Interests: Required Reforms and Standards for ICANN Transition," Heritage Foundation Backgrounder (Washington, D.C.: The Heritage Foundation, June 16, 2014), http://www.heritage.org/research/reports/2014/06/protecting-internet-freedom-and-american-interests-required-reforms-and-standards-for-icann-transition 1; Monika Zalnieriute and Thomas Schneider, "ICANN's Procedures and Policies in the Light of Human Rights, Fundamental Freedoms and Democratic Values" (Council of Europe, June 16, 2014) 9; Partridge & Lonardo, "ICANN Can or Can It?," 24; and DeNardis, *The Global War for Internet Governance*, 48-49.
[667] *See generally* Krattenmaker, *Telecommunications Law and Policy*, 21.
[668] Mueller & Thompson, "ICANN and INTELSAT," 70.
[669] Rosenzweig et al., "Protecting Internet Freedom and American Interests," 3.
[670] *Id.*
[671] Mueller & Thompson, "ICANN and INTELSAT," 65 ("ICANN was created by the executive branch of government, without any legislative authority.") and *Id.* at 69.
[672] Mueller & Thompson, "ICANN and INTELSAT," 63 (noring that ICANN can be "more heavy handed than an intergovernmental entity") and DeNardis, *The Global War for Internet Governance*, 46. *But see* Rosenzweig et al., "Protecting Internet Freedom and American Interests," 4.

function.[673] Thus on its face, ICANN fits into the state's governance structure and seems dissimilar from organizations like the IETF. However the NTIA, has recently announced it intention to transfer the IANA functions of ICANN to a multistakeholder regime. This serves an interesting example of a state relinquishing control of an Internet governance body, but the relinquishment is not to the international community as might be expected.[674]

The NTIA "unexpectedly" announced this transition in March of 2014.[675] The announcement stated that the NTIA would "transition key Internet domain name functions to the global multistakeholder community."[676] Notably, the announcement employs the word 'global' as opposed to 'international' in the announcement. In fact international only appears one time to 'global's six.[677] This indicates an intent to not turn this over to an IO. Instead, the announcement posits a new form of governance body, a global multistakeholder community, that is undefined in international governance. The NTIA announcement came shortly before the NetMundial conference held in Brazil in April of 2014. This civil society conference adopted a Statement on Multistakeholder governance, which helps to shed light on the idea of a 'global multistakeholder community." It states that:

> Internet governance should be built on democratic, multistakeholder processes, ensuring the meaningful and accountable participation of all stakeholders, including governments, the private sector, civil society, the technical community, the academic community and users. The respective roles and responsibilities of stakeholders should be

---

[673] Partridge & Lonardo, "ICANN Can or Can It?" 24.
[674] The move was "fully supported" by the Council of Europe. Zalnieriute & Schneider, "ICANN's Procedures and Policies," 9.
[675] Rosenzweig et al., "Protecting Internet Freedom and American Interests," 1-2.
[676] NTIA, "NTIA Announces Intent to Transition Key Internet Domain Name Functions."
[677] *Id.*

> interpreted in a flexible manner with reference to the issue under discussion.[678]

An obvious implication in this statement is that the state is just one of numerous stakeholders, and the NTIA announcement proximity to this highly publicized meeting indicates a consciousness decision of the NTIA in choosing the term 'multistakeholder.'[679] The transition of IANA is still ongoing, and at present it is unclear how the new multistakeholder governance over the DNS will be structured. The proposed transition can be seen as a reaction to controversies over ICANN's "legitimacy and ties to the U.S. Government."[680] Rosenzweig et al. argue that the goal of the transition should be "an Internet that is free from governmental control, either individually or through inter-governmental bodies."[681] In Multistakeholder governance, then, states are just "one type of stakeholder," which removes them from their usual place of dominance in world scale governance.[682] The state as a result is functioning in a new legal geography which differs from that of international governance.

The IANA functions administered by ICANN are a "global regulatory regime."[683] The numbers they control are referred to as "critical internet resources," and these numbers define what devices are *on* the Internet and,

---

[678] NetMudial, NETmundial Multistakeholder Statement (April 24, 2014) http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf

[679] Denardis states that the nature of Internet governance is multistakeholder." DeNardis, *The Global War for Internet Governance*, 18.

[680] Partridge & Lonardo, "ICANN Can or Can It?," 24 and DeNardis, *The Global War for Internet Governance*, 61-62.

[681] Rosenzweig et al., "Protecting Internet Freedom and American Interests."

[682] Hurwitz, "A New Normal?," 239.

[683] Mueller & Thompson, "ICANN and INTELSAT," 77.

thus, who is *in* Cyberspace.[684] ICANN also manages domain name dispute resolution administering a nonjudicial, arbitration system through which intellectual property disputes can be resolved.[685] ICANN manages these property rights in Cyberspace, specifically, because the state can not. Interoperability on the Internet necessitates a uniform root file. If two states were to resolve a domain name dispute differently, this could result in either an inability of one of these states to enforce its judgement or a fragmenting of the root file and thus the Internet. At the moment, parties can pursue a domain name dispute in US Federal Court, because it had jurisdiction over ICANN. This same jurisdictional authority allows US law enforcement to seize domains associated with criminal activities.[686] Whether such jurisdiction was would be possible under the future multistakeholder regime is an open question.

States are just one voice in multistakeholder governance, and their consent to be bound is not a necessary precursor for the adoption of a rule.[687] These Internet governance communities change the dynamic of a state's authority over transnational communications, and this is a new development in world scale government. IGCs are not the only entities changing authority. As ICANN in its current form indicates, private corporations are taking a seat at

---

[684] Denardis, *The Global War for Internet Governance*, 57-58 and Mueller & Thompson, "ICANN and INTELSAT," 77.
[685] This is done through ICANN's Uniform Dispute Resolution Policy (UDRP) Partridge & Lonardo, "ICANN Can or Can It?," 24–29.
[686] DeNardis, *The Global War for Internet Governance*, 184-189; Sean Gallagher, "Silk Road, Other Tor 'darknet' Sites May Have Been 'decloaked' through DDoS [Updated]," *Ars Technica*, November 9, 2014, http://arstechnica.com/security/2014/11/silk-road-other-tor-darknet-sites-may-have-been-decloaked-through-ddos/; and Mueller & Thompson, "ICANN and INTELSAT," 81.
[687] Leiner et al., "A Brief History of the Internet." ("With the success of the Internet has come a proliferation of stakeholders").

the multistakeholder table, and they perform a number of governance functions in Cyberspace.

III. Corporate Governance

As addressed in the first section of this chapter, states have traditionally maintained control over information at their borders. Their ability and right to control information *at* their borders was based on their ability and right to control information *within* their borders that flowed from the sovereignty recognized in the international system. This is why states have laws that set the extent to which citizen speech is protected, as well as why states have legal controls over intellectual property. In this system, citizens rely on the state to protect their speech rights and companies must rely on states to protect their intellectual property.[688] But digitization has changed the nature of both speech and property, making both difficult for the state to regulate effectively by exponentially multiplying the sites where such interactions occur.

Digitization makes information super-portable. Media of all sorts can be digitized and sent across the Internet. This means that a song, for instance, can be encoded as an MP3, attached to and email, and sent to a friend. This is the basic concept for one of the early business ventures on the Internet: Napster. Napster allowed individuals to share files with other users of the program by enabling peer-to-peer connections. This proved to be wildly popular with college students using high bandwidth connections to share music. While this was a great boon for individuals looking for digital files of

---

[688] *For example* US Constitution, Art. 1.8.8, 1st Amend.

their favorite songs, record companies were predictably concerned with such technologies, because the technologies enabled the copying and distribution of their copyrighted intellectual property.

As the Napster case foretold, intellectual property would become, and still is, one of the most heated battlegrounds in Internet law and policy. Though Napster's business model was stopped by the US legal system, a number of services filled its space with different technical specifications meant to subvert the law that was used to shut down Napster.[689] Copyright is not the only area of intellectual property that has been affected by Cyberspace, though it may be the most prominent. Trademark, as noted above, has been one of the biggest issues in ICANN's management of the DNS,[690] and patent has been implicated as corporations have attempted to protect the code that they use in Cyberspace.[691]

The reason that intellectual property has become such a contentious issue in Cyberspace is twofold. First, digitization makes sharing of intellectual property easy. As Lessig argues, intellectual property can be perfectly copied and transmitted across the Internet with ease.[692] The MP3 files that made Napster a phenomenon, could be easily copied without generational degradation associated with analog media. This means that digital files, such as a copyrighted song, can be perfectly copied and shared on massive scales when users are able to connect using peer to peer using technologies such as

---

[689] Lessig, *Free Culture*, 73-74.
[690] *See generally* Partridge & Lonardo, "ICANN Can or Can It?"
[691] *See generally* Vera Ranieri, "EFFecting Digital Freedom," *2600: The Hacker Quarterly*, 2014.
[692] Lessig, *Free Culture*, 62-79.

Bittorrent.[693] This means that the means of efficient copying have been combined with the means of efficient distribution.

The second issue fueling this debate is linked to the competing business models in Cyberspace. In analog media space, while there is a black market for intellectual property, in general content owners are responsible for the production and distribution of their property. Record companies, for instance, copy the songs they own onto CDs and sell them at record stores. They control the physical copying and distribution in such a way that it diminishes the ability of others to copy and share that information.[694] In a digital environment, intellectual property holders have the same goals: to make a profit from the sale or use of their intellectual property, but the structure of the environment in which they pursue these goals is dramatically different in Cyberspace. Users no longer go to a record store to buy music; they instead enter search terms. The results of that search might send them to the record company or a licensed distributor to buy the music, but it is just as likely to send the user to a third party that is distributing free copies of the file. Cyberspace creates a gap between the content owner and the content distributor, the Internet Content Provider (ICP).[695]

To see this gap in action, one merely needs to visit YouTube, an online video sharing website owned by Google.[696] YouTube's business model is based on user generated videos spawning web traffic to the site which nets profits

---

[693] Denardis, *Global War for Internet Governance*, 63-65.
[694] While black markets exist, their ability to function is dependent of equipment to copy, reproduce, and distribute physical media.
[695] ICPs include media sharing websites such as YouTube, but also include search engines and social media websites.
[696] http://www.youtube.com

through advertising revenues from ads served to users that visit the site. In basic terms, YouTube's business interest is in having as much content as possible available through its servers. More content brings in more viewers. An ICP's business goals are often in direct conflict with intellectual property owners that want to control the dissemination of their content. This has created a clash between owners and ICPs that has played out across a number of fora and has been the subject of domestic lawmaking, but an important trend can be traced as these intellectual property disputes have proliferated. There has been a ceding of power to commercial entities who control the content available in Cyberspace. This power is often exerted without recourse to formal legal procedures contained within the legal geography of the state.

In the case of intellectual property, this can be seen in the notice and take down procedures deployed in numerous states to balance the competing interests of content owners and ICPs who host user uploaded content. Under these regimes, content owners must give notice to the ICP that it is hosting protected content on its website. In return, the ICP is granted a safe harbor from legal liability by promptly taking down the content. The user is then given notice that the content has been removed. In the US context this is often referred to as being 'DCMAed,' a reference to the U.S. Digital Millennium Copyright Act (DMCA), the law that enacted the US regime for notice and takedown.[697] While the equities between the content owner and the ICP seem fair here, many scholars have noted that these regimes result in a burden being

[697] Digital Millennium Copyright Act, Pub. L. 105-304 (1998). The DMCA also put in place controversial rules about technologies that subvert Digital Rights Management (DRM) technology. Lessig, *Free Culture,* 157.

shifted to the user. So, for instance, going back to YouTube, if Warner Bros.'s identifies a clip from one of its films, then it fills out an online form which notifies YouTube. The clip is removed, and the user is sent an email notification informing them of the takedown. The user is then given the option to send a counter notification if they think the takedown has been in error. The information page on the counter notification process informs the user that his or her personal information will be revealed and that the "claimant may use this information to file a lawsuit against you." (See Fig. 7.1).[698] Users are left with the decision of whether they want to pursue a claim on which they are potentially out-gunned.[699] This burden shift means that corporations can over protect their content and block potentially valid uses such as parody or fair use based on the odds stacked against the user.[700]

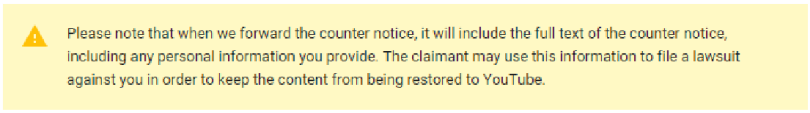

Fig. 7.1. YouTube counter notification notice.

Notice and takedown turns corporations and the technology they deploy into mediators of speech. Such mediation also takes place in the realm of self-regulation where corporations agree amongst themselves on how to best conduct their business. Self-regulation in the sphere of content standards in

---

[698] YouTube, "Counter Notification Basics," https://support.google.com/youtube/answer/2807684?hl=en (last visited Feb. 18, 2016).
[699] Lessig notes the possibility of $150,000 for a single infringement. Lessig, *Free Culture,* 187.
[700] *See* Goodman, "Media Policy and Free Speech," 1233 (noting that "scholars have likened copyright to a prior restraint").

the domestic context has been a feature of broadcast telecommunications that has been widely adopted in the context of Cyberspace.[701] Self-regulation of content within an interoperable arena is vastly different from broadcast and raises novel questions as to the extent that private companies should be able to control speech online. As Denardis and Hackl note, private actors are increasingly implementing technical architectures that mediates what speech is acceptable and what speech is not.[702]

In the context of particular social media sites this seems to be just the sort of community governance contemplated by early netficianados such as Barlow. It also reveals a startling removal of the state from the regulation of the political space in which speech takes place. It shifts power away from the individual by removing the court from between the individual and those that would suppress expression. In the place of the court are corporations that are seeking to maximize profits, rather than protect user rights. Laws like the DMCA, incentivize both intellectual property owners and ICPs to over protect data. This means that on the Internet "the rules of copyright law, as interpreted by the copyright owner, get built into the technology that delivers copyright content."[703] As a result, Cyberspace has "revealed the nexus between copyright and communications law, and the impact of both on speech."[704]

While mechanisms such as user agreements are a natural way to govern speech within the "walled gardens" of user experiences, the debate over net

---

[701] *See generally* Tambini et al., *Codifying Cyberspace*.
[702] Laura DeNardis and A. M. Hackl, "Internet Governance by Social Media Platforms," *Telecommunications Policy*, 2015.
[703] Lawrence Lessig, *Free Culture,* 148.
[704] Goodman, "Media Policy and Free Speech," 1212.

neutrality reveals a more troubling implication of corporate governance. Net neutrality, discussed in Chapter 2, centers on whether an ISP may legally favor some data or disfavor other data.[705] So, for instance, an ISP could enter a contractual agreement with a video streaming service for its data to move faster or it could block data from a competitor's server or it could slow certain types of data. ISPs say that they need this capability to efficiently manage their bandwidth, but those in opposition claim that if net neutrality erodes then ISPs will effectively control the content that users receive.[706] This means that "[e]ven routine technologies of bandwidth management are value-laden."[707] Media companies now must fight for the attention of viewers amidst a din of competition, and these same media companies have converged along with the technologies that they operate one. This means that intellectual property owners are often ISPs as well. For instance, two of the largest broadband providers in the United States, Comcast and Time-Warner, also function as ICPs and intellectual property owners.

From these examples a few key features of corporate governance should be observed. First, there is a severe lack of transparency when a corporate actor takes action against speech on the Internet, as there are no accepted procedures for such action. Second, this puts a severe burden on the individual to enforce his or her speech rights as there is a large imbalance of power between the corporate entity and the individual. Third, individuals may not even know whether their speech or access to information has been limited due

---

[705] DeNardis, *The Global War for Internet Governance*, 131-32.
[706] Verizon v. FCC, 6.
[707] DeNardis, *The Global War for Internet Governance*, 8.

to the nature of technical architecture. Finally, and most importantly, the state is passing these powers to the corporations involved to enforce directly. Notice and takedown is a statutory process, but it is one that removes the state as the central mediator of rights making it a peripheral entity in the process.

Other such mechanisms exist as well. The Copyright Alert System is the result of an agreement between ISPs and major copyright holders in which ISPs agree to use a tiered system to discourage copyright violators.[708] Under the agreement repeat violators can have their access to the Internet through the ISP eliminated.[709] Another example is the European 'right to be forgotten' which allows individuals to demand content about themselves to be removed from ICPs.[710] The right to be forgotten also suffers from the burden shifting that occurs with notice and takedown schemes for intellectual property.[711] Similarly, Maurashat and Shachtman both argue that ISPs are in the best position to regulate cybercrime.[712] These examples all point to a trend in which "the determination of conditions of participation in the public sphere is increasingly privatized."[713]

---

[708] Center for Copyright Information, "FAQ's on The Center for Copyright Information And Copyright Alert System," July 7, 2011, http://library.blountsfolly.com/space/items/show/183 and David Kravets, "ISPs to Disrupt Internet Access of Copyright Scofflaws," *Wired*, July 7, 2011, http://www.wired.com/2011/07/disrupting-internet-access/.

[709] *Id.*

[710] Rosen argues that the right to be forgotten is the "biggest threat to freedom on the Internet in the coming decade." Jeffrey Rosen, "The Right to Be Forgotten," *Stanford Law Review Online* 64 (February 13, 2012) http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten 88.

[711] *Id.* at 91-92.

[712] Maurashat, "Zombie Botnets," 379 and Noah Shachtman, "Pirates of the ISPs: Tactics for Turning Online Crooks Into International Pariahs," *Brookings Cybersecurity Paper*, June 2011, http://www.brookings.edu/~/media/Files/rc/papers/2011/0725_cybersecurity_shachtman/0725_cybersecurity_shachtman.pdf.

[713] DeNardis& Hackl, "Internet Governance by Social Media Platforms," 6.

The governance mechanisms "delegated" to "private intermediaries" are not just economic in their effects.[714] For example, Tambini et al. note that self-governance by corporations implicate them as the mediator of the right to expression.[715] Relatedly, Sunstein notes the effects of how commercial forums can be tailored into echo chambers that restrict deliberative democracy.[716] Finally, Lessig implicates corporate governance of intellectual property with the production of culture itself.[717] This means that corporations now "play a key role in ensuring and enabling" a number of human rights, especially "when an operator is dominant."[718] As a result, a Council of Europe report argues that Internet governance should be maintained in a way that "avoids predominance of particular deep-pocketed organizations that function as gatekeepers for online content."[719]

This is not to say that governance by corporations is a particularly new innovation. Many European empires of the 18-19th centuries were essentially corporations licensed to go out and govern, and neoliberal processes are premised upon MNCs effectively wielding power.[720] In fact, the rise of the Internet as a global force can be traced to a US preference for "private, and

---

[714] DeNardis, *The Global War for Internet Governance*, 13.
[715] Tambini et al., *Codifying Cyberspace,* 275. *See also* DeNardis, *The Global War for Internet Governance*, 157.
[716] Sunstein, *Republic. Com 2.0*.
[717] Lessig, *Free Culture,* 28-30. *See generally* Ismail Serageldin, "Cultural Heritage as a Public Good: Economic Analysis Applied to Historic Cities," in *Global Public Goods: International Cooperation in the 21st Century*, ed. Inge Kaul, Isabelle Grunberg, and Marc Stern (New York, Oxford: Oxford University Press, 1999), 240–63.
[718] Council of the EU, "EU Human Rights Guidelines on Freedom of Expression Online and Offline," I.D.34.
[719] Zalnieriute & Schneider, "ICANN's Procedures and Policies in the Light of Human Rights," 16.
[720] *See generally* Burbank & Cooper, *Empires*, 149-184.

avowedly economically rational, mechanisms of self regulation.[721] There is however, something distinctive about this in the context of Cyberspace, since "[f]unctionalist and technologist concerns regarding security, encryption, and domain name allocation become increasingly difficult to separate from the individual rights concerns regarding privacy, freedom of expression and public governance of the commons."[722] MNCs in this context are mediating the rights of individuals regardless of their location. A platform like Twitter, which is often mentioned in the same sentence with phrases like "global public sphere," can implement regulations that are effective globally and without and sort of public debate over these regulatory changes. In Cyberspace code is law, and this means that those who control code have authority. While states have the ability to regulate the code that will be implemented in their borders, for instance China's Great Firewall, corporations still maintain large areas of authority over users traversing their networks, and that authority often extends non-concurrently with the jurisdictional borders of the state from which the corporation is working from.

* * * * *

The international governance system is designed to allocate authority in a particular legal geography, in which the sovereign territorial state is the core political unit from which authority is to flow. This authority flows in two directions: it means the state is the sole holder of authority within the bounds of its territory, and it makes the states the holders of authority to take part in

[721]Tambini et al., *Codifying Cyberspace,* 15.
[722] *Id.*

international governance processes. This is why the international community has had such a difficult time dealing with mass atrocities. In order for the international community to stop such atrocities happening within the borders of a state, it must undermine its own spatial ordering.

Cyberspace presents a different legal geography that saps authority away from the state as a holder of international rights. Authority in this new legal geography is vested in those that control of development, adoption, and deployment of code that operates at a global level. The ITU's regime for governing telecommunications is focused on physical phenomenon that clearly occur at borders. Cyber-technologies, in particular the logical layer of the Internet, are ubiquitous, and regulation tied to the physical and legal geography of borders has proved to be ill suited. Cyberspace wields its own authority that is embedded deep within the code that architects its geography. The next and final chapter in this section will explore how this change in authority affects the rights of the individual engaging in the public sphere of Cyberspace. It will specifically engage with how changed territoriality and changed authority have reallocated the relationship between the individual and the state and introduces new ways of mediating rights.

Chapter 8

Unbordered Rights

At the end of World War I, states gathered together to negotiate a structure for international governance that would prevent conflicts like the one just experienced. The result of this negotiation was the Covenant of the League of Nations, an international organization that failed to live up to that promise.[723] While the League of Nations was primarily concerned ensuring peace, there was an emerging voice advocating for the self-determination of peoples. This was fueled in part by Point V of US President Woodrow Wilson's 14 Points, which called for an "adjustment of colonial claims" that weighed the "interests of the populations concerned" equally with the interests of colonial powers.[724] As the League of Nations was being formed, numerous activists courted Wilson and others in an attempt to move the role of rights of individuals to the fore of the emerging international system.[725] Human rights, however, did not make the cut in the final covenant.[726]

The call for self-determination though would fall on deaf ears until 1945, when the world was again reeling from a world scale conflict coupled with the

---

[723] *Covenant of the League of Nations* (April 28, 1919).
[724] Woodrow Wilson, "Fourteen Points" (Jan. 8, 1918) http://avalon.law.yale.edu/20th_century/wilson14.asp.
[725] Erez Manela, *The Wilsonian Moment: Self-Determination and the International Origins of ANticolonial Nationalism* (Oxford: Oxford University Press 2007) 59-60.
[726] There are a scant few references individual humans in the covenant, and the only 'rights' were soft pledges by states to improve conditions for laborers. Covenant of the League of Nations, Art. 22.

horror of the Holocaust. The newly negotiated UN Charter established a new international organization, the United Nations, which would serve as a central international fora in which states could interact. The UN Charter also implemented a role for human rights in the system of international governance. While the prevention of conflict maintained its primary role,[727] Article 1(2) of the Charter states that states are to have "respect for the principle of equal rights and self-determination of peoples."[728] This is a sea change moment in the development of international law in that it made human rights part of the political geography of states. While the Charter has many gaps that keep the UN from directly enforcing those rights, it made human rights a valid inquiry for international governance. Article 1(2) was followed by a bevy of documents that supported this new international identity for the individual, such as the Universal Declaration of Human Rights,[729] the Genocide Convention,[730] Covenant on Civil and Political Rights,[731] and the Covenant on Economic and Social Rights.[732] This expansion of political geography also included the slow development of international criminal law, which was used to hold perpetrators of international crimes individually criminally liable for acts that violated international law.[733]

---

[727] UN Charter, Art 1(1)
[728] *Id.* at Art. 1(2)
[729] "U.N. General Assembly Res. 217 A(III). Universal Declaration of Human Rights," December 10, 1948.
[730] *Convention on the Prevention and Punishment of the Crime of Genocide*, (Dec. 9, 1948).
[731] *International Covenant on Civil and Political Rights* (Dec. 16 1966).
[732] *International Covenant on Economic, Social and Cultural Rights* (Dec. 16, 1966).
[733] *See generally* Cornelis Arnold Pompe, *Aggressive War - An International Crime* (Martinus Nijhoff, 1953) and Antonio Cassese, *International Criminal Law* (Oxford: Oxford University Press 2003).

This post WWII expansion was important, but it was soon evident that the primary place that the sovereign state holds in international governance made it the primary means through which rights flowed to the individual. Due to the jurisdictional "claw back provisions" in the Charter, the state was the primary provider and impediment to human rights.[734] This resulted in human rights documents, negotiated by states, defined human rights in general terms. This allowed states leeway in their interpretation of the content of those rights. So for instance, while the United States was actively endorsing UDHR, it was actively violating many of the rights of African-Americans within its borders. This tendency of states to define rights to conform with their political geography can be seen very clearly in the universality of the acknowledgement of the freedom of speech compared to its very uneven application by states.[735] So, while the individual was given identity in the international legal geography, that identity is subservient to its national identity as the state remains the dominant source of rights.

Notwithstanding a few important regional human rights bodies, individuals have for the most part been unable to assert rights outside of the context of the political geography of the state in which they exist. The geography of Cyberspace is such though that it allows the individual to take part in a political geography that is not defined by the territorial borders.

---

[734] Elizabeth Borgwardt, *A New Deal for the World: America's Vision for Human Rights* (Cambridge, MA: Belknap, 2005) 191-192.

[735] As a stark example, Article 67 of the North Korean Constitution mimics the US Constitution's 1st Amendment, stating that "Citizens are guaranteed freedom of speech, of the press, of assembly, demonstration and association." Korea (Democratic People's Republic of)'s Constitution of 1972 with Amendments through 1998, https://www.constituteproject.org/constitution/Peoples_Republic_of_Korea_1998.pdf.

Cyberspace gives the individual identity in an alternate political geography, and allows individuals be the mediator of their own rights. This chapter will investigate how Cyberspace changes the international political geography by examining how Cyberspace reallocates rights through the reallocation of identity. Legal structures give "primacy to entitlements" and "release the entitled person from moral precepts and other prescriptions in a carefully circumscribed manner."[736] Such legal structures are shown here to be diminishing in importance as the "spatio-temporal location" of individuals is no longer a controlling condition for gaining the "artificial status of bearers of individual rights."[737]

This chapter will first address how encryption technologies enable individuals to mediate their own speech and associational rights in the space of Cyberspace. This section will investigate how digitized networks diminish a state's ability to constrain individual action. Spatial changes though do not simply empower individuals against states, it often empowers states against individuals. The second section will examine the use of mass surveillance technologies by states as a way of mediating the rights of individuals in extraterritorially, which causes a fissure in the usual understanding of the political space of the state. The final section will use the phenomenon of hacktivism to show how this reallocation of rights rewrites international political space and gives it global complexity.

---

[736] Habermas, *The Postnational Constellation,* 114.
[737] *Id.*

I. The Encrypted Self

Modern cryptography was born in Bletchley Park, England during WWII under the hand of Alan Turing.[738] The elite group that Turing led was tasked with cracking the encrypted messages sent through the German Enigma machine. This complex electro-mechanical machine had over 150 trillion possible combinations with which to encrypt a message, and the German military reset the combination being used each day. This meant that though the Allies could intercept the encrypted messages each day, it was physically impossible to run the messages through all the possible combinations in a single 24 hour period in order to decrypt the messages. Turing was a mathematician whose work had already described a theoretical machine, which came to be known as a Turing machine, that was foundational to the development of the modern computer.[739] At Bletchley Park, Turing worked to build a physical machine that would quickly move through the possible combinations of the Enigma machine in search of that day's combination. His work can be credited with changing the tide of the war for the Allies.

Cryptography today is a digital game. The Enigma Machine was based on the number of combinations for encrypting a text, and this number was a result of the settings that could be produced by its rotors and plu board. It was strong encryption until a machine was built that worked faster. An enigma

---

[738] On Turing *see generally* Brate, *Technomanifestos,* 53-84. For fictionalized accounts *see The Imitation Game* (Black Bear Pictures/Bristol Automotive 2014) and Neal Stephenson, *Cryptonomicon* (New York: Avon Books 1999).

[739] *See* David Berlinski, *The Advent of the Algorithm: The 300-Year Journey from an Idea to the Computer* (Houghton Mifflin Harcourt, 2000).187.

machine would likely be no match for for a smart phone, much less a military grade computer due to the massive amounts of processing power on these devices. This same processing power can be leveraged to create powerful encryption that is difficult for computers to break. To crack digital encryption users must either have a key or have a computer powerful enough to do the math in reverse. Many encryption techniques are premised on the inability of contemporary computers to do such math, and it is often stated that fastest way to decrypt some digital messages is to wait until computer technology has advanced to the point that it can do the functions necessary to decrypt the message.[740]

Encryption may seem esoteric to the individual user, but most people use some sort of encryption technology on the Internet daily. In fact, encryption technologies form the bedrock that commerce on the Internet relies on.[741] The ability to exchange data securely is paramount to the various trust systems implemented on the Internet. As an example, if an online business such as Amazon can not ensure that a customer's credit card information will be secure then it is likely that that business will not have any customers at all. Encryption is foundational to trust on the Internet.

Encryption, though, is not just a commercial or military technology. Individuals have long used encryption to keep their messages or identities secret, and modern computing has opened up the ability of individual users to gain access to advanced encryption technologies. The example of PGP, found

---

[740] This is based on Moore's Law which states "that processor speeds, or overall processing power for computers will double every two years." "Moore's Law," http://www.mooreslaw.org (last visited Feb. 18, 2016).
[741] DeNardis, *The Global War for Internet Governance*, 93.

in Chapter 3, is indicative of this. PGP was classified by the US as a munition, and it sought to stop the export of the technology to foreign countries. However, the nature of the Internet was such that the US was unable to stop the spread of the program across digital networks. The result being that individuals worldwide had access to military grade digital encryption. The effect of this was to spread the freedom of expression embedded in the code (Chapter 4 above) and make it "no local ordinance."[742]

Encryption technologies do two primary things. First, like the Enigma machine they can encrypt the contents of a communication. Second, and unlike the Enigma they can hide the identity of the communicator by the device's IP address thereby concealing the communicator's location.[743] As examples, PGP does the former, and the Tor web browser does the latter.[744] Encryption enables a spectrum of activities, but this section will examine two. The first of these activities is the much touted use of encryption by political dissidents in oppressive regimes.[745] The Internet itself offered the benefits of "cost, speed, and ease of use" to social movements and political dissidents.[746] Encryption

---

[742] Lessig, *Code 2.0*, 236.
[743] Greenberg, *This Machine Kills Secrets,* 65 ("encryption could hide not only *what was said* but *who was saying it*.") and Creighton Powell Davis, "The Internet As a Source of Political Change in Egypt and Saudi Arabia," *Al Noor* 1, no. 1 (2008), http://alnoorjournal.org/wp-content/uploads/2012/05/Al-Noor-2008.pdf#page=33 35 ("the Internet offers a cloak to both the identity and accountability of collaborators") . Encryption can also facilitate anonymous payment through Cryptocurrencies. *See generally* Elwell et al., "Bitcoin."
[744] Tor is an "onion routing" network that conceals the IP addresses of individuals using the software. *See generally* Greenberg, *This Machine Kills Secrets*, 135-168.
[745] *See generally* Fielder, "The Internet and Dissent in Authoritarian States," 161–91 and Castells, "Communication, Power and Counter-Power in the Network Society."
[746] Fielder, "The Internet and Dissent in Authoritarian States," 162.

enhances these benefits by allowing dissidents to organize and communicate in places where such rights are not guaranteed under the local law.[747]

As discussed in Chapter 4, Encryption technologies are closely tied to the anarcho-libertarian tradition in Cyberspace and specifically the Cypherpunks. This tradition frames cryptography as anti-authoritarian and pro-democratic. Encryption is a means with which to attack dominance and power of the state.[748] This attack on the dominance of the state comes through a technical renegotiation of identity.[749] Cypherpunks argue that power structures maintain control on power by controlling the information that is necessary to a deliberative democracy.[750] As an example, Julian Assange wrote a file encryption program "designed for activists in repressive regimes" and named it "Rubber Hose."[751] The name is a reference to the physical violence that the state would need to inflict in order to gain access to the contents of the encrypted files. Political dissidents are obviously criminals within their own state, but encryption allows them to remove themselves from the political geography constructed within a given territory. Greenberg interestingly casts this freedom in terms of physical geography noting that cryptography can free the individual from "governments that don't hesitate to knock down doors and

---

[747] The human right of freedom of expression is notoriously interpreted in a disconcerting number of ways by states. *See, for example*, Organization for Security and Co-operation in Europe, "Freedom of Expression on the Internet: A Study of Legal Provisions and Practices Related to Freedom of Expression, the Free Flow of Information and Media Pluralism on the Internet in OSCE Participating States," 2011 (noting disparities among OSCE nations)..

[748] Greenberg, *This Machine Kills Secrets*, 148; Domscheit-Berg, *Inside Wikileaks*, 189, and Assange, *Cypherpunks,* 1.

[749] Information is a resource to be distributed in these terms, and cyber libertarians recognize that "[w]ealth and resources are directly correlated with the ability to distribute speech." McIntosh & Cates, "Hard Travelin'," 94.

[750] Assange, *Cypherpunks*, 2012.

[751] Greenberg, *This Machine Kills Secrets*, 126-27.

haul away political enemies."[752] The individual escapes being identified by escaping their own location and thus escaping the political identity imposed on them through state mechanisms.

The criminal nature of political expression in some states leads us to a second activity that is polarized from political dissent: cybercrime. While the uses of encryption by political dissidents is important, cybercrime activities make up a substantial amount of the encrypted bandwidth used.[753] This is crime of all sorts.: extortion and fraud schemes, child pornography, identity theft, and terrorism.[754] Similar to dissidents, encryption allows criminals to step outside of their geographic strictures and escape the power of the state. However, only in the former instance can we say that the individual is expanding the rights to escape domestic political geography. Cybercriminals are usually engaging in activities that are criminal within their and their victim's jurisdiction meaning that they are only escaping their legal geography. Encryption protects both from the power of the state, but it allows the dissident to expand their political rights while it allows the criminal to subvert their legal obligations. The extension of self beyond the state and and its implications for political geography may best be seen in the role of encryption in terrorism.

---

[752] Greenberg, *This Machine Kills Secrets,* 136, 3.
[753] For example, Moore and Rid found that the bulk of .onion sites enabled by Tor were used for illicit purpose. Daniel Moore and Thomas Rid, "Cryptopolitik and the Darknet," *Survival*, 58:1 (2016) 21-25.
[754] *See generally* National Center for Justice and the Rule of Law, *Combating Cyber Crime: Essential Tools and Effective Organizational Structures* (Univ. of Mississippi 2007).

After the Paris and San Bernardino attacks of 2015,[755] a public debate has erupted over whether the government should have a back door to commercial encryption technologies in order to combat terrorism.[756] This debate was primed by revelations in the Snowden Leaks, which will be discussed in the context of state surveillance below. Here, though, the emphasis will be on how terrorist networks are able to extend themselves beyond their territorial confines to influence "world opinion."[757] Terrorist are seemingly both political actors and criminal actors. Indeed, it is uncontested that post 9/11 there are a number of terrorist organizations that now qualify as global political actors in an "'open source' anarchy."[758] Terrorist networks use the Internet for propaganda and recruiting as well as to communicate via encrypted networks. These technologies have allowed terrorist organizations to step beyond their territorial geography and subvert international geography through cybergeography.

---

[755] *See generally* "Paris Attacks: What Happened on the Night," *BBC News*, December 9, 2015, http://www.bbc.com/news/world-europe-34818994 and "Everything We Know about the San Bernardino Terror Attack Investigation so Far," *Los Angeles Times*, December 14, 2015, http://www.latimes.com/local/california/la-me-san-bernardino-shooting-terror-investigation-htmlstory.html.

[756] *For example* Sean Gallagher, "NSA's Director Says Paris Attacks 'would Not Have Happened' without Crypto," *Ars Technica*, February 18, 2016, http://arstechnica.com/tech-policy/2016/02/nsas-director-says-paris-attacks-would-not-have-happened-without-crypto/; Patrick Howell O'Neil, "Edward Snowden and Spread of Encryption Blamed after Paris Terror Attacks," *The Daily Dot*, December 9, 2015, http://www.dailydot.com/politics/paris-attack-encryption-snowden/; and Will Knight, "Controlling Encryption Will Not Stop Terrorists," *New Scientist*, accessed February 19, 2016, https://www.newscientist.com/article/dn1309-controlling-encryption-will-not-stop-terrorists/.

[757] Lewis, *The Crisis of Islam,* 147.

[758] The Princeton Project uses computer software and the Internet as metaphors to describe changes in international relations. Princeton Project on National Security, "Report of the Working Group on State Security and Transnational Threats" (Princeton, NJ, 2008), https://www.princeton.edu/~ppns/conferences/reports/fall/SSTT.pdf 10-11.

In fact, it could be argued that terrorists have no organized themselves around a decentralized logic similar to the Internet's, Bergen and Hoffman argue that the terrorist networks have a very specific strategy of diversifying the threat that they pose.[759] This means that the threat innovates along with technological innovation.[760] By decentralizing, these organizations are able to recruit operatives within the territorial geography of the target country and the digital connection to the recruit serves as a medium to wield power in that state. If there is a war on terrorism, and war is politics through other means, then the terrorist is using bits and bites to reshape the political landscape. Cyberspace gives terrorist political identity, and allows terrorist organizations to function as "quasi-states" that push subversive political ideology through violence.[761] This is not to say that encryption causes terrorism nor to say that it changes the content of the political message of terrorism. Instead, the argument is that encryption changes the political geography that surrounds the terrorist. It facilitates the strategy of allowing potentially anyone to become a global political actor by taking up the terrorist cause.

Of course terrorism is an extreme case and there are many documented legitimate uses of encryption technology to challenge political regimes.[762] The point here is not to choose a side in the debate over encryption. It is instead to

---

[759] Peter L. Bergen and Bruce Hoffman, *Assessing the Terrorist Threat: A Report of the Bipartisan Policy Center's National Security Preparedness Group* (Bipartisan Policy Center, 2010).
[760] Mark G. Stewart and John Mueller, "Cost-Benefit Analysis of Advanced Imaging Technology Full Body Scanners for Airline Passenger Security Screening," *Journal of Homeland Security and Emergency Management* 8, no. 1 (2011), 2.
[761] Clapham, "Degrees of Statehood," 150.
[762] *See also* Clinton, "Internet Rights and Wrongs." (noting the Internet's role in the Arab Spring and Iran's Green Movemebnt); Alexandra Dunn, "Unplugging a Nation: State Media Strategy During Egypt's January 25 Uprising," *Fletcher F. World Aff.* 35 (2011): 15.

show how it extends the political reach of the individual by "shift[ing] the balance of power from those with a monopoly on violence to those who comprehend mathematics and security design."[763] Encryption extends increased autonomy to the individual to assert rights denied within territorialized political geography.[764] As noted earlier, there is a current debate over whether the government should be able to require a back door into encryption programs. The US government could certainly require this, but to some extent it would be futile move.[765] This is because, as we see from PGP, anyone can code and release an encryption program, and as we see from the Liberator 3D-printed gun in Chapter 6, it is very easy to distribute code in contravention to US law. What we can see is that the United States has lost control over the communicative conditions of its own political geography.[766]

Encryption enables is the individual to have a "choice" in the "medium through which citizens exercise their political autonomy," where before that choice was lacking.[767] Encryption allows the individual to gain access to a political geography and participate on terms that are different from those produced by territorial geographies. If the Internet is indeed the "public space of the 21st century," then encryption technologies can be seen as marking the limits of its political geography.[768]

---

[763] Greenberg, *This Machine Kills Secrets* , 154
[764] Habermas, *The Postnational Constellation,* 118.
[765] A recent report makes just this point. *See* Berkman Center, *Don't Panic Making Progress on the "Going Dark" Debate* (Feb. 1, 2016) https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.
[766] Cohen, "Privacy, Visibility, Transparency, and Exposure," 200
[767] Habermas, *The Postnational Constellation*, 17.
[768] Clinton, "Internet Rights and Wrongs: Choices & Challenges in a Networked World."

II. Taming the Masses

Adolph Eichmann, a former Nazi leader, was kidnapped by the State of Israel from his home in Argentina where he had escaped to at the end of World War II. He was then secreted out of the country and into the jurisdiction of Israel where he stood trial for his role in the Holocaust.[769] It was generally agreed that Israel violated the sovereignty of Argentina in this extraordinary event,[770] but the two later signed an agreement settling the matter. The violation occurred because in international law territorial jurisdiction reigns supreme, or, In other words, international governance favors Argentina's border over Israel's interest in justice. This is why states use extradition treaties to govern the transfer of individuals within their territorial jurisdiction to other states that may have jurisdiction over a criminal act. In the usual scenario, Israel would be forced to concede to Argentina's dominance over its own territory and request that Argentina relinquish Eichmann.

Eichmann illustrates an important feature of the 1945 spatial settlement, which is that states are generally prohibited from mediating the rights of individuals extraterritorially. The right to self-determination was expressed internationally through "political independence" of the state.[771] States depended on territorially integrity to ensure that they maintained supreme

---

[769] *See generally* Hannah Arendt, *Eichmann in Jerusalem: A Report on the Banality of Evil* (New York: Penguin, 1963).
[770] United Nations Security Council, S/RES/138 Question relating to the case of Adolf Eichmann (1960).
[771] UN Charter Art. 1(2), 2(4).

authority within a given territory. In the wake of 9/11 however, states - or at least the United States - have begun to conceive of themselves as having mutable borders that can be extended at will.[772] Cyberspace is an instrumental tool in their conception of themselves in this manner. States now routinely mediate the rights of individuals in other countries through digital surveillance.[773]

Essentially, the same features that enable individuals to extend their rights through Cyberspace, also enable governments to use Cyberspace to surveil the individual. Despite the fact that encryption technologies are freely available, the bulk of Cyberspace communications happen on commercially encrypted networks. The networks collect vast quantities of data about individuals in a phenomenon known as "big data." As Lessig notes "[e]verything you do on the Net produces data" that "is in aggregate extremely valuable."[774] For instance, an ISP would have a record of IP addresses connected by a user which would reveal interests, shopping habits, professional and private associations. Beyond IP addresses bevies more information are held on computers, and as the US Supreme Court noted that the "sum of an individual's private life can be reconstructed" from the data on a cell phone.[775]

---

[772] For example see Bowman on the forward deployment of the US border. Gregory W. Bowman, "Thinking Outside the Border" 189–251.
[773] Lessig, *Code 2.0*, 209 ("'Digital surveillance' is the process by which some form of human activity is analyzed by a computer according to some specified rule.").
[774] Lessig, *Code 2.0* 216.
[775] Riley v. California, No. 13–132 (2014) 18.

A government's ability to access this information reveals much about an individual that traditional surveillance would entail.[776]

This type of data is collected for commercial purposes not for a single individual but for all users. As noted in Chapter 2, Cyberspace is a ubiquitous medium, meaning that if governments can tap into the commercial entities they can gather profiles of information on individuals worldwide.[777] The Internet enables global mass surveillance. It is this sort of activity that Edward Snowden revealed when he leaked a large trove of documents he collected as a National Security Agency (NSA) contractor.[778] These documents revealed a hidden legal and technical infrastructure implemented by the United States and its allies in the wake of 9/11 to intercept communications without a warrant. They gave an "unparalleled first hand look at the details of how the surveillance system actually operates."[779] Central to the public discourse on the Snowden Documents were their legality under US law in respect to US citizens, which is an important and interesting legal debate. The inquiry here though will not be into the legality of the United States actions, it will instead focus on how these actions reshaped international political geography. It will use the Snowden leaks to reveal how the United States reshaped the political geography of individuals it identified as "foreign."

---

[776] See, for example, Justice Sotomayor's 'mosaic theory. US v. Jones, 132 S. Ct. 945 (2012) (Sotomayor concurring).
[777] Lessig, *Free Culture*, 278.
[778] The leaks began to be released in June of 2013. Glenn Greenwald, "NSA Collecting Phone Records of Millions of Verizon Customers Daily," *The Guardian*, accessed May 6, 2014, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.
[779] Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (New York: Metropolitan Books 2014) 2.

PRISM serves as an excellent example of this US capability for mass global surveillance. First revealed in June of 2013, PRISM is a program that received direct feeds of data from a number of commercial companies such as Microsoft and Google that collectively "cover the vast majority of online email, search, video and communications networks."[780] This program required telecommunication companies to send all communications related to a "selector," such as an email address, to the NSA. PRISM constituted 91% of the "internet communications that the NSA acquired."[781] Similarly, the NSA engaged in "upstream collection" that relied on the "compelled assistance . . . of the providers that control the telecommunications backbone over which communications transit."[782] The Privacy and Civil Liberties Oversight Board (PCLOB) reports that "approximately 26.5 million Internet transactions a year" are collected through upstream collection.[783] Both of these push intelligence collection away from the locus an individual inhabits and into the Cyberspace

---

[780] Specific companies noted are Microsoft, Google, Facebook, Pal Talk, YouTube, Skype, AOL, and Apple. Greenwald & MacAskill, "NSA PRISM Program Taps in to User Data of Apple, Google and Others."; National Security Agency, "PRISM/US-984XN Overview of the SIGAD Used Most in NSA Reporting Overview [Snowden Leak June 7, 2013)," 2013; Gellman & Poitras, "U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program."; Glenn Greenwald et al., "Microsoft Handed the NSA Access to Encrypted Messages," *The Guardian*, July 12, 2013, http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data; and Ewen MacAskill, "NSA Paid Millions to Cover Prism Compliance Costs for Tech Companies," *The Guardian*, August 23, 2013, sec. US news, http://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid.

[781] Privacy and Civil Liberties Oversight Board, "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," July 2, 2014, http://library.blountsfolly.com/space/items/show/185 33-34. The PCLOB notes that 89,138 people were targeted under the legal provisions authorizing PRISM. *Id*. at 33. Greenwald and MacAskill claim that the program gives the NSA "direct access to the companies' servers." Greenwald & MacAskill, "NSA PRISM Program Taps in to User Data of Apple, Google and Others."

[782] PCLOB, "Report on the Surveillance Program," 35; National Security Agency, "(TS//SI/NF) FAA Certification Renewals With Caveats," October 12, 2011.

[783] PCLOB, "Report on the Surveillance Program," 37. An Internet transaction is "any set of data that travels across the Internet together such that it may be understood on a device on the Internet." *Id.* at 39.

an individual inhabits. Collected data is then retained in a database that could be queried by authorised NSA employees in order to find information on a target.[784]

The historical context of this surveillance system is important to understanding what it reveals about the changes in political geography. The overall surveillance program was authorized immediately after the 9/11 terrorist attacks via an executive order from George W. Bush.[785] The post 9/11 environment was such that "few foreign policy objectives have garnered as much support as the struggle against terrorism."[786] The Justice Department later determined that the President's Surveillance Program (PSP) needed a court approval, so it sought authorization from the classified Foreign

---

[784] BOUNDLESSINFORMANT was one of the tools used to manage the massive amounts of data that were being collected. Glenn Greenwald and Ewen MacAskill, "Boundless Informant: The NSA's Secret Tool to Track Global Surveillance Data," *The Guardian*, accessed May 6, 2014, http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining; National Security Agency, "BOUNDLESSINFORMANT - Frequently Asked Questions," September 6, 2012. Another tool is XKEYSCORE. Glenn Greenwald, "XKEYSCORE: NSA Tool Collects 'Nearly Everything a User Does on the Internet,'" *The Guardian*, July 31, 2013, http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

[785] Executive Order 12333: United States Intelligence Activities (2001). *See* National Security Agency Office of Inspector General, "Working Draft Report from March 24, 2009 on Stellar Wind (PSP) [Snowden Leak June 27, 2013]," March 24, 2009 1-3; PCLOB, "Report on the Surveillance Program," 16-18; and Daniel Gallington, "Perspectives on Collection, Retention, and Dissemination of Intelligence," Marshall Policy Outlook (United States: George C. Marshall Institute, May 2014), http://marshall.org/wp-content/uploads/2014/05/Collection-PO-May-14.pdf 2.

[786] Miroslav Nincic and Jennifer Ramos, "Torture in the Public Mind," *International Studies Perspectives* 12, no. 3 (2011): 231–49, 233. *See also* Stewart & Mueller, "Cost-Benefit Analysis of Advanced Imaging Technology, ("Terrorism is a frightening threat that influences our willingness to accept risk, a willingness that is influenced by psychological, social, cultural, institutional processes."); Gallington, "Perspectives on Collection, Retention, and Dissemination of Intelligence," 10 ("While technology is often blamed for loss of privacy, it has also worked to protect us from the insidious threat of terrorism."); Wittes, "The Intelligence Legitimacy Paradox." ("the threat environment America faces is growing ever more complicated"); Princeton Project on National Security, "Report of the Working Group," (9/11 "triggered a revolution in U.S. national security policies"); and Greenwald, *No Place to Hide*. 5 ("the fear of terrorism . . . has been exploited by US leaders to justify a wide array of extremist policies").

Intelligence Surveillance Court (FISC).[787] The program itself went through several iterations as the government struggled to meet constitutional compliance behind closed doors, and it was eventually given statutory authority, albeit in vague terms, in §702 of the Foreign Intelligence Surveillance Act (FISA).[788] At the center of the adjustments was ensuring that the surveillance methods were properly within the bounds of the 4th Amendment.[789] Under the FISA - the same legislation that created the FISC - the US government does not need a warrant to gather "foreign intelligence" from individuals that are not US person and are reasonably believed to be "located outside of the United States."[790] In other words, the 4th amendment does not apply to non US citizens outside the borders of the United States. As a result, the NSA's surveillance was premised on the non-territorial-ness of the

---

[787] NSA OIG, "Working Draft Report from March 24, 2009," 36-37. PCLOB, "Report on the Surveillance Program, 16-18, 42; and United States Department of Justice, "Exhibit A: Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to Be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended," (July 28, 2009). Gallington compares the FISC process to that of "any federal, state or large city court" when they evaluate search warrants or wiretap orders. Gallington, "Perspectives on Collection, Retention, and Dissemination of Intelligence," 5-6. In the case of warrantless mass surveillance FISC reviews both the targeting procedures and the minimization procedures in a review that has been characterized as limited. PCLOB, "Report on the Surveillance Program," 26-27.

[788] Foreign Intelligence Surveillance Act of 1978, 95 Pub.L. 511 (1978). Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, 110 Pub. L. 261 (2008) and
PCLOB, "Report on the Surveillance Program," 19. Sec. 702 was "an attempt to put a statutory framework around activities that were currently ongoing." *Id.* at 81-84. Greenwald and MacAskill note that PRISM was developed because there was a feeling that "FISA was broken because it provided privacy protections to people who were not 'entitled to them." Greenwald & MacAskill, "NSA PRISM Program Taps in to User Data of Apple, Google and Others."

[789] This is the "foreign intelligence exception" to the 4th Amendment. PCLOB, "Report on the Surveillance Program," 89-90.

[790] PCLOB "Report on the Surveillance Program," 20-21. Foreign intelligence is "information that relates to the ability of the United States to protect against actual or potential attack by a foreign power; sabotage, international terrorism, or the proliferation of weapons of mass destruction by a foreign power; or clandestine activities by a foreign power." *Id.* at 22. *See also* Gallington, "Perspectives on Collection, Retention, and Dissemination of Intelligence," 5 ("It is fair to observe that nowhere else in the world do citizens, nationals or residents of a country get the benefit of a presumption such as we have embodied in the 'U.S. Person' concept.").

target. Snowden argues that the use of "foreign" is a "rhetorical shift [that] is a tacit acknowledgement by governments that they recognize they have crossed beyond the boundaries of justifiable activities."[791] Snowden also revealed that the foreign surveillance sometimes bled back through the borders of the United States[792] "turn[ing] the U.S. into a foreign nation electromagnetically."[793] The uses revealed by Snowden show that "[t]echnology is agnostic of nationality," and the United States only required a "reasonable belief" that the individual was outside of United States territory to fulfill the "foreignness requirement."[794] Foreignness is important, because under the international governance system, the US surveillance of its own citizens is legal as a matter of sovereignty. It is foreign surveillance of individuals in territories outside of US

---

[791] Snowden, "Testimony before the Parliament of the European Union."

[792] Gellman & Poitras, "U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program."; Glenn Greenwald and Spencer Ackerman, "How the NSA Is Still Harvesting Your Online Data," *The Guardian*, June 27, 2013, http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection; Greenwald & Ball, "The Top Secret Rules That Allow NSA to Use US Data without a Warrant."; Glenn Greenwald and Spencer Ackerman, "NSA Collected Americans' Email Records in Bulk for Two Years under Obama," *The Guardian*, June 27, 2013, http://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama; James Ball and Spencer Ackerman, "NSA Loophole Allows Warrantless Search for US Citizens' Emails and Phone Calls," *The Guardian*, August 9, 2013, http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls; Barton Gellman, "NSA Broke Privacy Rules Thousands of Times per Year, Audit Finds," *The Washington Post*, August 15, 2013, http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html; and National Security Agency, "(U//FOUO) NSAW SID Intelligence Oversight (IO) Quarterly Report - First Quarter Calendar Year 2012 (1 January - 31 March 2012 - EXECUTIVE SUMMARY," May 3, 2012.

[793] Greenberg, *This Machine Kills Secrets,* 223. *See also* Wittes, "The Intelligence Legitimacy Paradox." ("the same technologies that are making the threat picture more complicated, more diverse, and more bewildering are also bringing the intelligence process into closer day-to-day contact with people living their daily lives."). The original presidential order post 9/11 allowed for counter terrorism surveillance in the United States for "limited time periods," but was later pulled back to covering just foreign intelligence. PCLOB, "Report on the Surveillance Program. The PCLOB also notes that there is a ban on "reverse targeting." *Id.* at 23. It also notes that the technology employed by the NSA is limited in its ability to filter out communications of individuals in the US. *Id.* at 42, 85.

[794] Snowden, "Testimony before the Parliament of the European Union," 5 and PCLOB, "Report on the Surveillance Program, 21, 43-52.

jurisdiction that seems to be most problematic within the international political geography.

It is not exceptional that a portion of the Bill of Rights does not extend outside the borders of the United States as it is a guarantee of rights in the United States some of which implement human rights in a more universal sense. The 4th Amendment is one of those rights that is guaranteed only to citizens and noncitizens within US borders.[795] This does present a somewhat dichotomous position for the United States. On one hand, Secretary of State Clinton argues for the extension of First Amendment rights to Cyberspace, and on the other hand the government is secretly not extending Fourth Amendment rights.[796] The dichotomy exists because the freedom of speech that the government asserts should be extended is protected by the 4th Amendment impediment to government interference in one's private life. So the "universal" rights that Clinton offers are extend unevenly based on a political identity.

The hallmark of the activities exposed by Snowden is the replacement of individualized suspicion of criminality critical in the 4th Amendment's warrant requirement, with a permanently suspect political identity of "foreign."[797] As a result FISC, does not make a determination as to whether a particular foreign individual will be surveilled. Judicial review is instead limited to determining whether the procedures, which are adopted and authorized secretly, "are

---

[795] *Id. at* 86-7. The PCLOB notes that the application of the "right to privacy" found in human rights documents is unclear. *Id.* at 100-102.
[796] Clinton, "Internet Rights and Wrongs: Choices & Challenges in a Networked World." *See also* US DoD, "Department of Defense Strategy for Operating in Cyberspace." (noting Cyberspace's importance in the "spread of free speech").
[797] PCLOB, "Report on the Surveillance Program," 18

reasonably designed" to prevent surveillance of US persons or individuals within the borders of the United States.[798] What is exceptional is the US government's power to actively transform political space outside of its borders. And it is able to do this because "much of the world's communications flow through the US."[799] This means that it is able to leverage its territory into the territory of other states.[800]

What Snowden revealed was not just a surveillance program, but a fundamental shift from the state's point of view in the extent to which it can shape the political geography outside its own borders. It has long been understood that surveillance reshapes space, and that "[p]rivacy has a spatial dimension."[801] This is the core idea in Jeremy Bentham's Panopticon, and Cohen argues that modern rhizomatic surveillance systems dramatically change public and private space.[802] Surveillance "alters the experience of

---

[798] For an example see United States Department of Justice, "Memorandum for the Attorney General: Proposed Amendment to the Department of Defense Procedures to Permit the National Security Agency to Conduct Analysis of Communications Metadata Associated with Persons in the United State," November 20, 2007; United States Department of Justice, "Exhibit A."; PCLOB, "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," 26-27.

[799] NSA, "PRISM/US-984XN"

[800] Lana Lam, "EXCLUSIVE: US Hacked Pacnet, Asia Pacific Fibre-Optic Network Operator, in 2009," *South China Morning Post*, June 22, 2013, http://www.scmp.com/news/hong-kong/article/1266875/exclusive-us-hacked-pacnet-asia-pacific-fibre-optic-network-operator; Lana Lam and Stephen Chen, "EXCLUSIVE: US Spies on Chinese Mobile Phone Companies, Steals SMS Data: Edward Snowden," *South China Morning Post*, June 22, 2013, http://www.scmp.com/news/china/article/1266821/us-hacks-chinese-mobile-phone-companies-steals-sms-data-edward-snowden?page=all; Laura Poitras, Marcel Rosenbach, and Holger Stark, "NSA Spies on 500 Million German Data Connections," *Spiegel Online*, June 30, 2013, http://www.spiegel.de/international/germany/nsa-spies-on-500-million-german-data-connections-a-908648.html.

[801] Cohen, "Privacy, Visibility, Transparency, and Exposure," 181. *See also* Debra Kirby, "Minding the Gap: The Growing Divide between Privacy and Surveillance Technology" (Thesis, Naval Postgraduate School, 2013), http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA585523 10-11.

[802] Cohen, "Privacy, Visibility, Transparency, and Exposure," 184-186

places in ways that do not depend entirely on whether anyone is actually watching."[803] Lessig terms it a "burden" that is imposed on the individual,[804] and Greenwald notes that a citizenry that is aware of always being watched quickly becomes a compliant and fearful one."[805] Transnational surveillance then exerts a new political geography on the individual by placing burdens on him or her which "alters the balance of powers and disabilities" within Cyberspace.[806] As a result, despite the fact that this is a government action, it is one that erodes the borders conceived on in international space, because borders historically inhibited surveillance of this scale and scope. This loss of "political independence" is exhibited in Snowden's testimony before the European Parliament in which he tell the MPs that "without getting out of my chair, I could have read the private communications of any member of this committee, as well as any ordinary citizen."[807] In fact, Snowden's leaks confirm that the United States engaged in just this sort of surveillance,[808] which bears "implications for our assumptions of how international relations unfold."[809]

---

[803] *Id*. at 192
[804] Lessig, *Code 2.0*, 218.
[805] Greenwald, *No Place to Hide,* 3.
[806] Cohen, "Privacy, Visibility, Transparency, and Exposure," 193.
[807] Snowden, "Testimony before the Parliament of the European Union," 2
[808] Ewen MacAskill et al., "GCHQ Intercepted Foreign Politicians' Communications at G20 Summits," *The Guardian*, June 17, 2013, http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits; Laura Poitras et al., "NSA Spied on European Union Offices," *Spiegel Online*, June 29, 2013, http://www.spiegel.de/international/europe/nsa-spied-on-european-union-offices-a-908590.html; Ewen MacAskill and Julian Borger, "New NSA Leaks Show How US Is Bugging Its European Allies," *The Guardian*, June 30, 2013, http://www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies; "NSA Hacked UN Videocalls as Part of Surveillance Program, Claims Report," *Al Jazeera America*, August 25, 2013, http://america.aljazeera.com/articles/2013/8/25/nsa-bugged-u-n-headquarters.html.
[809] J. Dittmer, "Everyday Diplomacy: UKUSA Intelligence Cooperation and Geopolitical Assemblages." *Annals of the Association of American Geographers* 105, no. 3 (04 2015): 604-05.

The ability of the United States to surveil the communications of foreign politicians indicates a change in their political geography, since "[s]paces exposed by surveillance function differently than spaces that are not so exposed."[810]

It should also be emphasized that the state's ability to transform political geography outside of its borders based on its ceding of authority to corporate intermediaries as discussed in the previous chapter.[811] The ability of these networks to expand their reach only extends the reach of the government, and as market actors they incentivize individuals to enroll in the "surveillant assemblage" using "benefits and pleasures, including price discounts, social status, and voyeuristic entertainment."[812] The state benefits from the corporate goal "to harness raw power of data."[813] Indeed the reliance on "private intermediaries has equipped states with new forms of sometimes

---

[810] Cohen, "Privacy, Visibility, Transparency, and Exposure," 194. *See also* Dittmer, "Everyday Diplomacy," 604–19.

[811] *See* Dominic Rushe, "Skype's Secret Project Chess Reportedly Helped NSA Access Customers' Data," *The Guardian,* June 20, 2013, http://www.theguardian.com/technology/2013/jun/20/skype-nsa-access-user-data; James Risen and Nick Wingfield, "Web's Reach Binds N.S.A. and Silicon Valley Leaders," *The New York Times*, June 19, 2013, sec. Technology, http://www.nytimes.com/2013/06/20/technology/silicon-valley-and-spy-agency-bound-by-strengthening-web.html; Glenn Greenwald et al., "Microsoft Handed the NSA Access to Encrypted Messages."; Craig Timberg and Ellen Nakashima, "Agreements with Private Companies Protect U.S. Access to Cables' Data for Surveillance," *The Washington Post*, July 6, 2013, http://www.washingtonpost.com/business/technology/agreements-with-private-companies-protect-us-access-to-cables-data-for-surveillance/2013/07/06/aa5d017a-df77-11e2-b2d4-ea6d8f477a01_story.html. James Ball, Luke Harding, and Juliette Garside, "BT and Vodafone among Telecoms Companies Passing Details to GCHQ," *The Guardian*, August 2, 2013, http://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq; Complainants in the UK referred to this as "the exploitation of network infrastructure" by the GCHQ and alleged numerous violations of rights. Greenet Ltd. et al v. GCHQ - Statement of Grounds (Investigatory Powers Tribunal (UK) 2014).

[812] Cohen, "Privacy, Visibility, Transparency, and Exposure," 187.

[813] *Id.* at 186.

unaccountable and nontransparent power over information flows."[814] It should also be noted that these activities are not limited to the United States, and Snowden revealed a "surveillant assemblage" that includes the United Kingdom,[815] France,[816] Australia,[817] and Germany.[818]

The state ability to transform political geography should also be remembered within the context of it to transform territorial geography discussed in Chapter 6. The IoT allows states to control physical infrastructure in foreign domains as shown with Stuxnet. It also enables digitized violence as found in the United States use of drones. The Predator drone was first developed as a surveillance tool for the air force, a purpose it served until the 2000s when it was fitted with munitions to carry out targeted killings in foreign countries.[819] The Predator is connected to a user in the United States via a communications link built on Internet technology and relayed by a commercial telecommunications satellite.[820] If the drone is understood as a 'thing' on the IoT, then it is the embodiment of digitized violence. The political geography

---

[814] DeNardis, *The Global War for Internet Governance*, 15.
[815] Hopkins & Borger, "Exclusive: NSA Pays £100m in Secret Funding for GCHQ."; Nick Hopkins, Julian Borger, and Luke Harding, "GCHQ: Inside the Top Secret World of Britain's Biggest Spy Agency," *The Guardian*, August 1, 2013, http://www.theguardian.com/world/2013/aug/02/gchq-spy-agency-nsa-snowden; Dittmer, "Everyday Diplomacy," 604–19.
[816] Angelique Chrisafis, "France 'Runs Vast Electronic Spying Operation Using NSA-Style Methods,'" *The Guardian*, July 4, 2013, http://www.theguardian.com/world/2013/jul/04/france-electronic-spying-operation-nsa.
[817] Philip Dorling, "Snowden Reveals Australia's Links to US Spy Web."
[818] "German Intelligence Agencies Used NSA Spying Program," *Spiegel Online*, July 20, 2013, http://www.spiegel.de/international/germany/german-intelligence-agencies-used-nsa-spying-program-a-912173.html.
[819] Arthur Holland Michel, "A History of Violence: How Rogue Techies Armed the Predator, Almost Stopped 9/11, and Accidentally Invented Remote War," *WIRED*, January 2016, http://www.wired.com/2015/12/how-rogue-techies-armed-the-predator-almost-stopped-911-and-accidentally-invented-remote-war/.
[820] *Id.*

ascribed to the targets of these killing by the international system is transformed through Cyberspace.

III. Networked Global Politics

What has been described in the previous two sections is a cross reaching of power, and they both describe changes in the political geography at a localized perspective. A further inquiry would be made into what this does to the political geography of international space. This inquiry will reveal borders are shifted when other entities are networked in at a power level that can directly contest states. One of the implications of the previous two sections is that states have ceded authority in Internet governance, and that they rely on their ability to blend in with nonstate actors online. This section will examine hackivists as evidence of a world scale political geography that networks in nonstate actors. The term itself invokes the idea of changing technology (i.e. hacking) for political change (i.e. activism). Hacktivists "use cryptography to effect political change," as a means of giving power "to the people."[821] This section will trace a narrative of hacktivism that will illustrate this transformation in global political geography.

In November of 2010, the website Wikileaks began to leak US State Department Diplomatic cables from its website, in an incident that came to be known as Cablegate. Wikileaks is a website founded by Julian Assange that is, in its own words, a "multi-national media organization and associated library"

---

[821] Greenberg, *This Machine Kills Secrets,* 131, 168.

that has a perfect record in "resistance to all censorship attempts."[822] The website "specializes in the analysis and publication of large datasets of censored or otherwise restricted official materials involving war, spying and corruption" (again in its own words).[823] Assange has gone so far as to put this in diplomatic terms, stating "WikiLeaks is a giant library of the world's most persecuted documents. We give asylum to these documents, we analyze them, we promote them and we obtain more."[824] According to Domscheit-Berg, Assange focused on the United States specifically "seeking out the biggest possible adversary."[825]

The Cablegate releases were the catalyst for Wikileaks', and Assange's quick rise to global prominence. This led to him being characterized in state rhetoric as a "terrorist" and "outrageous, reckless, and despicable."[826] The releases were unprecedented in nature and caused serious embarrassment for the United States as well as security concerns globally, though Wikileaks did attempt to minimize the exposure of human life. The 251,287 documents gave an unparalleled glimpse into the international relations of the United States, and exposed to the public eye government processes that in general remain closed. They were leaked by a young army soldier named Bradley Manning, who was later prosecuted in the United States for releasing the documents.[827]

---

[822] Wikileaks, "What is Wikileaks" (Nov. 3, 2015) https://wikileaks.org/What-is-Wikileaks.html

[823] *Id.*

[824] *Id.*

[825] Domscheit-Berg, *Inside Wikileaks,* 189. *See also Id.* at 160 (noting Assange stating about the Collateral Murder "I'm off to end a war." The video was footage from a US Apache Helicopter that showed Iraqi civilians being attacked by US forces.)

[826] Greenberg, *This Machine Kills Secrets,* 177

[827] Julie Tate, "Bradley Manning Sentenced to 35 Years in WikiLeaks Case," *The Washington Post*, August 20, 2013,

The United States began to mount a case against Assange, and began to apply diplomatic pressure in order to find a way to get to Assange .[828] Then in August of 2010, a warrant for Assange's arrest was issued in Sweden on the basis of rape allegations.[829] The United Kingdom place Assange on house arrest while it determined whether or not extradition was proper, and the UK Supreme Court determined that extradition was proper in May of 2012.[830] Assange then fled to the Ecuadorian Embassy in London where he was granted asylum. As of this writing, Assange is still in the Ecuadorian Embassy, but the UN Human Rights Council's Working Group on Arbitrary Detention released an opinion in February of 2016 that ruled the detention "arbitrary."[831]

Diplomatic pressure was not the only pressure that the United States mounted. It also attempted to get the corporations within their borders to put pressure on Assange and Wikileaks. To this end payment websites and web service providers were pressured to cease allowing their services to be used to support Wikileaks. Several major companies such as Amazon, PayPal, and Mastercard, succumbed to this pressure displaying the corporate authority over the Internet There was no public legal action taken against these

---

https://www.washingtonpost.com/world/national-security/judge-to-sentence-bradley-manning-today/2013/08/20/85bee184-09d0-11e3-b87c-476db8ac34cd_story.html.

[828] Glenn Greenwald and Ryan Gallagher, "Snowden Documents Reveal Covert Surveillance and Pressure Tactics Aimed at WikiLeaks and Its Supporters," *The Intercept*, February 18, 2014, https://theintercept.com/2014/02/18/snowden-docs-reveal-covert-surveillance-and-pressure-tactics-aimed-at-wikileaks-and-its-supporters/.http://www.thedailybeast.com/articles/2010/08/10/a-western-crackdown-on-wikileaks.html.

[829] Domscheit-Berg, *Inside Wikileaks,* 203-215.

[830] Owen Bowcott, "Julian Assange Loses Appeal against Extradition," *The Guardian*, May 30, 2012, sec. Media, http://www.theguardian.com/media/2012/may/30/julian-assange-loses-appeal-extradition.

[831] UN Human Rights Council's Working Group on Arbitrary Detention, Opinion No. 54/2015 concerning Julian Assange (Sweden and the United Kingdom of Great Britain and Northern Ireland) Para 99.

corporations, and the government denied such actions.[832] This cued the entrance of the hacktivist group Anonymous.

Anonymous is a hacker collective that is geographically distributed and whose identities are as secret as code can keep them. In the group's own words, "Anonymous is a loose collection of individual people around the world. . . . Anonymous is notoriously associated with hacking and hacking operations, but over the years has evolved into a majority protest/civil activist movement."[833] Significantly, Anonymous has no leader and anyone can join.[834] The "nihilistic" group has been associated with a number of high profile hacks that generally have some variety of social justice motive.[835] They have declared operations against groups like the CIA,[836] Westboro Baptist Church,[837] mexican drug cartels,[838] the Church of Scientology,[839] the Islamic State,[840] and even Kanye West.[841] These are the tactics that they employed as Cablegate unfolded. Anonymous employed DDoS attacks against the corporations that they claimed

---

[832] Greenwald & Gallagher, "Snowden Documents Reveal Covert Surveillance" and Clinton, "Internet Rights and Wrongs,"

[833] AnonHQ, "The Most Frequently Asked Questions People Have About Anonymous," (Jan. 16, 2016). http://anonhq.com/43605-2/.

[834] *Id.*

[835] Greenberg, *This Machine Kills Secrets,* 185.

[836] Chloe Albanesius, "Anonymous Takes Down CIA Web Site," *PC Magazine*, February 10, 2012, http://www.pcmag.com/article2/0,2817,2400140,00.asp.

[837] Helen A. S. Popkin, "Anonymous 'Brandjacks' Westboro Baptist Church on Facebook," *NBC News*, April 17, 2013, http://www.nbcnews.com/technology/anonymous-brandjacks-westboro-baptist-church-facebook-1C9395459.

[838] Associated Press, "'Anonymous' Hackers Threaten Drug Cartel," *CBS News*, October 31, 2011, http://www.cbsnews.com/news/anonymous-hackers-threaten-drug-cartel/.

[839] Anonymous and Wikileaks both targeted Scientology. *See* Daniel Domscheit-Berg, *Inside Wikileaks,* 35.

[840] E.T. Brooking, "Anonymous vs. the Islamic State," *Foreign Policy*, November 13, 2015, https://foreignpolicy.com/2015/11/13/anonymous-hackers-islamic-state-isis-chan-online-war/.

[841] "Kanye West Targeted by 'Anonymous' in Searing Video," *Billboard*, March 12, 2015, http://www.billboard.com/articles/columns/the-juice/6501935/anonymous-kanye-west-video.

were censoring Wikileaks.[842] In addition to corporations, Anonymous also attacked governments such as Zimbabwe and Tunisia that were censoring the documents.[843] Anonymous' actions were undergirded by a philosophy that "knowledge is free," a phrase that resonates with the political geography described in Chapter 4.[844]

A third, but unlikely to be final, act in this leaking drama are the leaks of Edward Snowden. Snowden, it must be assumed, was to some extent inspired by this global drama over government transparency, and like Manning he released a trove of government documents to the press. Several days after the first leak, the same journalists that broke the leaks also broke the identity of the leaker by publishing an interview with Snowden. In this interview he stated that he hoped his leaks "will trigger [debate] among citizens around the globe about what kind of world we want to live in."[845] Snowden's interview was from a hotel room in Hong Kong. While the United States scrambled to put in motion the legal process for getting to Snowden, he was quietly shuttled onto a plane that took him to the international terminal of the Moscow airport before

---

[842] Robert Mackey, "'Operation Payback' Attacks Target MasterCard and PayPal Sites to Avenge WikiLeaks," *The Lede*, 1291819254, http://thelede.blogs.nytimes.com/2010/12/08/operation-payback-targets-mastercard-and-paypal-sites-to-avenge-wikileaks/.

[843] "Anonymous Activists Target Tunisian Government Sites," *BBC News*, January 4, 2014, http://www.bbc.com/news/technology-12110892.

[844] Greenberg, *This Machine Kills Secrets,* 185.

[845] Glenn Greenwald, Ewen MacAskill, and Laura Poitras, "Edward Snowden: The Whistleblower behind the NSA Surveillance Revelations," *The Guardian*, June 11, 2013, sec. US news, http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance. Snowden's time in Hong Kong can be seen in the documentary *Citizen Four* (HBO Films 2014).

the United States could cancel his passport.[846] He lived in the international zone of the airport, outside the legal and political borders of any state, for more than a month.[847] During this time, it was rumored that he was going to be given asylum in Bolivia and that he was aboard a diplomatic flight transporting the president of Bolivia.[848] The United States applied a great deal of diplomatic pressure, and as a result Portugal, France, Italy, and Spain denied access to their airspace.[849] The plane was rerouted to Vienna, where it was searched and the Austrian Foreign Minister confirmed that Snowden was not aboard.[850] Snowden was granted a temporary asylum for one year in Russia, which has since been renewed.[851] Snowden was represented by Wikileaks attorneys in the negotiations with the Russian government. In fact, Wikileaks contributed a great deal of resources to ensuring that Snowden did not fall back within the jurisdiction of the United States.[852] From a legal and political enclave of

---

[846] Tania Branigan and Miriam Elder, "Edward Snowden Leaves Hong Kong for Moscow," *The Guardian*, June 23, 2013, sec. US news, http://www.theguardian.com/world/2013/jun/23/edward-snowden-leaves-hong-kong-moscow.

[847] Alec Luhn, "Edward Snowden Leaves Moscow Airport after Russia Grants Asylum," *The Guardian*, August 1, 2013, sec. US news, http://www.theguardian.com/world/2013/aug/01/edward-snowden-grant-temporary-asylum-russia.

[848] Dan Roberts, "Bolivian President's Jet Rerouted amid Suspicions Edward Snowden on Board," *The Guardian*, July 3, 2013, sec. World news, http://www.theguardian.com/world/2013/jul/03/edward-snowden-bolivia-plane-vienna & Kathy Lally and Juan Forero, "Bolivian President's Plane Forced to Land in Austria in Hunt for Snowden," *The Washington Post*, July 3, 2013, https://www.washingtonpost.com/world/bolivian-presidents-plane-forced-to-land-in-austria-in-hunt-for-snowden/2013/07/03/c281c2f4-e3eb-11e2-a11e-c2ea876a8f30_story.html.

[849] *Id.*

[850] *Id.*

[851] Branigan & Elder, "Edward Snowden Leaves Hong Kong for Moscow."

[852] Michael B. Kelley, "Edward Snowden's Relationship With WikiLeaks Should Concern Everyone," *Business Insider*, January 4, 2014, http://www.businessinsider.com/edward-snowden-and-wikileaks-2014-1 and Matt Sledge, "Edward Snowden Gambles On Alliance With WikiLeaks," *The Huffington Post*, June 27, 2013, http://www.huffingtonpost.com/2013/06/27/edward-snowden-wikileaks_n_3506232.html.

Ecuador in the territory of the United Kingdom, Assange was able to wield global political power to subvert the international power of the United States.

This narrative is not intended to lionize Assange, Manning, Snowden, or the members of Anonymous. The facts surrounding each require particularized ethical reflection. Instead, this narrative is used to expose a new form of global networked power that is pushing up against the territorially ordered international political system. Three observations of this narrative illustrate aspects of the new political geography formed as cybergeography comes into proximity with international geography. The first observation is the role of encryption technologies within this narrative. Greenberg notes that "the technology that enables the spillers of secrets has been accelerating with the dawn of the computer" and that the Internet caused a "cambrian explosion" of tools to empower the individual.[853] Encryption technologies are foundational to the Wikileaks platform, critical to hiding the identity of Anonymous activists, and were the tool used by Snowden to transfer his leaks to the press. In the Cablegate episode, Manning may never have been caught except that he revealed himself to a fellow hacker that turned him in,[854] and Snowden revealed his own identity. Encryption allows the leaker to transform politics within the global space by transforming their own identity, a function enabled within the communicative condition of Cyberspace.

The second observations is the role of borders within this narrative. Borders are freely deconstructed and reconstructed at will by states creating

---

[853] Greenberg, *This Machine Kills Secrets,"* 6.
[854] *Id.* at 31-32.

ripples in the construction of the International system. Borders themselves are recoded to hold both traditional content as well as new fluid geographies. For instance, at numerous points we see borders forming traditional functions. Assange is subject to the international process of extradition, but he claims asylum within the diplomatic borders of Ecuador. Assange is thus protected through established international governance mechanisms. Similarly, Hong Kong allowed Snowden to leave for Moscow claiming that "documents filed by the US did not fully comply with legal requirements."[855] In addition, we see a display of states flexing their territorial authority in denying their airspace to a plane that potentially carried Snowden. At the same time, borders are reinscribed in different ways that reveal their imaginariness. Assange's exile reveals the legal fiction of territory, which gets highlighted when the same type of diplomatic territory is so easily violated in the case of the Austrian search of Bolivia's diplomatic flight. Similarly, Snowden's existence in the nowhere of an airport displays the fictions of territory. While Assange and Snowden are relying on international geography for protection they reveal the imaginaries that surround the individual and hack together new spatial realities for themselves. The role of territorial, legal, and political borders across this narrative arc is indicative of geographic duality that Cyberspace enables. Individuals, exploit the geography of Cyberspace and remained unconfined in their ability to reach out and affect processes outside the territory in which they exist.

---

[855] Branigan & Elder, "Edward Snowden Leaves Hong Kong for Moscow."

Finally, the articulation of power within this narrative shows new patterns that reflect a new shape of world scale political geography. Within this narrative states are engaged in international politics in order to resolve the issues caused by transnational actors. This power though is often inflected through corporate power structures as can be seen in the Cablegate episode and in the programs such as PRISM that Snowden unveiled. The state's power is now part of a, pardon the pun, diversified portfolio. Power is inflected back at the state thing through individuals that assert themselves as adversary's to the state on equal grounds and become "global political player[s]."[856] Though each has their own interesting spatial standing, each is able to leverage themselves in such a way that they challenge the political space of the state from outside of its political geography. Interestingly, Assange is reported to have "adopted the language of the power mongers he claimed to be combatting," which shows how he was positioning Wikileaks as an adversary of equal standing to the state.[857] These acts are beyond civil disobedience, which is "a public nonviolent conscientious yet political act contrary to law" with the goal of changing the status quo.[858] These technologies remove the "price" of legal consequences through the use of encryption technologies.[859] Instead, as an anonymous author stated in *2600: The Hacker Quarterly* "[h]ackers are no longer anonymous independent operators or groups: We are now a known and calculated factor" in power structures.[860] While this is easily read as boastful, it

---

[856] Domscheit-Berg, *Inside Wikileaks,* 270.
[857] Domscheit-Berg, *Inside Wikileaks.* 200-201.
[858] Rawls, *A Theory of Justice*, 364.
[859] Rawls, *A Theory of Justice*, 367.
[860] Prisoner #6, "The 21st Century Hacker Manifesto." 50.

is hard to ignore the attention that cybersecurity is receiving at the top levels of governments and corporations, among others. Indeed, governments, corporations, and hacktivists much be examined together to reveal "the baroque workings of power" in global politics.[861] These "baroque workings" are highlighted not just by attacks on corporations and states by groups like Anonymous, but also in cases attacks on corporations by states such as North Korea and Sony.

Geographic duality is maybe the best way to describe the situation in which Cyberspace exists within international space and international space exist within cyberspace creating a unified world scale geography in which neither is dominant. While this rings like an attempt at empty metaphysics, we find it reflected in the architecture of Cyberspace. The physical layers of Cyberspace and the users in Cyberspace exist within the borders of the state and therefore within the borders of the international. But the logical layer of the Internet is made of algorithms, and these are ideas operationalized through machinery.[862] This means that the logical layer is a manifestation of human consciousness. Or in simpler terms, the logical layer is ideas, and ideas are notoriously hard to control.

* * * * *

This chapter has shown how world scale political geography is shifting as new actors become mediums for power within the system. This chapter has

---

[861] Dittmer "Everyday Diplomacy," 616.
[862] David Berlinski, *The Advent of the Algorithm: The 300-Year Journey from an Idea to the Computer,* xii.

served as a capstone for Part II which highlights encounters where cybergeographies come into proximity of international geographies. The various cases and incidents addressed in this section are meant to reveal complexity within the system by layering the spatial, legal, and political geography of Cyberspace. This layering shows the junctures and disjunctures of these two intermingled geographies, the following final chapter will pull these various threads together and posit that Cyberspace short circuits international governance processes and allows actors to reprogram the world.

Conclusion

"The algorithm has come to occupy a central place in our imagination. It is the second great scientific idea of the West. There is no third."

- David Berlinski

Chapter 9

Reprogramming the World

In 1515, a live rhinoceros arrived in Portugal. It was a gift Sultan Muzafar II of Gujarat to King Manuel I of Portugal. Thing King gifted the creature on to Pope Leo X, but the rhino died in transport. The pope instead received the taxidermied corpse, and German artist Albrecht Dürer based a drawing he titled *Rhinoceron* on a sketch and second hand description of that corpse(See Fig 9.1). This drawing was then turned into a woodcut that made it reproducible on the printing press. Dürer's rhinoceros, though fairly innacurate was reproduce through the printing press and became the dominant depiction of the rhinoceros for well over a hundred years. The medium introduced by Gutenberg, facilitated the spread of an idea that became tenaciously melded into the public understanding of what constituted the thing that was signified by a rhinoceros.[863]

[863] David Quammen, *The Boilerplate Rhino: Nature in the Eye of the Beholder* (New York: Scribner, 2000) 201-209.

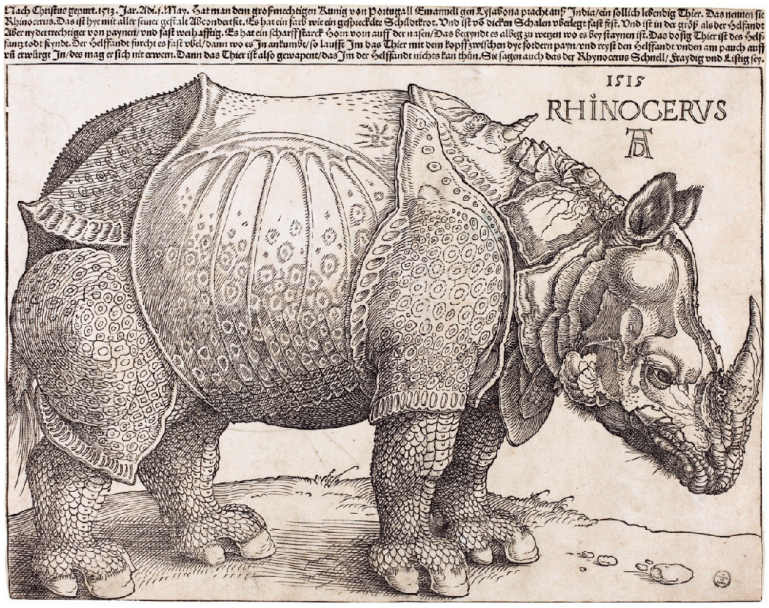

Fig. 9.1: Albrecht Dürer's *Rhinoceron*.

The "boilerplate rhino" is a function "Gutenberg's revolution," and it illustrates the ability of ideas to entrench themselves through reproduction.[864] The power of the image is itself a function of its reach, and Dürer's decision to make the image a woodcut shows his intent for mass market publication.[865] Similarly, Chapter 5 discussed the power of cartography in constructing imaginary cartographies. These images of the international system are the graphic conceptualization of the "Westphalian state." This term itself is one that has been entrenched through repetition and reification and is still used to describe the international system despite the dramatic differences between the contemporary state and the state that emerged from the Peace of Westphalia.[866] The resulting 'boilerplate state' is one that reifies its border

[864] *Id.* at 203.
[865] *Id.* at 206.
[866] *See generally* Clark, *Legitimacy in International Society*, 51-70.

through the projection of legal jurisdiction and political identity across a spatial geography denoted by solid black lines on a map. The Westphalian imaginary was repeatedly recast onto the developing international system as a descriptor and a depictor.

This final chapter will examine how Cyberspace reprograms international governance. The first section of this chapter will use the metaphor of lawmaking as programming as an analytic lens to show how Cyberspace changes the processes of the international system. The second section will then delve into some of the theoretical implications of a reprogrammed world. Specifically, this section will examine the connection between a global cybergeography and the project of Cosmopolitanism and global governance. The final section will identify challenges and questions that a reprogrammed world presents for future research.

I. Rule by Algorithm

Director Terry Gilliam's film *Brazil* paints a dystopian future governed by complexly bureaucratic government.[867] In the film, a farcical error in a printer causes the death of a innocent civilian by putting in motion a bureaucratic process that runs to completion. The terrorist, played by Robert De Niro, is a renegade heating and air conditioning repairman who now fixes HVAC systems without filing the proper paperwork, much to the chagrin of the process oriented government. The film's aesthetic is marked by the use of bizarre machines that personify the complex bureaucratic machinations of the

[867] *Brazil* (Embassy International Productions/Brazil Productions 1985).

governance system. Indeed, De Niro's character, Archibald Tuttle's crime of terror is short circuiting the governance system and bypassing established processes. In the world Gilliam creates, code is not law as much as law is code.

What Gilliam portrays in *Brazil* is an farcical version of what George Orwell's grim depiction in *Nineteen-Eighty-Four*.[868] It is a government that has become so process burdened, that its own existence and internal legitimacy seem to be functions of its processing power - its ability to administer its state. What these two artists, who certainly are not alone in their use of this trope, are exploiting is the metaphor of governance as a machine. The metaphor is an apt one, and one can almost see Orwell having the cogs of the Enigma machine in mind as he was writing his work in the 1940s. The reason that it has such power is that the modern bureaucratic state emerges with the industrial age. Bureaucracy is a form of government that is meant to work like a machine to some extent. Lawmakers make laws that are then implemented and carried out by government officials. In this model, lawmakers define the inputs and the outputs and the administrative branch of government devises procedures (i.e. regulation) for accomplishing these tasks. While administrators make decisions, the processes they must follow confine their actions in such a way as to ensure the legislated outcomes.

If it is accepted that code is law, then programmers are lawmakers. Whether they are working to spec on a contract or working for their own personal purposes, programmers create rules by writing algorithms. Computer programs are made of algorithms, which are "*effective procedure*[*s* or] a way of

---

[868] George Orwell, *1984* (London: Secker & Warburg 1949).

getting something done in a finite number of discrete steps."[869] This is the similar role of procedural legitimacy, which seeks to set procedures that reproduce just outcomes consistently. Rawls, for instance, noted this metaphorical link between computing and governance, describing the "political process as a machine which makes social decisions when the views of representatives and their constituents are fed into."[870] This observation points to the central metaphor employed by this section which is understanding law as code. This metaphor will be used as an analytic tool to illustrate pragmatically how Cyberspace reprograms world. At the outset, it should be noted that this is a limited metaphor, but it is being used at a very high level of application in order to illustrate why the model presented herein matters to scholars of international governance.

Computer code is esoteric to the average individual despite its ubiquity. It is the magic in the machine that is often depicted in movies as a dizzying stream of green 1s and 0s whizzing past coders typing at lightening speed. While computer code can be quite complex, how it functions should not be esoteric. Code can be understood as a syntax for instructions to produce different results. Code is a manifestation of formal logic in that it often occurs as if/then and x = y type statements. Code is quite simply, a set of instructions or procedures.

Code tells the computer (i.e. the machine itself) what to do through a set of logical arguments that come in a specific order. As an example, a

---

[869] David Berlinski, *The Advent of the Algorithm,* xvi.
[870] Rawls, *A Theory of Justice*, 196.

microcontroller is a small computer that can be programmed to manipulate physical objects. Beginners are often taught how to write code that uses microcontroller to turn an LED light on and off with the press of a button. This code functions in a series of steps (see Fig. 9.2). It will first assign the button to an input and the LED to an output. Next, it will tell the computer to check the state of the input and store it. Then it instructs the machine that if the button is pushed, then the light should be turned on. Otherwise, the light should be off. These procedures run over and over constantly monitoring for the state of the button and adjusting as necessary. Until the program is stopped these are the rules that govern the functions of the machine by instructing how to turn its inputs into outputs.

```
#define LED 12            //assigns LED to output pin
#define BUTTON 7          //assigns button to input pen

int val = 0;              //val is a variable used to
                          //store the staof the input
int state = 0;            //state is a variable,
                          //0=LED on & 1 =LED on

void setup()              //portion of the program sets up
                          //microcontroller
{
  pinMode(LED, OUTPUT);    //LED is an output
  pinMode(BUTTON, INPUT);  //BUTTON is an input
}

void loop()                  //the procedures that will be repeated

{
  val = digitalRead(BUTTON);  //read the input and store it as val

  if (val == HIGH){           //Check to see if the button is pressed
    state = 1 - state;        //Change state variable

  }
  if  (state == 1) {          //if the button is pressed
    digitalWrite(LED, HIGH);  //turn on the LED
  }
  else {                      //if the button is not pressed
    digitalWrite(LED, LOW);   //turn off the LED
  }}
```

Fig. 9.2: Simple Arduino microcontroller program from turning and LED light on and off with a button. Adapted from Banzi.[871]

One of the unexplored areas of Lessig's code is law principles is the use of it as a means to reflect back on law as code. In a modern bureaucratic state,

[871] Massimo Banzi, *Getting Started With Arduino*, 2nd ed. (Beijing: O'Reilly 2011).

law can be explained in terms of code.[872] In this model a State's constitution is an operating system, its legislation becomes its programs, and regulations become the procedures that are performed over and over to produce results, such as justice, until the program is changed by users. The international system is akin to a network that connects the various operating systems and mediates the interactions between these autonomous computers.

The first thing to note here is how this connects with legitimacy as discussed in Chapter 4. The legislature in this model sets outputs which include things such as practical outcomes (e.g. the lowering of crime), efficiency (e.g. maintaining processing power), and political outcomes in terms of rights. The procedure serves the purpose of maintaining consistency in these outcomes. The procedures also serve as a verification mechanism that allows users to ensure that the system is properly programmed to produce to desired outcome. The procedures are used to compute or process outputs consistent with the requirements of substantive legitimacy within that operating system. Procedures are meant to be a limitation of choice to exclude the whims of individual government agents from the governance process.[873] This is similar to a computer program which is a set of processes that the computer goes through in order to create an output, the major difference being that the computer, without reprogramming, is unable to violate the rules it has been given, whereas the administrative official can violate those rules.

---

[872] Berlinski, *The Advent of the Algorithm,* xiii ("A digital computer may well do what a bureaucracy has done").
[873] Coicaud, *Legitimacy and Politics*, 32.

This difference aside, at a high level we can see that the metaphor of law as code reveals something interesting about the nature of governance. Programming is a skill that requires a coder to conceptualize and set outputs of a program through a set of instructions written in a standardized language. Importantly, different programmers accomplish tasks in different ways, and they must make decisions that balance between practical outputs, processing power, and substantive outputs for the user of the program. The nature of the computer transforms the governance as machine metaphor into a governance as computation metaphor. The "abstract norms that obtain regularity and predictability" for programmers are written in algorithms.[874] The algorithm itself emerged well before the computer and was posited as a way in which abstract mathematical formulas could be used to describe quite literally the entire cosmos.[875] The algorithm found in the digital computer a device that could make its output manifest. The algorithm is process through which programmers can manipulate and recreate the world, it allows for the creation of imagined spaces and Cyberspace might best be understood a multiverse of ideas.[876]

Law and regulation are similarly ideas that are given effect through the bureaucratic administrative machine. A simple government program for the disbursement of a government benefit functions analogously. Legislation defines the inputs and outputs and regulations then puts into place a series of

---

[874] *Id.* at 20.
[875] David Berlinski, *The Advent of the Algorithm*.
[876] For example, Tanz states that designing video games is like "beta testing a universe."Jason Tanz, "Playing for Time: A Father, a Dying Son, and the Quest to Make the Most Profound Videogame Ever," *Wired*, January 2016, http://www.wired.com/2016/01/that-dragon-cancer/. *See also* Lloyd, *Programming the Universe*.

procedures that government officials use to process public administration. A citizen seeking to claim a benefit would give inputs required by the program. These inputs would then be checked against a set of variables or criteria. If the individual meets those criteria the official disburses the benefit, else the government official does not disburse the benefit.

In this metaphor, the international governance system becomes a networking protocol that allows the state operating systems to communicate by instituting transaction points for the different systems to communicate, such as the ITU. The protocol though, is one that facilitates interconnection and not interoperability. As a result it requires those it connects to have certain features in order to take part in the network. This allows us to probe why Cyberspace is can be said to reprogram the world. As noted in Chapter I, international governance has historically been successful at deploying international law that governs world scale technology, but it has been unable to encompass Cyberspace technologies effectively within its regime. It is submitted here that this is a direct result of the materiality of international governance. The territorial rootedness of the international system indicates a need for transnational physicality in order for it to effectively interconnect parties for solutions. As noted in Chapter 7, the ITU's ability to successfully govern international telecommunications is a function of its ability to create law that governs the physical circumstances of the technology, but not the ideational content carried on that technology. This is a constant theme in international law. A good example can be found in the Genocide Convention and the UDHR, which were both passed in December 1948. The Genocide

Convention did not include a provision on racist and discriminatory speech, because the United States opposed its inclusion on grounds that it violated the right of free speech.[877] The UDHR, on the other hand, included the right to free speech, but was not adopted as a binding treaty and the Soviet States abstained from voting.

In international governance, the state is the only device that can connect to the network and take part as a full member of the political geography. International governance is only equipped with the tools that ensure "territorial integrity" against physical incursions. Ideational incursions have always been outside the realm of the international network, and states have been left free to control these incursions in a best efforts system. The international network then is not interoperable, because of the operating systems are able to resist certain inputs. The physical layer of the internet are clearly technologies that the the international system is equipped to regulate fueling realist interpretations of Cyberspace. The logical layer though subverts the physicality of that border crossing by freeing content from its analog barriers. The protocols that function at the core of the internet pushes code-making abilities to the user by making human interaction interoperable across borders. It breaks the strictures of the operating system allowing for geographic convergence and multiplying interaction points.

An example might better illustrate this. The operating system on a device limits the types of instructions that that device can run, which limits the programs it can run. In the early days of computing the operating system was a

---

[877] Schabas, *Genocide in International Law*, 320.

significant limitation on what programs one could run, and it can still be very limiting. Applications like Google Docs[878] subvert the strictures of the operating system by allowing the user to run a program through their web browser, erasing the borders set by the operating system. This is analogous to what is happening in the international system. The logical layer of the Internet is at once content and medium; the medium is literally inseparable from the message.[879] This allows interoperability not conceived of within the international geography. This give entrance to hackers like Assange who are literally able to hack to international network. Cyberspace is a geography that enables individuals, corporations, and states to short circuit the international protocols creating interoperability across borders and across actors.

What this reveals is that law is code is just as important as code is law. For instance, the mass surveillance discussed in Chapter 8 allows the state to extend its law and power over individuals outside its borders in contravention of the assumed materiality found in international governance. The state is clearly circumventing the coordinating process of the international system through Cyberspace. This hack can not be patched by international governance, because it has never been vested with the ability to regulate ideas. The technology opens the possibility of global interoperability.

---

[878] This research was written in Google Docs, and a substantial amount of research was done through Google Scholar.
[879] *See* Berlinski, *The Advent of the Algorithm*, 309-310.

II. A Digital Cosmopolis

Much of the juxtaposition in this research has been to pit Cyberspace in contrast to 'realist' readings which tend to imagine the state as pursuing its interests against other states using power, which is embodied by military might and economic wealth, or blood and treasure.[880] While a reprogrammed world does not completely diminish realism's explanatory power, it does remove the state from dominance in its control of a number of activities including war. For instance, while Stuxnet is could read in realist terms, such an analysis will likely gloss over some of the central problems that Cyberspace causes for realism. The primary problem is in realism's conception of power. Power in terms of military might is no longer something monopolized by the state. The state still has access to and the ability to wield power in Cyberspace, but it is no longer the sole holder of that power. Power itself has been reprogrammed so as to allow others to wield power similar to the state. Similarly, power in terms of treasure have changed as well. Technologies like Bitcoin have changed the nature of currency, removing the state's ability to control the flow of funds. Digitized power is transferable to other entities beside the state

This critique of realism, might lead one to try and place the reprogrammed world within the context of cosmopolitan theory. Cosmopolitanism exists in various forms, but its theorists all converge on the idea of a world governance system that extends political and social rights to

---

[880] Simon Caney, "Review Article: International Distributive Justice," *Political Studies* 49, no. 5 (2001): 986-87.

individuals as opposed to states.[881] These theorists argue that the development of a world scale governance order of this type is the only way to overcome the various injustices observed in states globally by extending "[p]rinciples of distributive justice . . . [to] a global scope."[882] Cosmopolitanism is different in scope from the "loose community of states" represented by the UN. It is a project that seeks ways to form a "community of world citizens, who can legitimate their political decisions . . . on the basis of democratic opinion."[883] Cosmopolitan theorists extend reciprocal rights and obligations from the sphere of the state, making a universalist claim giving individuals "moral personality."[884]

At face value, Cosmopolitanism seems like a theoretical outlook that can accommodate the alternative geographies of the reprogrammed world, since the Internet "has unleashed the extraordinary possibility for many to participate in the process of building and cultivating culture that reaches far beyond local boundaries."[885] Even Schmitt notes the power of a "global consciousness . . . oriented to a common hope" in the shaping of world space.[886] Cosmopolitanism embraces such respatializations as it itself pushes a global rather than international perspective abandoning the "state [as] the natural

---

[881] *See generally*, Caney, "Review Article"; Campbell Craig, "The Resurgent Idea of World Government," *Ethics & International Affairs* 22, no. 2 (2008): 133–42; and Fred Dallmayr, "Cosmopolitanism: Moral and Political," *Political Theory* 31, no. 3 (2003): 421–42.
[882] Caney, "Review Article," 975.
[883] Habermas, *The Postnational Constellation,* 105-106. *See also* Held, *Democracy and Global Order*, 22-23.
[884] Caney, "Review Article," 977.
[885] Lessig, *Free Culture, 9*.
[886] Schmitt, *Nomos of the Earth*, 50.

container of and vehicle for politics.[887] Cosmopolitanism even shares rhetorical and discursive ties to cyber-utopians like John Perry Barlow.[888]

Indeed, despite the decentralized nature of Cyberspace, its technology holds a hope for cosmopolitanism. Cyberspace display the ability to reconceptualize world space and connect individuals without the interference of the state. Multistakeholder governance reflects core notions of cosmopolitanism in its deliberative approach which places governance in a "global context . . . defined by multiple and overlapping networks.[889] Cyberspace represents "global space," and as a result from the perspective of the cosmopolitan it manifests the possibility of new global imaginations. So for instance, social movements using Cyberspace often employ "cosmopolitan repertoires."[890] Pragmatically, the technology could help to fill gaps in data that would be critical to any such enterprise,[891] and it holds the most promise as a technology for facilitating world scale deliberation.

Despite the hope found in the technology, the reprogrammed world does not necessarily mesh with Cosmopolitanism. Central to this is the authority structure that discussed in Chapter 7. The Internet as part of its code bucks centralization. A core function of the packet switching is to eliminate "global control."[892] So while Cosmopolitanism seeks the "establishment of some sort

---

[887] *For instance* Goodhart, "Human Rights and Global Democracy," 401.
[888] *See generally* Fred Turner, *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network and the rise of Digital Utopianism* (Chicago: University of Chicago Press 2006).
[889] Goodhart, "Human Rights and Global Democracy," 401-402.
[890] Fielder, "The Internet and Dissent in Authoritarian States," 167.
[891] *See generally* Jean-Marc Coicaud and Ibrahim Tahri, "Nationally Based Data: Challenges for Global Governance (and Global Policy)," *Global Policy* 5, no. 2 (2014): 135–45.
[892] Leiner et al., "A Brief History of the Internet."

of authoritative regime" to spread equality, Cyberspace only serves to unite the globe through an interoperable protocol which fragments the world into networks.[893] Cyberspace does not seek equality in its users, only interoperability. So while Cyberspace opens a global geographies, it can not be said to have yet opened a cosmopolitan geography that could accommodate deliberative democracy of a global scale.

What this tells us is that while Cyberspace presents an unprecedented opportunity for the deployment of cosmopolitan or utopian visions, technological determinism is a mistake. Technological solutions for building world scale community were critiqued as early as the 1930s through "skepticism about the capacity of a global community of connectivity to transmute into a global community of responsibility."[894] The technology itself may be a necessary precursor to s cosmopolitan system, but is not sufficient by itself.[895] Despite all the tools that Cyberspace presents "society may lack the informational tools necessary to involve everyone in democratic decision-making and to foster widespread economic and social flourishing."[896] As a result despite the increase in intercultural interchange "global democracy is nowhere in sight,"[897] and "programmed utopias" should likely be met with

---

[893] Craig, "The Resurgent Idea of World Government," 135.
[894] Critque by Reinhold Niebhur in Menon, "Pious Words, Puny Deeds 236. *See also* Cooper, "What Is the Concept of Globalization Good For? 193 ("The concept of territory and connectivity has been reconfigured many times; each deserves particular attention.").
[895] Streck, "Pulling the Plug on Electronic Town Meetings," 19 ("the promises of spiritual and or social transcendence in cyberspace rest on a sent of untenable assumptions concerning the nature of technology, experience, communication, and culture.").
[896] Goodman & Chen, "Modeling Policy for New Public Service Media Networks," 114.
[897] J. Mohan Rao, "Equity in A Global Public Goods Framework," in *Global Public Goods: International Cooperation in the 21st Century*, ed. Inge Kaul, Isabelle Grunberg, and Marc Stern (New York, Oxford: Oxford University Press, 1999), 68–87, 68

skepticism.[898] Technology is powerful, but cosmopolitanism is still at its core a problem of developing global knowledge."[899]

It is easy to view Cyberspace as a tool with with which to reprogram the world into a digital cosmopolis, but the capability of the technology to restructure global affairs along cosmopolitan values will be closely related to how Cyberspace itself is governed. As Lessig reminds, the Cyberspace that currently exists is not the only Cyberspace possible.[900] Whether or not cosmopolitan geographies are possible, will depend in large part of the innovative capacity that is pushed to the edges of the networks.

III. Defragmenting the International

This research posits that the international system developed to coordinate world scale governance in the wake of WWII is being transformed by cyber-technologies that are driving a reconceptualization of global order. The first section in this chapter used the metaphor of programming to show how Cyberspace allows borders to be hacked and recoded. The second section used cosmopolitanism as a lens through which to show that though Cyberspace helps to conceptualize other global geographies, it has it's own logics that these structures must also contend with as they seek to build global knowledge. These two discussions both point to uncertainty in the future that Cyberspace might enable. This is because the "mental consequences of the Internet . . . are

---

[898] Bearman, "The Untold Story of Silk Road."
[899] Featherstone & Venn, "Problematizing Global Knowledge and the New Encyclopaedia Project," 10-11.
[900] Lessig, *Code 2.0*, 31-37.

still very hard to assess."[901] One thing should be certain though, and that is that Cyberspace is going to continue to shape the space in which global affairs unfold. This calls for tracking future encounters between Cyberspace and international geography to build a proper understanding of how geography is being reprogrammed. Outside of defining the nature and scope of systemic changes, there are a number of theoretical questions that are ripe to be evaluated in light of restructured world scale geography.

The primary question that should be raised is how we can conceptualize the legitimation within dual geographies. There is need international legitimacy and Cyberspace legitimacy are based on different principles, but they both tap into similar ideas of democracy and human rights.[902] For instance, the Western liberal democratic state is premised on representative democracy in which voters are defined by territory. Cyberspace as a spatial territory is everywhere, so internet governance communities depend on democratic voting but are open to participation by all interested individuals. Legitimacy though is closely tied to consent, which is skewed as a result of Cyberspace. The state's ability to legislate change in the Internet within its territory maintains the risk of changing the Internet in another state's territory contrary to the consent of its citizens. At the same, a small group of elites that form IGCs can make decisions based on consent that can change how the Internet works without going through processes established within a state to

---

[901] Jürgen Habermas, *The Postnational Constellation*, 43.
[902] *Id.* at 119 ("human rights provide the sole recognized basis of legitimation").

ensure in part the administration of justice.[903] This raises deep questions about the nature of legitimacy within the space of multiple dynamic regulatory systems.

A second, related question is what the nature of democracy is within Cyberspace. Cyber-utopians have long called for community governance arguing that such governance is more democratic, but the suggestion that "democracy in cyberspace means democracy in the real world . . . is false."[904] Democracy, however, is not a static condition, and the democracy that is seen in IGCs is open and inclusive in thought, but participation is de facto limited by the high level of technical knowledge needed to meaningfully participate. This means that not only are most people unable to engage in these processes, the processes themselves are in potential danger of being co-opted by groups that flood the membership of IGCs. Corporations and states can send individual representatives to take part in the deliberations and are seemingly not limited to a single representative since membership is open to individuals. In other words, how do users reconcile their "multiple identities" and "plural affiliations," and take part in multiple governance systems.[905]

Additionally, community governance can be seen to have undemocratic tendencies, and can come in "its form of lynch-mob" sanctions.[906] Libertarian

---

[903] Alvestrand & Lie, "Development of Core Internet Standards," 129 ("there is no formal requirement for qualification as an IETF member, but the people who participate tend to be networking professionals.")
[904] Streck, "Pulling the Plug on Electronic Town Meetings," 18–47, 40. Streck also notes that Cyberspace may be "more anarchic than democratic." *Id.* at 41.
[905] Amartya Sen, "Global Justice: Beyond International Equity," in *Global Public Goods: International Cooperation in the 21st Century*, ed. Inge Kaul, Isabelle Grunberg, and Marc Stern (New York, Oxford: Oxford University Press, 1999), 116–25, 120-121
[906] Tambini et al., *Codifying Cyberspace,* 3.

coders have even sought to use it as a marketplace for assassinations.[907] Thus, a second layer of questions on democracy in Cyberspace result from the fora of public discourse being privately owned social media platforms such as Facebook and Twitter.[908] While a private fourth estate has been considered central to liberal democracy, the lines become blurred through the phenomenon of the "citizen reporter." The Wikileaks controversy is instructive as it shows how states can use diplomatic pressure to place burdens on expression through pressure on dominant corporations. This example shows that "the privatization of information flows offers possibilities for private monopoly and sub-optimal exclusion of social groups."[909] These technologies recode the public discursive space, and democracy under such conditions is insufficiently theorized.[910]

Third, and building upon the previous two questions, is what the nature of global multistakeholder governance will be as it unfolds as a new category within world scale governance structure.[911] This question is one of determining how such a governance structure, that removes the state from the dominant role will interact with international government mechanisms. This new category of governance will create rules and norms that can be made effective within the territory of the state without the consent mechanisms found in

---

[907] Greenberg, *This Machine Kills Secrets*, 69-70 and Bearman, "The Untold Story of Silk Road."
[908] DeNardis & Hackl, "Internet Governance by Social Media Platforms."
[909] Tambini et al., *Codifying Cyberspace,* 10.
[910] *See generally* Andrew Chadwick, "Bringing E-Democracy Back In Why It Matters for Future Research on E-Governance," *Social Science Computer Review* 21, no. 4 (2003): 443–55.
[911] Leiner et al., "A Brief History of the Internet." ("The most pressing question for the future of the Internet is not how the technology will change, but how the process of change and evolution itself will be managed.").

international organizations. Multistakeholder governance is still an emerging concept and it is still yet to be defined with much clarity.

Finally, a raft of ethical and philosophical questions arise in terms how to best structure Cyberspace. Its design is currently foundational to the way in which it alters geography, and its architecture is a highly contested in a number of fora.[912] If we accept that "we can and we should make more use of technology for participatory democracy," then there are critical issues to ensuring that Cyberspace governance maintains that possibility,[913] so that it can "promote communicative opportunities."[914] Cyberspace, like other major technological advances, has already changed the world, but there is a challenge in ensuring that it continues to impact the world in a positive manner. As we see with Stuxnet and with its use by terrorists, Cyberspace also has the potential to be used in a way that causes harm to humanity as a whole. As a result, it should be expected that Cyberspace governance will become more contested as its uses and reach increase. Amidst policy circles there is a need for understanding the role of Cyberspace in the reprogrammed world, and the technical nature of its social imbrication. Cyberspace is an incomplete, and likely an incompletable, process. Based on the logic of the algorithm, Cyberspace grows at the rate of ideas. As a result, to some extent we can think of Cyberspace as a manifestation of the human consciousness. Cyberspace is more than just technical standards, and governance as a result must contend with the age old problem constructing political space that allows freedom of

---

[912] *See generally* DeNardis, *The Global War for Internet Governance*.
[913] Noveck, "Designing Deliberative Democracy in Cyberspace," 5.
[914] Goodman, "Media Policy and Free Speech," 1211.

ideas, but at the same time keeps the governance structure from collapsing on itself.

The questions raised here are by no means ignored in the vast literature on Cyberspace, but they are most often engaged with at the level of particular technologies. These questions are raised here in relation to Cyberspace as an alternative geography to the international. The international system is a legal and political settlement that defines territorial space, but Cyberspace is a technology that is uprooting that settlement by recoding the borders that the international constitutes, and as such these questions need to be contemplated on as the technology continues to reshape global social life.

* * * * *

Computer programs are ideas that are both medium and message. International governance has been effective at regulating the conduits, but has limited success in extending its regulatory net to include the content. Digitization presents a unique challenge to international governance because it inseparably bonds the message and the medium. As a result, states have shown a limited ability to exert a variety of controls over Cyberspace domestically, but they have been unable to address it as a transborder phenomenon that is a ”composite of the space of flows and the space of places.”[915]

The convergence of medium and message creates a challenge for international governance that is premised on material territorial borders. This is not the only reason that the international will be increasingly challenged by

[915] Castells, “Communication, Power and Counter-Power in the Network Society,” 249.

Cyberspace. The message-medium convergence is also implicit in emerging social understandings of the space of consciousness. The networking of the world means that individuals "can change [their] geography, and *anything* that happens there creates a change in someone's *physical* geography."[916]. It is these innovative connections that are currently driving economics, politics, and a range of other social interactions. In much that same way that the dropping of Little Man on Hiroshima and the first orbit of Sputnik did, Cyberspace is changing the shape of the world. The Cold War fear of distant powers raining fire from the sky has been replaced by a post 9/11 fear of the Internet radicalized neighbor. Similarly, the power and awe of strategic nuclear weapons and space exploration that has held so much sway over international politics is being replaced by the power of Cyberspace and the struggle to maintain and manage it in such a way as to enrich humanity. If the Internet and Cyberspace are to be effective tools of liberty, freedom, and justice then Cyberspace must be understood not just within the domestic legal governance, but also within the international governance system which defines the borders that enclose domestic systems. In Schmitt's words: "The new *nomos* of our planet is growing irresistibly. . . .But what is coming is not therefore boundless or a nothingness hostile to *nomos*. Also in timorous rings of old and new forces, right measures and meaningful proportions can originate."[917]

---

[916] Hayden, "The Future of Things Cyber," 4.
[917] Schmitt, *The Nomos of the Earth*, 355.

Bibliography

"A Tale of Many Hackers," *2600: The Hacker Quarterly*, 2015.

"A Thing About Machines," *The Twilight Zone*, season 1, episode 40 (1960).

Aaronson, Xavier, "The DIY Engineer Who Built a Nuclear Reactor in His Basement," Motherboard, August 27, 2014, http://motherboard.vice.com/read/the-diy-engineer-who-built-a-nuclear-reactor-in-his-basement.

"About Pong," www.ponggame.org (last visited February 11, 2016).

Addis, Adeno, "The Thin State in Thick Globalism: Sovereignty in the Information Age," *Vanderbilt Journal of Transnational Law* 37, (2004): 1-107.

Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space (December 3, 1968).

Albanesius, Chloe, "Anonymous Takes Down CIA Web Site," *PC Magazine*, February 10, 2012, http://www.pcmag.com/article2/0,2817,2400140,00.asp.

American Broadcasting Company v. Aereo, 573 U.S. (2014).

AnonHQ, "The Most Frequently Asked Questions People Have About Anonymous," (Jan. 16, 2016), http://anonhq.com/43605-2/.

"Anonymous Activists Target Tunisian Government Sites," *BBC News*, January 4, 2014, http://www.bbc.com/news/technology-12110892.

Akehurst, Michael, "Jurisdiction in International Law," *Brit. YB Int'l L.* 46 (1972): 145.

Allan, Collin S., "Attribution Issues in Cyberspace," *Chi.-Kent J. Int'l & Comp. L.* 13 (2013): 55–201.

Alvestrand, Harald and Hakon Wium Lie, "Development of Core Internet Standards: The Work of IETF and W3C," in *Internet Governance: Infrastructure and Institutions*, ed. Lee A. Bygrave and Jon Bing (Oxford: Oxford University Press, 2009), 126–46.

American Convention on Human Rights (entered into force July 18, 1978).

Antarctic Treaty (December 1, 1959).

Arendt, Hannah, *Eichmann in Jerusalem : A Report on the Banality of Evil* (New York: Penguin, 1963).

Arms Trade Treaty (entered into force Dec. 24, 2014).

Assange, Julian, "Conspiracy as Governance," *IQ. Org*, 2006, http://library.blountsfolly.com/space/items/show/172.

Assange, Julian et al., *Cypherpunks: Freedom and the Future of the Internet* (Or Books, 2012).

Associated Press, "'Anonymous' Hackers Threaten Drug Cartel," *CBS News*, October 31, 2011, http://www.cbsnews.com/news/anonymous-hackers-threaten-drug-cartel/.

Ball, James and Spencer Ackerman, "NSA Loophole Allows Warrantless Search for US Citizens' Emails and Phone Calls," *The Guardian*, August 9, 2013, http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls.

Ball, James, Luke Harding, and Juliette Garside, “BT and Vodafone among Telecoms Companies Passing Details to GCHQ,” *The Guardian*, August 2, 2013, http://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq.

Banks, David, “The Politics of Communications Technology,” Cyborgology, May 5, 2013, http://thesocietypages.org/cyborgology/2013/05/04/the-politics-of-communications-technology/.

Banzi, Massimo, *Getting Started With Arduino*, 2nd ed. (Beijing: O’Reilly 2011).

Barlow, John Perry, “The Declaration of Independance for Cyberspace,” February 8, 1996, https://projects.eff.org/~barlow/Declaration-Final.html.

Battaglia, Debbora, "Arresting Hospitality: the Case of the ‘Handshake in Space'," *Journal of the Royal Anthropological Institute*, v. 18/1 (June 2012) S76-S89.

Bearman, Joshua, “The Untold Story of Silk Road, Part 2: The Fall,” *WIRED*, May 14, 2015, http://www.wired.com/2015/05/silk-road-2/.

Bell, Daniel, “The East Asian Challenge to Human Rights: Reflections on an East West Dialogue,” *Human Rights Quarterly* 18, no. 3 (1996): 641–67.

Bellamy, Alex J., “Whither the Responsibility to Protect? Humanitarian Intervention and the 2005 World Summit,” *Ethics & International Affairs* 20, no. 2 (2006): 143–69.

Bergen, Peter L. and Bruce Hoffman, *Assessing the Terrorist Threat: A Report of the Bipartisan Policy Center's National Security Preparedness Group* (Bipartisan Policy Center, 2010).

Berkman Center, *Don't Panic Making Progress on the "Going Dark" Debate* (Feb. 1, 2016) https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

Berlinski, David, *The Advent of the Algorithm: The 300-Year Journey from an Idea to the Computer* (Houghton Mifflin Harcourt, 2000).

Bernard, Doug, "Iran's Next Step in Building a 'Halal' Internet," *Voice of America*, March 9, 2015, http://www.voanews.com/content/irans-next-step-in-building-a-halal-internet/2672948.html.

Betz, David J., "Clausewitz and Connectivity," *Infinity Journal* 3, no. 1 (March 2013), https://www.infinityjournal.com/article/84/Clausewitz_and_Connectivity/.

Betz, David J. and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power* (London: Routledge, 2011).

Bigo, Didier, "The Emergence of a Consensus: Global Terrorism, Global Insecurity, and Global Security.," in *Immigration, Integration, and Security. America and Europe in Comparative Perspective*, ed. Ariane Chebel d'Appollonia and Simon Reich (University of Pittsburgh Press, 2008), 76–94.

Dittmer, J., "Everyday Diplomacy: UKUSA Intelligence Cooperation and Geopolitical Assemblages," *Annals of the Association of American Geographers* 105, no. 3 (04 2015): 604–19.

Blount, P. J., "Jurisdiction in Outer Space: Challenges of Private Individuals in Space," *J. Space L.* 33 (2007): 299.

Blount, P. J., "The Preoperational Legal Review of Cyber Capabilities: Ensuring the Legality of Cyber Weapons," *Northern Kentucky Law Review* 39, no. 2 (2012): 211–20, http://papers.ssrn.com/abstract=2380359.

Blount, P. J., "Renovating Space: The Future of International Space Law," *Denv. J. Int'l L. & Pol'y* 40 (2012): 515–686.

Borger, Julian, "NSA Files: Why the Guardian in London Destroyed Hard Drives of Leaked Files," *The Guardian*, accessed April 12, 2014, http://www.theguardian.com/world/2013/aug/20/nsa-snowden-files-drives-destroyed-london.

Borgwardt, Elizabeth, *A New Deal for the World: America's Vision for Human Rights* (Cambridge, MA: Belknap, 2005).

Bowcott, Owen, "Julian Assange Loses Appeal against Extradition," *The Guardian*, May 30, 2012, sec. Media, http://www.theguardian.com/media/2012/may/30/julian-assange-loses-appeal-extradition.

Bowman, Gregory W., "Thinking Outside the Border: Homeland Security and the Forward Deployment of the US Border," *Houston Law Review* 44, no. 2 (2007): 189–251.

Branigan, Tania and Miriam Elder, "Edward Snowden Leaves Hong Kong for Moscow," *The Guardian*, June 23, 2013, sec. US news, http://www.theguardian.com/world/2013/jun/23/edward-snowden-leaves-hong-kong-moscow.

Brate, Adam, *Technomanifestos: Visions of the Information Revolutionaries*, 1 edition (New York: Texere, 2002).

Brazil (Embassy International Productions/Brazil Productions 1985).

Brenner, Joel, "Gray Matter," *Foreign Policy*, March 8, 2013, http://www.foreignpolicy.com/articles/2013/03/08/gray_matter.

Broad, William J., John Markoff, and David E. Sanger, "Stuxnet Worm Used Against Iran Was Tested in Israel," *The New York Times*, January 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

Brooking, E.T., "Anonymous vs. the Islamic State," *Foreign Policy*, November 13, 2015, https://foreignpolicy.com/2015/11/13/anonymous-hackers-islamic-state-isis-chan-online-war/.

Brown, Mark, "Pirate Bay Mirror Is Proxy-Friendly, Bypasses UK Ban," *Wired UK*, May 24, 2012, http://www.wired.co.uk/news/archive/2012-05/24/the-proxy-bay.

Brown, Wendy, *Walled States, Waning Sovereignty* (New York; Cambridge, Mass.: Zone Books ; Distributed by the MIT Press, 2010).

Buckminster Fuller Institute, "The Dymaxion Map," https://bfi.org/about-fuller/big-ideas/dymaxion-world/dymaxion-map (last visited Feb. 15, 2016).

Burbank, Jane and Frederick Cooper, *Empires in World History: Power and Politics of Difference* (Princeton: Princeton University Press, 2010).

Bush, Vannevar, *Modern Arms & Free Men* (MIT Press, 1968).

Cadwalladr, Carole, "Meet Cody Wilson, Creator of the 3D-Gun, Anarchist, Libertarian," *The Guardian*, February 10, 2014, sec. Technology, http://www.theguardian.com/technology/2014/feb/10/cody-wilson-3d-gun-anarchist.

Caney, Simon, "Review Article: International Distributive Justice," *Political Studies* 49, no. 5 (2001): 974–97.

Carey, James, "A Cultural Approach to Communication," in *McQuail's Reader in Mass Communication Theory*, ed. Denis McQuail, 2002, 36–45.

Carrington, Damian, "The Maldives Is the Extreme Test Case for Climate Change Action," *The Guardian*, September 26, 2013, sec. Environment, http://www.theguardian.com/environment/damian-carrington-blog/2013/sep/26/maldives-test-case-climate-change-action.

Carroll, Rory, "Barack Obama and Xi Jinping Meet as Cyber-Scandals Swirl," *The Guardian*, June 8, 2013, sec. US news, http://www.theguardian.com/world/2013/jun/08/obama-xi-jinping-meet-cyberscandals.

Cassese, Antonio, International Criminal Law (Oxford: Oxford University Press 2003).

Castells, Manuel, "Communication, Power and Counter-Power in the Network Society," *International Journal of Communication* 1, no. 1 (2007): 29.

Center for Copyright Information, “FAQ’s on The Center for Copyright Information And Copyright Alert System,” July 7, 2011, http://library.blountsfolly.com/space/items/show/183.

Chen, Thomas M., “An Assessment of the Department of Defense Strategy for Operating in Cyberspace” (DTIC Document, 2013), http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA58643.

Chrisafis, Angelique, “France ‘Runs Vast Electronic Spying Operation Using NSA-Style Methods,’” *The Guardian*, July 4, 2013, http://www.theguardian.com/world/2013/jul/04/france-electronic-spying-operation-nsa.

Citizen Four (HBO Films 2014).

Chadwick, Andrew, “Bringing E-Democracy Back In Why It Matters for Future Research on E-Governance,” *Social Science Computer Review* 21, no. 4 (2003): 443–55.

Clapham, Christopher, “Degrees of Statehood,” *Review of International Studies* 24, no. 02 (1998): 143–57.

Clark, Ian, *Legitimacy in International Society* (Oxford University Press, 2005).

Clark, David D. and Susan Landau, “Untangling Attribution,” in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, 2010.

Clinton, Hillary, “Internet Rights and Wrongs: Choices & Challenges in a Networked World,” remarks, *U.S. Department of State*, (February 15,

2011),
http://www.state.gov/secretary/20092013clinton/rm/2011/02/156619.htm.

Codding Jr., George A., "The International Telecommunications Union: 130 Years of Telecommunications Regulation," *Denver Journal International Law & Policy* 23 (1994): 501.

Cohen, Julie E., "Privacy, Visibility, Transparency, and Exposure," *The University of Chicago Law Review*, 2008, 181–201.

Coicaud, Jean-Marc, "Deconstructing International Legitimacy," in *Fault Lines of International Legitimacy*, ed. Hilary Charlesworth and Jean-Marc Coicaud (Cambridge University Press, 2009), 29–86.

Coicaud, Jean-Marc, *Legitimacy and Politics: A Contribution to the Study of Political Right and Political Responsibility*, trans. David Ames Curtis (Cambridge: Cambridge University Press, 2002).

Coicaud, Jean-Marc and Ibrahim Tahri, "Nationally Based Data: Challenges for Global Governance (and Global Policy)," *Global Policy* 5, no. 2 (2014): 135–45.

Constitution of the International Telecommunication Union (2010).

Convention on Civil Aviation (Dec. 7, 1944).

Convention on Cybercrime (entered into force July 1, 2004).

Convention on the Prevention and Punishment of the Crime of Genocide, (Dec. 9,1948).

Cooper, Frederick, "What Is the Concept of Globalization Good For? An African Historian's Perspective," *African Affairs* 100, no. 399 (2001): 189–213.

Council of the European Union, "EU Human Rights Guidelines on Freedom of Expression Online and Offline," May 12, 2014, ec.europa.eu//digital-agenda/en/news/eu-human-rights-guidelines-freedom-expression-online-and-offline.

Covenant of the League of Nations (April 28, 1919).

Cowell, Alan, "After 350 Years, Vatican Says Galileo Was Right: It Moves," *The New York Times*, October 31, 1992, sec. World, http://www.nytimes.com/1992/10/31/world/after-350-years-vatican-says-galileo-was-right-it-moves.html.

Craig, Campbell, "The Resurgent Idea of World Government," *Ethics & International Affairs* 22, no. 2 (2008): 133–42.

Dallmayr, Fred, "Cosmopolitanism: Moral and Political," *Political Theory* 31, no. 3 (2003): 421–42.

Davis, Creighton Powell, "The Internet As a Source of Political Change in Egypt and Saudi Arabia," *Al Noor* 1, no. 1 (2008), http://alnoorjournal.org/wp-content/uploads/2012/05/Al-Noor-2008.pdf#page=33.

Defense Distributed, "Downloads," https://defdist.org/downloads/ (last visted Feb. 17, 2016).

DeNardis, Laura, *The Global War for Internet Governance* (New Haven: Yale University Press, 2014).

DeNardis, Laura and A. M. Hackl, "Internet Governance by Social Media Platforms," *Telecommunications Policy*, 2015.

Department of the Army, "FM 3-38: Cyber Electromagnetic Activities," February 12, 2014, http://library.blountsfolly.com/space/items/show/194.

Diaconescu, Adrian, "Inside Job: Lizard Squad and Ex-Sony Employees Likely Aided North Korea's Hack Attack," *Digital Trends*, December 14, 2014, http://www.digitaltrends.com/computing/lizard-squad-and-ex-sony-employees-likely-involved-in-hack/.

Dickinson, Samantha, "How Will Internet Governance Change after the ITU Conference?," *The Guardian*, November 7, 2014, sec. Technology, http://www.theguardian.com/technology/2014/nov/07/how-will-internet-governance-change-after-the-itu-conference.

Digital Millennium Copyright Act, Pub. L. 105-304 (1998).

Dinstein, Yoram, *The Conduct of Hostilities Under the Law of International Armed Conflict* (Cambridge University Press, 2004).

Dipert, Randall R., "The Essential Features of an Ontology for Cyberwarfare," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton: Taylor & Francis, 2013), 35–48.

Dodge, Martin, "An Atlas of Cyberspace," https://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/topology.html (last visited February 15, 2016).

Dodge, Martin and Rob Kitchin, "Ways to Map Cyberspace," Directions Magazine, November 7, 2001, http://www.directionsmag.com/entry/ways-to-map-cyberspace/124119

Domscheit-Berg, Daniel, *Inside Wikileaks : My Time with Julian Assange at the World's Most Dangerous Website* (New York: Crown Publishers, 2011).

Donnelly, Jack, "Human Rights: A New Standard of Civilization?," *International Affairs* 74, no. 1 (1998): 1–23.

Dorling, Philip, "Snowden Reveals Australia's Links to US Spy Web," *The Sydney Morning Herald*, July 8, 2013, http://www.smh.com.au/world/snowden-reveals-australias-links-to-us-spy-web-20130708-2plyg.html.

Draft Articles on the Responsibility of States for Internationally Wrongful Acts, 53 UN GAOR Supp. (No. 10) at 43, U.N. Doc. A/56/10 (2001).

Du Bois, W. E. B., *The Souls of Black Folk* (New York: Pocket Books, 2005).

Dunlap Jr., Charles J. , "Perspectives for Cyberstrategists on Cyberlaw for Cyberwar," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton: Taylor & Francis, 2013), 211–32.

Dunn, Alexandra, "Unplugging a Nation: State Media Strategy During Egypt's January 25 Uprising," *Fletcher F. World Aff.* 35 (2011): 15.

e-Estonia, "What is e-Residency?", https://e-estonia.com/e-residents/about/ (last accessed October 6, 2015).

Elwell, Craig K., M. M. Murphy, and Michael V. Seitzinger, "Bitcoin: Questions, Answers, and Analysis of Legal Issues," Report (United States: Library of Congress. Congressional Research Service., December 20, 2013), United States.

Eppenstein, Madelaine and Elizabeth J. Aisenberg, "Radio Propaganda in the Contexts of International Regulation and the Free Flow of Information as a Human Right [notes]," *Brooklyn Journal of International Law* 5 (1979): 154.

European Convention on Human Rights (entered into for June 1, 2010)

EUTELSAT, "Eutelsat condemns jamming of broadcasts from Iran and renews appeals for decisive action to international regulators," PR/62/12, Oct. 4, 2012, http://www.eutelsat.com/home/news/press-releases/Archives/2012/press-list-container/eutelsat-condemns-jamming-of-bro.html

"Everything We Know about the San Bernardino Terror Attack Investigation so Far," *Los Angeles Times*, December 14, 2015, http://www.latimes.com/local/california/la-me-san-bernardino-shooting-terror-investigation-htmlstory.html.

Executive Order 12333: United States Intelligence Activities (2001).

FBI Press Office, "Update on the Sony Investigation," Dec. 19, 2014, http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

Featherstone, Mike, "Genealogies of the Global," *Theory, Culture & Society* 23, no. 2/3 (March 2006): 387–92.

Featherstone, Mike and Couze Venn, "Problematizing Global Knowledge and the New Encyclopaedia Project: An Introduction," *Theory, Culture & Society* 23, no. 2–3 (2006): 1–20.

Fenlon, Wesley, "Did Google Maps Cause an International Border Dispute?," *HowStuffWorks*, October 3, 2011, http://computer.howstuffworks.com/google-maps-international-border-dispute.htm.

Ferguson, James, *Global Shadows: Africa in the Neoliberal Global Order* (Durham: Duke University Press, 2006).

Ferguson, Yale H. and Richard W Mansbach, *Globalization: The Return of Borders to a Borderless World?* (New York: Routledge, 2012).

Feuer, Alan, "Cody Wilson, Who Posted Gun Instructions Online, Sues State Department," *The New York Times*, May 6, 2015, http://www.nytimes.com/2015/05/07/us/cody-wilson-who-posted-gun-instructions-online-sues-state-department.html.

Fidler, David P., "The Internet, Human Rights, and U.S. Foreign Policy: The Global Online Freedom Act of 2012," *ASIL Insights* 16, no. 18 (May 24, 2012), http://www.asil.org/insights/volume/16/issue/18/internet-human-rights-and-us-foreign-policy-global-online-freedom-act.

Fielder, James D., "The Internet and Dissent in Authoritarian States," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton: Taylor & Francis, 2013), 161–91.

Findlay, Trevor, "Why Treaties Work, Don't Work and What to Do About It?" (Canadian Institute of International Affairs, January 25, 2006), http://carleton.ca/npsia/wp-content/uploads/ciia_present_06.pdf.

"Finland Makes Broadband a 'Legal Right,'" *BBC News*, accessed December 2, 2015, http://www.bbc.com/news/10461048.

Finnemore, Martha and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization* 52, no. 04 (1998): 887–917.

Fish, Isaac, "Could North Koreans Ever Really Invade America?," *Foreign Policy*, November 21, 2012, https://foreignpolicy.com/2012/11/21/could-north-koreans-ever-really-invade-america/.

Fleischmann, Kenneth R. et al., "Thematic Analysis of Words That Invoke Values in the Net Neutrality Debate," March 15, 2015, https://www.ideals.illinois.edu/handle/2142/73433.

Foreign Intelligence Surveillance Act of 1978, 95 Pub.L. 511 (1978).

Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, 110 Pub. L. 261 (2008).

Friedman, Benjamin H. and Christopher A. Preble, "A Military Response to Cyberattacks Is Preposterous," *Cato Institute*, June 2, 2011, http://www.cato.org/publications/commentary/military-response-cyber attacks-is-preposterous.

Fritsch, Stefan, "Technology and Global Affairs," *International Studies Perspectives* 12, no. 1 (2011): 27–45.

Gallagher, Sean, "NSA's Director Says Paris Attacks 'would Not Have Happened' without Crypto," *Ars Technica*, February 18, 2016,

http://arstechnica.com/tech-policy/2016/02/nsas-director-says-paris-attacks-would-not-have-happened-without-crypto/.

Gallagher, Sean, "Silk Road, Other Tor 'darknet' Sites May Have Been 'decloaked' through DDoS [Updated]," *Ars Technica*, November 9, 2014, http://arstechnica.com/security/2014/11/silk-road-other-tor-darknet-sites-may-have-been-decloaked-through-ddos/.

Gallington, Daniel, "Perspectives on Collection, Retention, and Dissemination of Intelligence," Marshall Policy Outlook (United States: George C. Marshall Institute, May 2014), http://marshall.org/wp-content/uploads/2014/05/Collection-PO-May-14.pdf.

Gelernter, David, "The End of the Web, Search, and Computer as We Know It," *Wired Opinion*, February 1, 2013, http://www.wired.com/opinion/2013/02/the-end-of-the-web-computers-and-search-as-we-know-it/.

Gellman, Robert, "Civil Liberties and Privacy Implications of Policies to Prevent Cyberattacks," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, by Committee on Deterring Cyberattacks: Informing Strategies and Developing Options; National Research Council (Washington, D.C.: National Academies Press, 2010), 273–309, http://www.nap.edu/openbook.php?record_id=12997&page=273.

Gellman, Barton, "NSA Broke Privacy Rules Thousands of Times per Year, Audit Finds," *The Washington Post*, August 15, 2013,

http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html.

Gellman, Barton and Laura Poitras, "U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program," *The Washington Post*, June 7, 2013, http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

"German Intelligence Agencies Used NSA Spying Program," *Spiegel Online*, July 20, 2013, http://www.spiegel.de/international/germany/german-intelligence-agencies-used-nsa-spying-program-a-912173.html.

Geyer, Michael and Charles Bright, "World History in a Global Age," *The American Historical Review* 100, no. 4 (1995): 1034–60.

Goldsmith, Jack L., "Against Cyberanarchy," *The University of Chicago Law Review* 65, no. 4 (1998): 1199–1250.

Goldsmith, Jack L., "The Sony Hack: Attribution Problems, and the Connection to Domestic Surveillance," *Lawfare*, December 19, 2014, https://www.lawfareblog.com/sony-hack-attribution-problems-and-connection-domestic-surveillance.

Gompert, David C. and Phillip C. Saunders, *Paradox of Power: Sino-American Strategic Restraint in an Age of Vulnerability* (Washington, DC: National Defense University Press, 2012).

Goodhart, Michael, "Human Rights and Global Democracy," *Ethics & International Affairs* 22, no. 4 (2008): 395–420.

Goodman, Ellen P., "Media Policy and Free Speech: The First Amendment at War with Itself," *Hofstra Law Review* 35 (2007).

Goodman, Ellen P. and Anne H. Chen, "Modeling Policy for New Public Service Media Networks," *Harv. JL & Tech.* 24 (2010): 111.

Gorman, Siobahn and Siobhan Gorman And Julian E. Barnes, "Cyber Combat: Act of War," *Wall Street Journal*, May 31, 2011, sec. Tech, http://www.wsj.com/articles/SB10001424052702304563104576355623135782718.

Gourley, Stephen K., "Cyber Sovereignty," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton: Taylor & Francis, 2013), 277–89.

Greenberg, Andy, "I Made an Untraceable AR-15 'Ghost Gun' in My Office—And It Was Easy," *WIRED*, June 3, 2015, http://www.wired.com/2015/06/i-made-an-untraceable-ar-15-ghost-gun/.

Greenberg, Andy, *This Machine Kills Secrets : How WikiLeakers, Cypherpunks and Hacktivists Aim to Free the World's Information* (New York: Dutton, 2012).

Greenet Ltd. et al v. GCHQ - Statement of Grounds (Investigatory Powers Tribunal (UK) 2014).

Greenwald, Glenn, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (New York: Metropolitan Books 2014)

Greenwald, Glenn, "NSA Collecting Phone Records of Millions of Verizon Customers Daily," *The Guardian*, accessed May 6, 2014, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

Greenwald, Glenn, "XKEYSCORE: NSA Tool Collects 'Nearly Everything a User Does on the Internet,'" *The Guardian*, July 31, 2013, http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

Greenwald, Glenn and Spencer Ackerman, "How the NSA Is Still Harvesting Your Online Data," *The Guardian*, June 27, 2013, http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection.

Greenwald, Glenn and Spencer Ackerman, "NSA Collected Americans' Email Records in Bulk for Two Years under Obama," *The Guardian*, June 27, 2013, http://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama.

Greenwald, Glenn and James Ball, "The Top Secret Rules That Allow NSA to Use US Data without a Warrant," *The Guardian*, accessed May 6, 2014, http://www.theguardian.com/world/2013/jun/20/fisa-court-nsa-without-warrant

Greenwald, Glenn and Ryan Gallagher, “Snowden Documents Reveal Covert Surveillance and Pressure Tactics Aimed at WikiLeaks and Its Supporters,” *The Intercept*, February 18, 2014, https://theintercept.com/2014/02/18/snowden-docs-reveal-covert-surveillance-and-pressure-tactics-aimed-at-wikileaks-and-its-supporters/.

Greenwald, Glenn and Ewen MacAskill, “Boundless Informant: The NSA’s Secret Tool to Track Global Surveillance Data,” *The Guardian*, accessed May 6, 2014, http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining.

Greenwald, Glenn and Ewen MacAskill, “NSA PRISM Program Taps in to User Data of Apple, Google and Others,” *The Guardian*, June 7, 2013, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

Greenwald, Glenn, Ewen MacAskill, and Laura Poitras, “Edward Snowden: The Whistleblower behind the NSA Surveillance Revelations,” *The Guardian*, June 11, 2013, sec. US news, http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

Greenwald, Glenn, Ewen MacAskill, Laura Poitras, Spencer Ackerman, and Dominic Rushe. “Microsoft Handed the NSA Access to Encrypted Messages.” The Guardian. July 12, 2013. http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data.

Habermas, Jürgen, *The Postnational Constellation: Political Essays*, ed. and trans. Max Pensky (MIT Press, 2001).

Hague Code of Conduct Against Ballistic Missile Proliferation (November 25, 2002).

Halvorssen, Thor and Alexander Lloyd, "We Hacked North Korea With Balloons and USB Drives," *The Atlantic*, January 15, 2014, http://www.theatlantic.com/international/archive/2014/01/we-hacked-north-korea-with-balloons-and-usb-drives/283106/.

Hamill, Jasper, "Pirate Bay Is BACK - Torrent Site to Return in One Week," *The Mirror*, January 26, 2015, http://www.mirror.co.uk/news/technology-science/technology/pirate-bay-back---torrent-5045073.

Harrison, Roger, *Space and Verification, Volume I: Policy Implications* (Eisenhower Center for Space and Defence Studies 2007) .

Harvey, David, *A Brief History of Neoliberalism* (Oxford: Oxford Univ. Press, 2009).

Hayden, Michael V., "The Future of Things Cyber," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton: Taylor & Francis, 2013), 3–8.

Heddaya, Mostafa, "See A Map, Not a Territory: Apple and the End of Skeuomorphism," Hyperallergenic, June 27, 2013, http://hyperallergic.com/74308/a-map-not-a-territory-apple-and-the-end-of-skeuomorphism/.

Held, David, *Democracy and the Global Order: From the Modern State to Cosmopolitan Governance* (Stanford: Stanford University Press 1995).

Hille, Kathrin, "China Cracks Down on Online Maps," *Financial Times*, May 21, 2010, http://www.ft.com/cms/s/0/9569b59e-64f3-11df-aa4d-00144feab49a.html#axzz40FUFCz8W.

Hooper, Charlotte, *Manly States: Masculinities, International Relations, and Gender Politics* (New York: Columbia University Press 2001).

Hopkins, Nick and Julian Borger, "Exclusive: NSA Pays £100m in Secret Funding for GCHQ," *The Guardian*, August 1, 2013, http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden.

Hopkins, Nick, Julian Borger, and Luke Harding, "GCHQ: Inside the Top Secret World of Britain's Biggest Spy Agency," *The Guardian*, August 1, 2013, http://www.theguardian.com/world/2013/aug/02/gchq-spy-agency-nsa-snowden

Hurwitz, Roger, "A New Normal? The Cultivation of Global Norms as Part of a Cybersecurity Strategy," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton: Taylor & Francis, 2013), 233–64.

The Imitation Game (Black Bear Pictures/Bristol Automotive 2014).

"India Google Maps Controversy Is Modern Drama," Democracy Chronicles, July 29, 2014,

https://democracychronicles.com/india-google-maps-controversy-modern-drama/.

International Covenant on Civil and Political Rights (entered into force Mar. 23, 1976).

International Covenant on Economic, Social and Cultural Rights (Dec. 16, 1966).

International Docking System Standard, Interface Definition Document, Revision D (April 30, 2015) http://www.internationaldockingstandard.com/download/IDSS_IDD_Revision_D_043015.pdf.

International Table Tennis Federation, "The Laws of Table Tennis," http://www.ittf.com/ittf_handbook/2016/2016_EN_HBK_CHPT_2.pdf (last visited February 11, 2016).

International Telecommunication Union, *ICT Facts and Figures 2015* (2015)

International Telecommunication Union, "Resolution 2 (Rev. Busan, 2014) World Telecommunication/Information and Communication Technology Policy Forum," 2014.

International Telecommunication Union, "Resolution 101 (Rev. Busan, 2014) Internet Protocol-Based Networks," 2014.

International Telecommunication Union, "Resolution 102 (Rev. Busan, 2014) ITU's Role with Regard to International Public Policy Issues Pertaining to the Internet and the Management of Internet Resources, Including Domain Names and Addresses," 2014.

International Telecommunication Union, “Resolution 133 (Rev. Busan, 2014) Role of Administrations of Member States in the Management of Internationalized (Multilingual Domain Names,” 2014.

International Telecommunications Union, “Resolution 140 (Rev. Buan, 2014) ITU’s Role in Implementing the Outcomes of the World Summit on the Information Society and in the Overall Review by United Nations General Assembly of Their Implementation,” 2014.

International Telecommunication Union, “Resolution 180 (Rev. Busan, 2014) Facilitating the Transition from IPv4 to IPv6,” 2014.

International Traffic in Arms Regulations, 22 C.F.R. 120-130 (2015)

Internet Engineering Task Force, “The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force” (2012) at https://www.ietf.org/tao.html.

Jayakar, Krishna, “Globalization and the Legitimacy of International Telecommunications Standard-Setting Organizations,” *Indiana Journal of Global Legal Studies* 5 (1998): 711–38.

Johnson, David R. and David Post, “Law and Borders: The Rise of Law in Cyberspace,” *Stanford Law Review* 48, no. 5 (1996): 1367–1402.

Jentleson, Bruce W., “The Obama Administration and R2P: Progress, Problems and Prospects,” *Global Responsibility to Protect* 4, no. 4 (2012): 399–423.

Jurgenson, Nathan, “Digital Dualism versus Augmented Reality,” *Cyborgology*, February 24, 2011,

http://thesocietypages.org/cyborgology/2011/02/24/digital-dualism-versus-augmented-reality/.

Kallberg, Jan and Rosemary A. Burk, "Cyberdefense as Environmental Protection - The Broader Potential Impact of Failed Defensive Counter Cyber Operations," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton: Taylor & Francis, 2013), 265–75.

"Kanye West Targeted by 'Anonymous' in Searing Video," *Billboard*, March 12, 2015, http://www.billboard.com/articles/columns/the-juice/6501935/anonymous-kanye-west-video.

Kelley, Michael B., "Edward Snowden's Relationship With WikiLeaks Should Concern Everyone," *Business Insider*, January 4, 2014, http://www.businessinsider.com/edward-snowden-and-wikileaks-2014-1.

Kellner, Douglas, "Intellectuals, the New Public Sphere, and Technopolitics," in *The Politics of Cyberspace*, ed. Chris Toulouse and Timothy W. Luke (New York: Routledge, 1998), 147–86.

Kende, Michael, "The Digital Handshake: Connecting Internet Backbones" (Washington, D.C.: Federal Communications Commission, 2000).

Kennedy, Charles H. and M. Veronica Pastor, *An Introduction to International Telecommunications Law* (Boston: Artech House, 1996).

Kirby, Debra, "Minding the Gap: The Growing Divide between Privacy and Surveillance Technology" (Thesis, Naval Postgraduate School, 2013),

http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA585523.

kliq, "Xfinite Absurdity: True Confessions of a Former Comcast Tech Support Agent," *2600: The Hacker Quarterly*, 2014.

Knight, Will, "Controlling Encryption Will Not Stop Terrorists," *New Scientist*, accessed February 19, 2016, https://www.newscientist.com/article/dn1309-controlling-encryption-will-not-stop-terrorists/.

Korea (Democratic People's Republic of)'s Constitution of 1972 with Amendments through 1998, https://www.constituteproject.org/constitution/Peoples_Republic_of_Korea_1998.pdf.

Kracht, James, "The Hacker Perspective," *2600: The Hacker Quarterly*, 2014.

Krattenmaker, Thomas G., *Telecommunications Law and Policy*, 2nd ed. (Durham, NC: Carolina Academic Press, 1998).

Kravets, David, "ISPs to Disrupt Internet Access of Copyright Scofflaws," *Wired*, July 7, 2011, http://www.wired.com/2011/07/disrupting-internet-access/.

Kulesza, Joanna, *International Internet Law*, trans. Magdalena Arent and Wojciech Wotoszyk (Routledge, 2013).

Lally, Kathy and Juan Forero, "Bolivian President's Plane Forced to Land in Austria in Hunt for Snowden," *The Washington Post*, July 3, 2013, https://www.washingtonpost.com/world/bolivian-presidents-plane-forc

ed-to-land-in-austria-in-hunt-for-snowden/2013/07/03/c281c2f4-e3eb-11e2-a11e-c2ea876a8f30_story.html.

Lam, Lana, "EXCLUSIVE: US Hacked Pacnet, Asia Pacific Fibre-Optic Network Operator, in 2009," *South China Morning Post*, June 22, 2013, http://www.scmp.com/news/hong-kong/article/1266875/exclusive-us-hacked-pacnet-asia-pacific-fibre-optic-network-operator.

Lam, Lana and Stephen Chen, "EXCLUSIVE: US Spies on Chinese Mobile Phone Companies, Steals SMS Data: Edward Snowden," *South China Morning Post*, June 22, 2013, http://www.scmp.com/news/china/article/1266821/us-hacks-chinese-mobile-phone-companies-steals-sms-data-edward-snowden?page=all.

Lee, Robert M., "The Feds Got the Sony Hack Right, But the Way They're Framing It Is Dangerous," *Wired*, January 10, 2015, http://www.wired.com/2015/01/feds-got-sony-hack-right-way-theyre-framing-dangerous

Lee, Robert M. and Thomas Rid, "OMG Cyber! Thirteen Reasons Why Hype Makes for Bad Policy," *The RUSI Journal* 159, no. 5 (2014): 4–12.

Leiner, Barry M. et al., "A Brief History of the Internet" (The Internet Society, October 15, 2012), http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet.

Lessig, Lawrence, *Code 2.0* (Basic Books, 2006).

Lessig, Lawrence, *Free Culture : The Nature and Future of Creativity* (New York: New York : Penguin Books., 2004).

Lewis, Bernard, *The Crisis of Islam: Holy War and Unholy Terror* (Random House LLC, 2004).

Libicki, Martin C., "Two Maybe Three Cheers for Ambiguity," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton: Taylor & Francis, 2013), 27–34.

Lipschutz, Ronnie D., "Environmental History, Political Economy and Change: Frameworks and Tools for Research and Analysis," *Global Environmental Politics* 1, no. 3 (2001): 72–91.

Liu, Edward C. et al., "Cybersecurity: Selected Legal Issues," Report (Congressional Research Service, Library of Congress, April 20, 2012).

Lloyd, Seth, *Programming the Universe: A Quantum Computer Scientist Takes on the Cosmos*, 2006.

Lucas Jr., George R. , "Can There Be an Ethical Cyber War?," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton: Taylor & Francis, 2013), 195–209.

Luhn, Alec, "Edward Snowden Leaves Moscow Airport after Russia Grants Asylum," *The Guardian*, August 1, 2013, sec. US news, http://www.theguardian.com/world/2013/aug/01/edward-snowden-grant-temporary-asylum-russia.

Luke, Timothy W., "The Politics of Digital Inequality: Access, Capability and Distribution in Cyberspace," in *The Politics of Cyberspace*, ed. Chris Toulouse and Timothy W. Luke (New York: Routledge, 1998), 120–43.

Lyall, Francis and Paul B. Larsen, Space Law: A Treatise (Ashgate 2009).

MacAskill, Ewen, "NSA Paid Millions to Cover Prism Compliance Costs for Tech Companies," *The Guardian*, August 23, 2013, sec. US news, http://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid.

MacAskill, Ewen and Julian Borger, "New NSA Leaks Show How US Is Bugging Its European Allies," *The Guardian*, June 30, 2013, http://www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies.

MacAskill, Ewen, Nick Davies, Nick Hopkins, Julian Borger, and James Ball. "GCHQ Intercepted Foreign Politicians' Communications at G20 Summits." The Guardian. June 17, 2013. http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits.

Macklem, Patrick, "Humanitarian Intervention and the Distribution of Sovereignty in International Law," *Ethics & International Affairs* 22, no. 4 (2008): 369–93.

Mackey, Robert, "'Operation Payback' Attacks Target MasterCard and PayPal Sites to Avenge WikiLeaks," *The Lede*, 1291819254, http://thelede.blogs.nytimes.com/2010/12/08/operation-payback-targets-mastercard-and-paypal-sites-to-avenge-wikileaks/.

Major, Jason, "This Is the Very First Photo of Earth From Space," *Universe Today*, October 24, 2014,

http://www.universetoday.com/115641/this-is-the-very-first-photo-of-earth-from-space/.

Manela, Erez, *The Wilsonian Moment: Self-Determination and the International Origins of Anticolonial Nationalism* (Oxford: Oxford University Press 2007) 59-60.

Martin, C. Dianne, "Using the US Constitution to Frame the Governance of Cyberspace," *ACM Inroads* 6, no. 1 (2015): 24–26.

Mattelart, Armand, *Networking the World, 1794-2000* (University of Minnesota Press, 2000).

Mattice, Lynn, "Taming the '21st Century's Wild West' of Cyberspace?," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton: Taylor & Francis, 2013), 9–12.

Maurashat, Alana, "Zombie Botnets," *SCRIPTed* 7, no. 2 (2010): 370–83, http://www2.law.ed.ac.uk/ahrc/script-ed/vol7-2/maurushat.asp.

McDermott, Rose, "Decision Making Under Uncertainty," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, by Committee on Deterring Cyberattacks: Informing Strategies and Developing Options; National Research Council (Washington, D.C.: National Academies Press, 2010), 227–41, http://www.nap.edu/openbook.php?record_id=12997&page=273.

McIntosh, Wayne and Cynthia Cates, "Hard Travelin': Free Speech in the Age of the Information Super Highway," in *The Politics of Cyberspace*, ed.

Chris Toulouse and Timothy W. Luke (New York: Routledge, 1998), 84–118.

McTaggart, Craig, "A Layered Approach to Internet Legal Analysis," *McGill LJ* 48 (2003): 571.

Menon, Rajan, "Pious Words, Puny Deeds: The 'International Community' and Mass Atrocities," *Ethics & International Affairs* 23, no. 3 (September 1, 2009): 235–46.

Merges, Robert P., Peter S. Menell, and Mark A. Lemley, *Intellectual Property in the New Technological Age, Sixth Edition*, 6 edition (New York: Aspen Publishers, 2012).

Michel, Arthur Holland, "A History of Violence: How Rogue Techies Armed the Predator, Almost Stopped 9/11, and Accidentally Invented Remote War," *WIRED*, January 2016, http://www.wired.com/2015/12/how-rogue-techies-armed-the-predator-almost-stopped-911-and-accidentally-invented-remote-war/.

Microsoft, "HoloLens," https://www.microsoft.com/microsoft-hololens/en-us (last accessed October 6, 2015).

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986, p. 14.

Mlot, Stephanie, "The Pirate Bay Is Back Online (Sort Of)," *PCMAG*, December 15, 2014, http://www.pcmag.com/article2/0,2817,2473661,00.asp.

Moore, Daniel and Thomas Rid, "Cryptopolitik and the Darknet," *Survival*, 58:1 (2016) 7-38.

"Moore's Law," http://www.mooreslaw.org (last visited Feb. 18, 2016).

Morgan, Forrest E., "Deterrence and First-Strike Stability in Space: A Preliminary Assessment" (DTIC Document, 2010).

Morozov, Evgeny, "Political Repression 2.0," *The New York Times*, September 1, 2011, sec. Opinion, http://www.nytimes.com/2011/09/02/opinion/political-repression-2-0.html.

National Aeronautics and Space Administration, "Blue Marble - Image of the Earth from Apollo 17," NASA, (July 31, 2015), http://www.nasa.gov/content/blue-marble-image-of-the-earth-from-apollo-17.

National Center for Justice and the Rule of Law, *Combating Cyber Crime: Essential Tools and Effective Organizational Structures* (Univ. of Mississippi 2007).

National Security Agency, "BOUNDLESSINFORMANT - Frequently Asked Questions," September 6, 2012.

National Security Agency, "(TS//SI/NF) FAA Certification Renewals With Caveats," October 12, 2011.

National Security Agency, "(U//FOUO) NSAW SID Intelligence Oversight (IO) Quarterly Report - First Quarter Calendar Year 2012 (1 January - 31 March 2012 - EXECUTIVE SUMMARY," May 3, 2012.

National Security Agency, "PRISM/US-984XN Overview of the SIGAD Used Most in NSA Reporting Overview," 2013.

National Security Agency Office of Inspector General, "Working Draft Report from March 24, 2009 on Stellar Wind (PSP)," March 24, 2009.

National Telecommunications & Information Administration, "NTIA Announces Intent to Transition Key Internet Domain Name Functions," March 14, 2014, http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions.

NetMudial, *NETmundial Multistakeholder Statement* (April 24, 2014) http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf.

Nincic, Miroslav and Jennifer Ramos, "Torture in the Public Mind," *International Studies Perspectives* 12, no. 3 (2011): 231–49, http://onlinelibrary.wiley.com/doi/10.1111/j.1528-3585.2011.00429.x/abstract.

Noveck, Beth Simone, "Designing Deliberative Democracy in Cyberspace: The Role of the Cyber-Lawyer," *BUJ Sci. & Tech. L.* 9 (2003): 1.

"NSA Hacked UN Videocalls as Part of Surveillance Program, Claims Report," *Al Jazeera America*, August 25, 2013, http://america.aljazeera.com/articles/2013/8/25/nsa-bugged-u-n-headquarters.html.

O'Meara, Richard M., "Jus Post Bellum: War Closure in the 21st Century," in *Routledge Handbook of Ethics and War: Just War Theory in the 21st Century*, ed. Fritz Allhoff, Nicholas G. Evans, and Adam Henschke (Routledge, 2013), 105–19.

O'Neil, Patrick Howell, "Edward Snowden and Spread of Encryption Blamed after Paris Terror Attacks," *The Daily Dot*, December 9, 2015, http://www.dailydot.com/politics/paris-attack-encryption-snowden/.

Oliver, Eric P., "Stuxnet: A Case Study in Cyber Warfare," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton: Taylor & Francis, 2013), 127–59.

*Olmstead v. United State*s, 277 U.S. 438, 466 (1928).

Organization for Security and Co-operation in Europe, "Freedom of Expression on the Internet: A Study of Legal Provisions and Practices Related to Freedom of Expression, the Free Flow of Information and Media Pluralism on the Internet in OSCE Participating States," 2011.

Orwell, George, *1984* (London: Secker & Warburg 1949).

Osgood, Rick, "Net Neutrality and the FCC Hack," in *Hackaday Omnibus 2014*, ed. Mike Szczys, 2014.

"Paris Attacks: What Happened on the Night," *BBC News*, December 9, 2015, http://www.bbc.com/news/world-europe-34818994.

Partridge, Mark V.B. and Scott T. Lonardo, "ICANN Can or Can It?: Recent Developments in Internet Governance Involving Cybersquatting, Online Infringement, and Registration Practices," *Landslide* 1, no. 5 (2009): 24–29.

Poitras, Laura, Marcel Rosenbach, Fidelius Schmid, and Holger Stark. "NSA Spied on European Union Offices." Spiegel Online. June 29, 2013.

http://www.spiegel.de/international/europe/nsa-spied-on-european-union-offices-a-908590.html.

Poitras, Laura, Marcel Rosenbach, and Holger Stark, "NSA Spies on 500 Million German Data Connections," *Spiegel Online*, June 30, 2013, http://www.spiegel.de/international/germany/nsa-spies-on-500-million-german-data-connections-a-908648.html.

Pompe, Cornelis Arnold, *Aggressive War - An International Crime* (Martinus Nijhoff, 1953).

Post, David G., "Against 'Against Cyberanarchy,'" *Berkeley Technology Law Journal* 17 (2002): 1365.

Post, David G., *In Search of Jefferson's Moose: Notes on the State of Cyberspace* (Oxford; New York: Oxford University Press, 2012).

Post, David, "It's 'the Internet.' Please.," *The Volokh Conspiracy*, August 11, 2011, http://volokh.com/2011/08/11/its-the-internet-please/.

Popkin, Helen A. S., "Anonymous 'Brandjacks' Westboro Baptist Church on Facebook," *NBC News*, April 17, 2013, http://www.nbcnews.com/technology/anonymous-brandjacks-westboro-baptist-church-facebook-1C9395459.

Power, Andrew and Oisín Tobin, "Soft Law for the Internet, Lessons from International Law," *SCRIPTed* 8, no. 1 (2011): 31–45, http://www2.law.ed.ac.uk/ahrc/script-ed/vol8-1/power.pdf.

Princeton Project on National Security, "Report of the Working Group on State Security and Transnational Threats" (Princeton, NJ, 2008), https://www.princeton.edu/~ppns/conferences/reports/fall/SSTT.pdf.

Prisoner #6, "The 21st Century Hacker Manifesto," *2600: The Hacker Quarterly*, 2014-2015.

Privacy and Civil Liberties Oversight Board, "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," July 2, 2014, http://library.blountsfolly.com/space/items/show/185.

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) (June 8, 1977)

Quammen, David, *The Boilerplate Rhino: Nature in the Eye of the Beholder* (New York: Scribner, 2000), https://books.google.com/books?hl=en&lr=&id=DI_8RkJyMHMC&oi=fnd&pg=PA9&dq=quammen+the+boilerplate+rhino&ots=owTBLJ_L-t&sig=quUPL-7EvjKq2DWE1dOqWCRyr7M.

Radio Regulations (2012) http://www.itu.int/dms_pub/itu-s/oth/02/02/S02020000244501PDFE.PDF.

Ramey, Christopher H., "When AT&T Asked Us to 'Reach out and Touch Someone', Did They Mean That Literally?," *Psychology Today*, July 7, 2008, http://www.psychologytoday.com/blog/the-metaphorical-mind/200807/when-att-asked-us-reach-out-and-touch-someone-did-they-mean.

Ranieri, Vera, "EFFecting Digital Freedom," *2600: The Hacker Quarterly*, v. 31/3 (2014).

Ranieri, Vera, "EFFecting Digital Freedom," *2600: The Hacker Quarterly*, v. 31/4, (2014-2015).

Rao, J. Mohan, "Equity in A Global Public Goods Framework," in *Global Public Goods: International Cooperation in the 21st Century*, ed. Inge Kaul, Isabelle Grunberg, and Marc Stern (New York, Oxford: Oxford University Press, 1999), 68–87.

Rawls, John, *A Theory of Justice* (Cambridge, Mass.: Belknap Press, 1971).

Raymond, Eric S., *The New Hacker's Dictionary*, 3d ed. (Cambridge, MA: MIT Press 1996).

Reed, David P., "Critiquing the Layered Regulatory Model," *J. on Telecomm. & High Tech. L.* 4 (2005): 281.

Reisman, W. Michael, "International Incidents: Introduction to a New Genre in the Study of International Law," *Yale J. Int'l L.* 10 (1984): 1.

Resnick, David, "Politics on the Internet: The Normalization of Cyberspace," in *The Politics of Cyberspace*, ed. Chris Toulouse and Timothy W. Luke (New York: Routledge, 1998), 48–68.

Richardson, Valerie, "Sony kills 'The Interview' after North Korea hack, terror threat," The Washington Times, Dec. 17, 2014, http://www.washingtontimes.com/news/2014/dec/17/sony-kills-the-interview-after-north-korea-hack-te/?page=all

Richtel, Matt, "Egypt Cuts Off Most Internet and Cellphone Service," *The New York Times*, January 28, 2011, http://www.nytimes.com/2011/01/29/technology/internet/29cutoff.html.

Riley v. California, No. 13-132 (Supreme Court 2014).

Risen, James and Nick Wingfield, "Web's Reach Binds N.S.A. and Silicon Valley Leaders," *The New York Times*, June 19, 2013, sec. Technology, http://www.nytimes.com/2013/06/20/technology/silicon-valley-and-spy-agency-bound-by-strengthening-web.html.

Roberts, Dan, "Bolivian President's Jet Rerouted amid Suspicions Edward Snowden on Board," *The Guardian*, July 3, 2013, sec. World news, http://www.theguardian.com/world/2013/jul/03/edward-snowden-bolivia-plane-vienna.

Robertson, Horace B., "The Suppression of Pirate Radio Broadcasting: A Test Case of the International System for Control of Activities Outside National Territory," *Law and Contemporary Problems*, 1982, 71–101.

Robinson, George S., "Addressing the Legal Status of Evolving 'Envoys of Mankind,'" *Annals of Air and Space Law* 36 (2011): 447–512.

Robinson, George, "Astronauts and a Unique Jurisprudence: A Treaty for Spacekind," 7 *Hastings Int'l & Comp. L. Rev.* 483 (1983-1984).

Roht-Arriaza, Naomi, "The Pinochet Precedent and Universal Jurisdiction," *New England Law Jour*nal 35, no. 2 (2001): 311–19.

Rosen, Jeffrey, "The Right to Be Forgotten," *Stanford Law Review Online* 64 (February 13, 2012): 88, http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten.

Rosenzweig, Paul et al., "Protecting Internet Freedom and American Interests: Required Reforms and Standards for ICANN Transition," Heritage

Foundation Backgrounder (Washington, D.C.: The Heritage Foundation, June 16, 2014), http://www.heritage.org/research/reports/2014/06/protecting-internet-freedom-and-american-interests-required-reforms-and-standards-for-icann-transition.

Rowe , Neil C. et al., "Challenges in Monitoring Cyberarms Compliance," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton: Taylor & Francis, 2013), 81–99.

Rushdie, Salman, *Midnight's Children* (New York: Random House 2006).

Rushe, Dominic, "Skype's Secret Project Chess Reportedly Helped NSA Access Customers' Data," *The Guardian*, June 20, 2013, http://www.theguardian.com/technology/2013/jun/20/skype-nsa-access-user-data.

Rychlak, Ronald J., "Compassion, Hatred, and Free Expression," *Miss. CL Rev.* 27 (2007): 407.

Sadiq, Kamal, *Paper Citizens: How Illegal Immigrants Acquire Citizenship in Developing Countries* (Oxford: Oxford University Press 2010)

Sanger, David E. and Elisabeth Bumiller, "Pentagon to Consider Cyberattacks Acts of War," *The New York Times*, May 31, 2011, http://www.nytimes.com/2011/06/01/us/politics/01cyber.html.

Sajó, András, *Constitutional Sentiments* (New Haven [Conn.]: Yale University Press, 2011).

Saro-Wiwa, Ken, "On Environmental Rights of the Ogoni People in Nigeria (1995)" in Micheline Ishay, The Human Rights Reader: Major Political Writings, Essays, Speeches, and Documents from the Bible to the Present (Routledge, 2007) 360-363.

Sassen, Saskia, *Territory, Authority,* R*ights: From Medieval to Global Assemblages* (Princeton University Press 2006).

Scahill, Jeremy, *Blackwater: The Rise of the World's Most Powerful Mercenary Army* (New York: Nation Books, 2007).

Schabas, William A., *Genocide in International Law: The Crime of Crimes*, 2d ed. (Cambridge: Cambridge University Press 2009).

Schmitt, Carl, *The Nomos of the Earth in the International Law of the Jus Publicum Europaeum*, trans. G.L. Ulmen (New York: Telos Press, 2003).

Schmitt, David D., "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflict," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, 2010, 151.

Schmitt, Michael N., ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013).

Schneier, Bruce, "Attributing the Sony Attack," Schneier on Security, Jan. 7, 2015, https://www.schneier.com/blog/archives/2015/01/attributing_the.html.

Seife, Charles, *Decoding the Universe: How the New Science of Information Is Explaining Everything in t*he Cosmos, from Our Brains to Black Holes, 2007.

Sen, Amartya, "Global Justice: Beyond International Equity," in *Global Public Goods: International Cooperation in the 21st Century*, ed. Inge Kaul, Isabelle Grunberg, and Marc Stern (New York, Oxford: Oxford University Press, 1999), 116–25.

Serageldin, Ismail, "Cultural Heritage as a Public Good: Economic Analysis Applied to Historic Cities," in *Global Public Goods: International Cooperation in the 21st Century*, ed. Inge Kaul, Isabelle Grunberg, and Marc Stern (New York, Oxford: Oxford University Press, 1999), 240–63, http://econpapers.repec.org/RePEc:oxp:obooks:9780195130522.

Sexton, Michael, "Accurately Attributing the Sony Hack Is More Important than Retaliating," *Georgetown Security Studies Review*, January 13, 2015, http://georgetownsecuritystudiesreview.org/2015/01/13/accurately-attributing-the-sony-hack-is-more-important-than-retaliating/.

Shachtman, Noah, "Pirates of the ISPs: Tactics for Turning Online Crooks Into International Pariahs," *Brookings Cybersecurity Paper*, June 2011, http://www.brookings.edu/~/media/Files/rc/papers/2011/0725_cybersecurity_shachtman/0725_cybersecurity_shachtman.pdf.

Shaw, Malcolm, *International Law*, 4th ed. (Cambridge: Cambridge University Press 1997)

Silverman, Jacob, "A Gun, a Printer, an Ideology," *The New Yorker*, May 7, 2013, http://www.newyorker.com/tech/elements/a-gun-a-printer-an-ideology.

Singer, Peter Warren, *Corporate Warriors: The Rise of the Privatized Military Industry* (Ithaca, NY: Cornell University Press, 2011).

Sledge, Matt, "Edward Snowden Gambles On Alliance With WikiLeaks," *The Huffington Post*, June 27, 2013, http://www.huffingtonpost.com/2013/06/27/edward-snowden-wikileaks_n_3506232.html.

Sneed, Tierney, "Sony Hack Takes Darker Turn," *US News & World Report*, December 17, 2014, http://www.usnews.com/news/articles/2014/12/17/sony-hack-takes-darker-turn-with-interview-terror-threat.

Snowden, Edward, "Testimony before the Parliament of the European Union," March 7, 2014, http://library.blountsfolly.com/space/items/show/171.

Sofner, Abraham, David Clark, and Whitfield Diffie, "Cyber Security and International Agreements," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, ed. Committee on Deterring Cyberattacks: Informing Strategies and Developing Options; National Research Council (Washington, DC; [s.l.]: National Academies Press, 2010), http://www.nap.edu/catalog.php?record_id=12997.

Solum, Lawrence B. and Minn Chung, "The Layers Principle: Internet Architecture and the Law," *Notre Dame L. Rev.* 79 (2003): 815.

Spar, Debora L., "The Public Face of Cyberspace," in *Global Public Goods: International Cooperation in the 21st Century*, ed. Inge Kaul, Isabelle Grunberg, and Marc Stern (New York, Oxford: Oxford University Press, 1999), 344–62.

Sparkes, Matthew, “Internet in North Korea: Everything You Need to Know,” December 23, 2014, sec. Technology, http://www.telegraph.co.uk/technology/11309882/Internet-in-North-Korea-everything-you-need-to-know.html.

Stadtmiller, Mandy, “Virtual Reality Sex Is Coming — and the Toys Are Already Here,” *Mashable*, May 29, 2015, http://mashable.com/2015/05/29/virtual-reality-sex/.

“Static,” *The Twilight Zone*, season 2, episode 20 (1961).

Stephenson, Neal, *Cryptonomicon* (New York: Avon Books 1999).

Stewart, Mark G. and John Mueller, “Cost-Benefit Analysis of Advanced Imaging Technology Full Body Scanners for Airline Passenger Security Screening,” *Journal of Homeland Security and Emergency Management* 8, no. 1 (2011), http://politicalscience.osu.edu/faculty/jmueller/ait2.pdf.

Stiglitz, Joseph E., “Knowledge as a Global Public Good,” in *Global Public Goods: International Cooperation in the 21st Century*, ed. Inge Kaul, Isabelle Grunberg, and Marc Stern (New York, Oxford: Oxford University Press, 1999), 308–25.

Stout, Hilary, “Comcast-Time Warner Cable Deal’s Collapse Leaves Frustrated Customers Out in the Cold,” *The New York Times*, April 26, 2015, http://www.nytimes.com/2015/04/27/business/media/mergers-collapse-leaves-frustrated-cable-customers-out-in-the-cold.html.

Streck, John, “Pulling the Plug on Electronic Town Meetings: Participatory Democracy and the Reality of Usenet,” in *The Politics of Cyberspace*, ed.

Chris Toulouse and Timothy W. Luke (New York: Routledge, 1998), 18–47.

Sunstein, Cass R., *Republic. Com 2.0* (Princeton, NJ: Princeton University Press, 2007).

Sy, J. Habib, "Global Communications for a More Equitable World," in *Global Public Goods: International Cooperation in the 21st Century*, ed. Inge Kaul, Isabelle Grunberg, and Marc Stern (New York, Oxford: Oxford University Press, 1999), 326–43.

Tambini, Damian, Danilo Leonardi, and Christopher T. Marsden, *Codifying Cyberspace: Communications Self-Regulation in the Age of Internet Convergence* (Routledge, 2008).

Tanz, Jason, "Playing for Time: A Father, a Dying Son, and the Quest to Make the Most Profound Videogame Ever," *Wired*, January 2016, http://www.wired.com/2016/01/that-dragon-cancer/.

Tate, Julie, "Bradley Manning Sentenced to 35 Years in WikiLeaks Case," *The Washington Post*, August 20, 2013, https://www.washingtonpost.com/world/national-security/judge-to-sentence-bradley-manning-today/2013/08/20/85bee184-09d0-11e3-b87c-476db8ac34cd_story.html.

Taylor, Adam, "The Simple Way Google Maps Could Side-Step Its Crimea Controversy," *The Washington Post*, April 1, 2014, https://www.washingtonpost.com/news/worldviews/wp/2014/04/01/the-simple-way-google-maps-could-side-step-its-crimea-controversy/.

Taylor, Jr., Fred and Jerry Carter, "Cyberspace Superiority Considerations," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton: Taylor & Francis, 2013), 13–25.

Thingaverse, https://www.thingiverse.com/ (last accessed September 30, 2015)

Timberg, Craig and Ellen Nakashima, "Agreements with Private Companies Protect U.S. Access to Cables' Data for Surveillance," *The Washington Post*, July 6, 2013, http://www.washingtonpost.com/business/technology/agreements-with-private-companies-protect-us-access-to-cables-data-for-surveillance/2013/07/06/aa5d017a-df77-11e2-b2d4-ea6d8f477a01_story.html.

Toulouse, Chris, "Introduction," in *The Politics of Cyberspace*, ed. Chris Toulouse and Timothy W. Luke (New York: Routledge, 1998), 1–16.

Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water, (entered into force October 10, 1963).

Treaty Between The United States of America and The Union of Soviet Socialist Republics on The Limitation of Anti-Ballistic Missile Systems (ABM Treaty) (May 26, 1972).

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, (entered into force October 10, 1967).

Treaty on the Non-Proliferation of Nuclear Weapons, 729 UNTS 161 (entered into force

March 5, 1970).

Turner, Fred, *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network and the rise of Digital Utopianism* (Chicago: University of Chicago Press 2006).

UN Charter (1945).

United Nations Convention on the Law of the Sea (December 10, 1982).

United Nations General Assembly, Res. 217 A(III). Universal Declaration of Human Rights, (December 10, 1948).

United Nations General Assembly, "Res. 37/92: Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting," December 10, 1982.

United Nations Human Rights Council's Working Group on Arbitrary Detention, Opinion No. 54/2015 concerning Julian Assange (Sweden and the United Kingdom of Great Britain and Northern Ireland).

United Nations Security Council, S/RES/138 Question relating to the case of Adolf Eichmann (1960).

United States Air Force, *Legal Reviews of Weapons and Cyber Capabilities, A.F. Instruction 51-402* (July 27, 2011).

United States Constitution.

United States Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," July 2011, http://library.blountsfolly.com/space/items/show/184.

United States Department of Justice, "Exhibit A: Procedures Used by the National Security Agency for Targeting Non-United States Persons

Reasonably Believed to Be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended," (July 28, 2009).

United States Department of Justice, "Memorandum for the Attorney General: Proposed Amendment to the Department of Defense Procedures to Permit the National Security Agency to Conduct Analysis of Communications Metadata Associated with Persons in the United States," (November 20, 2007.)

United States Department Of State, "Outcomes from the International Telecommunication Union 2014 Plenipotentiary Conference in Busan, Republic of Korea," Press Release|Media Note, *U.S. Department of State*, (November 11, 2014), http://www.state.gov/r/pa/prs/ps/2014/11/233914.htm.

United States v. Jones, 132 S. Ct. 945 (2012).

United States v. Wang et al. - Indictment (W.D. Penn. 2014).

Verizon v. FCC, No. 11-1355, 740 F. 3d 623 (Court of Appeals, Dist. of Columbia Circuit 2014)

Wakefield, Jane, "Smart LED Light Bulbs Leak Wi-Fi Passwords," *BBC News*, July 8, 2014, http://www.bbc.com/news/technology-28208905.

Walzer, Michael, "The Moral Standing of States: A Response to Four Critics," *Philosophy & Public Affairs*, 1980, 209–29.

Wassenaar Arrangement, "About Us," http://www.wassenaar.org/about-us/ (last visited Feb. 17. 2016).

Weisman, Aly, "A Timeline of the Crazy Events in the Sony Hacking Scandal," *Business Insider*, December 9, 2014, http://www.businessinsider.com/sony-cyber-hack-timeline-2014-12.

Werbach, Kevin, "A Layered Model for Internet Policy," *J. on Telecomm. & High Tech. L.* 1 (2002): 37.

Werbach, Kevin, "Breaking the Ice: Rethinking Telecommunications Law for the Digital Age," *J.* on Telecomm. & High Tech. L. 4 (2005): 59.

White House, Executive Order -- Imposing Additional Sanctions with Respect to North Korea (Jan. 2, 2015), http://www.whitehouse.gov/the-press-office/2015/01/02/executive-order-imposing-additional-sanctions-respect-north-korea

White House, "PPD-20: U.S. Cyber Operations," January 2013,

Alfred North Whitehead, *Science and the Modern World* (Simon and Schuster, 1967).

Wight, Martin, *International Theory: The Three Traditions* (Holmes & Meier for the Royal Institute of International Affairs, 1992).

Wikileaks, "What is Wikileaks" (Nov. 3, 2015) https://wikileaks.org/What-is-Wikileaks.html.

Wilson, Woodrow, "Fourteen Points" (Jan. 8, 1918) http://avalon.law.yale.edu/20th_century/wilson14.asp.

Wingfield, Thomas C., "Legal Aspects of Offensive Information Operations in Space," 1998, http://www.au.af.mil/au/awc/awcgate/dod-io-legal/wingfield.pdf.

Wittes, Benjamin, "The Intelligence Legitimacy Paradox," blog, *Lawfare*, (May 15, 2014), http://www.lawfareblog.com/2014/05/the-intelligence-legitimacy-paradox/.

World Wide Web Consortium, "About W3C," https://www.w3.org/Consortium/ (last visited Feb. 11, 2016).

Yahoo! Inc. v. La Ligue Contre Le Racisme, 433 F. 3d 1199 (9th Cir. 2006).

Yannakogeorgos, Panayotis A. and Adam B. Lowther, "The Prospects for Cyber Deterrence: American Sponsorship of Global Norms," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton: Taylor & Francis, 2013), 49–77.

Zaid, Mark S., "Military Might versus Sovereign Right: The Kidnapping of Dr. Humberto Alvarez-Machain and the Resulting Fallout," *Hous. J. Int'l L.* 19 (1996): 829.

Zalnieriute, Monika, "An International Constitutional Moment for Data Privacy in the Times of Mass-Surveillance," *International Journal of Law and Information Technology* 23, no. 2 (2015): 99–133.

Zalnieriute, Monika and Thomas Schneider, "ICANN's Procedures and Policies in the Light of Human Rights, Fundamental Freedoms and Democratic Values" (Council of Europe, June 16, 2014).

Zetter, Kim, *Countdown to Zero Day : Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown Publishers, 2014).

Zetter, Kim, “Everything We Know About Ukraine’s Power Plant Hack,” *WIRED*, January 20, 2016, http://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/.