IF YOU LOVE INFORMATION, SET IT FREE!
PROMOTING FREEDOM OF EXPRESSION BY EXPANDING CYBERSPACE OPERATIONS

BY

KRIS E. BARCOMB, MAJOR, USAF

A THESIS PRESENTED TO THE FACULTY OF
THE SCHOOL OF ADVANCED AIR AND SPACE STUDIES
FOR COMPLETION OF GRADUATION REQUIREMENTS

SCHOOL OF ADVANCED AIR AND SPACE STUDIES
AIR UNIVERSITY
MAXWELL AIR FORCE BASE, ALABAMA
JUNE 2012

DISCLAIMER

ABOUT THE AUTHOR

Maj Kris Barcomb received his commission through the Air Force Reserve Officer Training Corps at Clarkson University in May 1999. He is a developmental engineer and operator for the US Air Force. His first assignment was at Vandenberg AFB, California where he performed spacelift operations as an Atlas and Titan Launch Controller and Launch Director. He then attended the Rochester Institute of Technology under the Air Force Institute of Technology's Advanced Academic Degree program. After earning his degree and spending six months working with industry, he followed on to the National Capital Region. While he was there, he worked in satellite operations, space systems acquisition, and research and development.

Major Barcomb has a B.S. in Computer Engineering from Clarkson University, an M.B.A from the University of La Verne, an M.S. in Imaging Science from the Rochester Institute of Technology, and an M.S. in Cyber Warfare from the Air Force Institute of Technology. Following graduation from the School of Advanced Air and Space Studies, he will become a cyberspace strategist for 24AF at Lackland AFB, Texas. He is married to a wonderful woman and they are both blessed with two beautiful children.

ACKNOWLEDGMENTS

This thesis would not have been possible without the support of many truly remarkable people. I would like to offer my sincere appreciation to faculty and staff at the School of Advanced Air and Space Studies. This is an extraordinary academic institution and I am blessed to have been a part of it. In particular, I would like to thank my advisor, Dr. John Sheldon. His guidance and insight helped shape the final product in many invaluable ways. I would also like to thank Col Suzanne Buono for directing our cyberspace course and for her perceptive critique of this work. To my fellow students in Class XXI, all I can say is "Wow!" I am humbled to have been included in such an outstanding group of leaders, professionals, dedicated soldiers and strategists.

To my family, I offer my sincerest love and appreciation. You have stood by me, supported me and sacrificed for me throughout this long year. You are the best!

Finally, I would like to thank God for the many gifts, opportunities and blessings He has given me. I pray that I am able to put them to good use. With His help, I'm sure that I can.

ABSTRACT

This thesis examines freedom of expression in the Internet Age. Throughout history, authoritarian regimes have used information control as a way to retain their power, but information technology is making achieving this objective increasingly difficult. In the modern era, attempting to control information may be a strategic weakness of authoritarian regimes that democratic nations can exploit. By expanding access to the Internet and helping oppressed individuals circumvent political censorship, democratic nations may be able to expand the sphere of global freedom and produce a more peaceful and stable world order. This thesis reviews how both censorship and circumvention work. It also examines how various agencies in the United States view cyberspace and the role that cyberspace plays in their strategies for influencing others. Freedom will not come without some difficulty; therefore, potential problems associated with promoting freedom through information technology are also presented. Finally, this thesis presents a series of recommendations, largely focused on the Department of Defense, for promoting freedom of expression through Internet freedom initiatives.

CONTENTS

ILLUSTRATIONS

Introduction

If you want to liberate a government, give them the Internet.
- Wael Ghonim

Censorship reflects a society's lack of confidence in itself. It is a hallmark of an authoritarian regime.
– Potter Stewart

Cyberspace exists to promote fast, global and robust information sharing. Rich applications, fault-tolerant networks, diverse connectivity paths, distributed algorithms and low-cost means of access have helped the World Wide Web, and many other information-sharing mechanisms of cyberspace, touch the lives of nearly everyone on the planet. Modern information technologies have fostered a worldwide information society that in many ways transcends geographic boundaries, cultures, and socio-economic statuses. The free flow of information in and through cyberspace is revolutionizing human affairs on a global scale.

Despite the tremendous benefits attained through information technologies, authoritarian governments and dictatorial leaders increasingly see widespread access to the Internet as a threat to their existence. Many are suppressing information sharing by shutting down communication services, expanding surveillance programs and enacting restrictive laws. They take these actions because they see information freedom as detrimental to their means of control. Often, their actions are in response, not to hostilities originating outside their borders, but to their own citizens yearning for the same freedoms enjoyed by much of the democratic world. These governments see freedom within their populaces as a threat to their strategic interests. Indeed, as Walter

Wriston proclaimed, "The control of information is the bedrock of all totalitarian regimes."[1] He expands on the point as follows:

> Information has always been a key to political power. But when information abounds and overflows in public, when an entire society is privy to what once may have been closely guarded "secrets," political strategies based on a close holding of information no longer work. When everyone in the nation, at least potentially, can join in a single national "conversation," there are only two ways… in which a government can keep its power: It can allow its policies to be guided by that national conversation or it can revert to a level of repression that even totalitarian regimes find inconvenient in the best of times and which in an age of instant information brings opprobrium.[2]

Through sound, unified policy across the whole of government, leadership by example and partnership with private industry, the United States can capitalize on this strategic vulnerability of repressive regimes.

Before policy makers can see information control as a strategic weakness, they must first see information freedom as a strategic strength. The United States has embraced freedom since the first colonies appeared along the east coast of America in the 17th century. This belief in a free society was formally expressed later in the Declaration of Independence of 1776 and then codified in the Constitution in 1787. In the Declaration of Independence, the Founding Fathers declared, "All men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness. That to secure these rights, Governments are instituted among Men, deriving their just powers from the consent of the governed."[3] Their position on liberty rested in their firm belief that mankind does have the power to convey fundamental

---

[1] Walter B. Wriston, *The Twilight of Sovereignty: How the Information Revolution Is Transforming Our World* (New York: Scribner, 1992), 52.
[2] Wriston, *The Twilight of Sovereignty*, 138.
[3] United States, "Declaration of Independence," 4 July 1776. http://www.archives.gov/exhibits/charters/declaration_transcript.html (accessed 8 April 2012).

human rights. These rights do not come from monarchs or dictators, despite these rulers' claims to the contrary. They are inherent in us all.

The Founding Fathers rejected the idea of a highly centralized government under the guidance of an all-powerful sovereign. They spurned the coldhearted realism found in Thomas Hobbes' worldview that "every man is enemy to every man" and that mankind's existence is characterized by "continual fear, and danger of violent death; and the life of man, solitary, poor, nasty brutish, and short."[4] America would not return to a Leviathan state after rejecting the British monarchy. Instead, the Founding Fathers held firm to a belief that mankind was more good than evil and codified a liberal ideology into America's founding documents. In doing so, they established the fledgling nation under principles of freedom and self-determination that are still deeply ingrained in American culture over two centuries later.

Perhaps the most revolutionary tenet of the Declaration of Independence is its pronouncement that "Governments are instituted among Men, deriving their just powers from the consent of the governed." The Founding Fathers believed that governments did not have any inherent power of their own. The Constitution of the United States established this concept as the law of the land. Its first sentence states, "We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defence, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America."[5] The entire US system of government is based on the fact that any power the government has is only the result of its citizens ("We the people…") permitting it to exercise

[4] Encyclopedia Britannica, *Great Books #23 - Machiavelli – Hobbes*, (University of Chicago, 1952), 85.
[5] United States, "The Constitution of the United States of America," 17 September 1778. http://www.archives.gov/exhibits/charters/constitution_transcript.html (accessed 8 April 2012).

that power ("do ordain and establish"), and that power may be altered or abolished according to the will of the governed.

It is no coincidence that the first of the ten amendments articulated in the Bill of Rights provides for the free flow of information and ideas within American society. The First Amendment ensures the freedom of religion, the freedom of speech, the freedom of the press, a right to peaceably assemble and to petition the government for the redress of grievances. These first freedoms enable the American society to educate itself so that it can make sound decisions when granting power to the government. This is the essence of self-determination, a principle crucial to many considerations of what is just and unjust in both domestic and international relations.

Two-and-a-quarter centuries later, the Internet has become the primary means of transmitting information among the citizens of the United States and in many other countries around the world. Never before in the history of mankind has there been so much access to so much information in so little time with so little effort. The Founding Fathers would be truly amazed at the technologies of cyberspace and its ability to promote the freedoms described in the First Amendment. The US has protected these freedoms with both blood and treasure because it recognizes the tremendous benefits they provide to society as a whole. The US sees these rights as fundamental to all of humanity, and as such, it strives to protect them for all, not just its own citizens. For the last century, America has demonstrated its willingness to protect the oppressed across the world so that they may also share in the dignity and opportunities that come with liberty.

In the Information Age, America's strategy for extending access to these freedoms must change to acknowledge the realities of cyberspace. Military power projection will retain a prominent role for the foreseeable

future, but from an effects-based perspective, the military may be able to do even more good by simply ensuring that others have the means to participate in the free flow of information across cyberspace. President George W. Bush said, "Men and women in every culture need liberty like they need food and water and air. Everywhere that freedom arrives, humanity rejoices; and everywhere that freedom stirs, let tyrants fear."[6] By addressing the tyrants, he was not just referring to the fear they would feel over the military power that he was exercising at the time, but instead he was implying they should fear the power inherent in a free people for establishing their own destiny.

President Bush's thoughts echoed those of his predecessor, Ronald Reagan, who promoted information freedom as a means of tearing down the Iron Curtain. When urging Mikhail Gorbachev to open up the totalitarian Soviet Union, Reagan avowed, "Information is the oxygen of the modern age. It seeps through the walls topped by barbed wire, it wafts across the electrified, booby-trapped borders." [7] He added, "The Goliath of totalitarianism will be brought down by the David of the microchip."[8] Strategy is the combination of ways and means to achieve ends. Both leaders saw information as the *means*, freedom as the *ways* and peace as the *ends*.

The notion that freedom and peace are mutually reinforcing is not new. Immanuel Kant proclaimed his theory of "Perpetual Peace" in 1795. He predicted that the number of states founded on liberal principles would continue to expand. As a result, war would diminish because he believed, due to their compatible values and character, liberal states

---

[6] George W. Bush. "Remarks by the President from the USS Abraham Lincoln," Delivered 1 May 2003. http://georgewbush-whitehouse.archives.gov/news/releases/2003/05/20030501-15.html (accessed 7 April 2012).

[7] Associated Press, "Reagan Urges 'Risk' on Gorbachev: Soviet Leader May Be Only Hope for Change, He Says," *Los Angeles Times*, 13 June 1989. http://articles.latimes.com/1989-06-13/news/mn-2300_1_soviets-arms-control-iron-curtain (accessed 20 April 2012).

[8] Associated Press, "Reagan Urges 'Risk' on Gorbachev."

would not fight against each other. In his theory, Kant also found incompatibilities between liberal and non-liberal states, which led him to conclude that war would persist between them. Therefore, international peace required nations to foster the global adoption of three "definitive principles": 1) the civil constitution of every state should be republican; 2) the law of nations should be founded on a federation of free states; and 3) the law of world citizenship should be limited to conditions of universal hospitality. The first principle reflects how states should organize to protect their internal freedoms, while the latter two concern international freedoms for promoting the exchange of ideas and commerce.[9] Kant's work planted the foundations for modern "Democratic Peace Theory."

Though Kant's work predated the Information Age, the Internet can be viewed as a facilitator for promoting Kant's "pacific union" of nations. If one subscribes to Kant's ideology, then the Internet is an ideal medium for promoting the free exchange of information both within a nation and between nations. Low-cost information technologies help individuals and organizations band together for greater political effect and, hopefully, to enhance their political situations. As Jonathan Zittrain and John Palfrey proclaimed, "The Internet is a potential force for democracy by increasing means for citizen participation in the regimes in which they live. The Internet is increasingly a way to let sunlight fall upon actions of those in power—and providing an effective disinfectant in the process."[10]

If liberal states are less likely to go to war with each other, and the Internet facilitates the spread liberalistic ideals, then nations can and ought to promote the spread of information and communication

[9] Michael W. Doyle, *Ways of War and Peace: Realism, Liberalism, and Socialism* (New York: W. W. Norton & Company, 1997), 251-284.
[10] Jonathan Zittrain and John Palfrey, "Internet Filtering: The Politics and Mechanisms of Control," *Access Denied: the Practice and Policy of Global Internet Filtering*, Jonathan L. Zittrain et al., eds. (Cambridge, MA: The MIT Press, 2008), 50.

technologies to neighboring states. Kant would likely have seen attempts by non-liberal states to suppress information as detrimental to world peace and, by extension, would likely have seen peaceful efforts to circumvent that oppression as just. Michael Doyle summarizes Kant's view as follows:

> [Kant] argues that each nation "can and ought to" demand that its neighboring nations enter into the pacific union of Liberal states—that is, become republican.... Internationally, free speech and the effective communication of accurate conceptions of the political life of foreign peoples is essential to establish and preserve the understanding on which the guarantee of respect depends.[11]

Promoting Internet freedom is not high on the priority list of most Americans. In many instances the opposite is true because they see the US reliance on information technology as a strategic vulnerability.[12] That myopic and risk averse viewpoint fails to appropriately consider the benefits such technologies provide the country. It also fosters a mindset that puts decision-makers on the strategic defensive in cyberspace. As this thesis will demonstrate, many existing US policies concerning cyberspace are reactive. They emphasize protection and defense primarily through "denial of benefit" strategies, such as security awareness initiatives, properly configuring networks and software patching. While these means are extremely important for securing America's information, the US needs to include more proactive strategies for cyberspace that help reinforce American values.

One such strategy is to help ensure the oppressed have access to digital information, the capacity to express their thoughts online and the tools necessary to self-organize. America's own strategic interests will be

[11] Doyle, *Ways of War and Peace*, 282.
[12] Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, Reprint ed. (New York: Ecco, 2011).

enhanced by promoting broader Internet access and providing tools to circumvent political censorship. America will not be able to control how liberty is used once it is attained, but it must trust, as its forefathers did, that the greatest benefits will emerge from people empowered with freedom.

This thesis examines the implications of adopting a strategy for promoting Internet freedom. The research focuses on the *ways* and *ends* of strategy. It leaves the *means* to future analysis since prioritizing resources is more a question of efficiency than effect. The focus here is on the effect. It begins by examining the practical *ways* of implementing such a strategy and then examines the diversity of existing US policy on the subject. Next, it scrutinizes potential *ends* to help policy makers decide if the benefits outweigh the risks. Finally, it concludes with a series of recommendations aimed primarily at the Department of Defense (DOD) for preparing for, and for supporting, an Internet freedom strategy.

Chapter 1 provides a detailed review of the kinds of information that nations aim to censor; the range of technical, legal, economic and social mechanisms used to control information on the Internet; and how those mechanisms have evolved over time. Then, it categorizes and explains tools for both censorship and circumvention in depth. While the technical aspects of digital censorship have received more attention historically, the legal, economic and social forms of censorship are becoming more effective and harder to overcome.

Chapter 2 shows how freedom of expression is a fundamental value, not only for America, but also for the international community. It then examines the methods that the DOD, the Department of Homeland Security (DHS) and the State Department employ to influence international actors toward this value. Each agency has unique and sometimes conflicting approaches with respect to cyberspace. The goal

of the chapter is to identify the similarities and difference in policy to help US policy makers form a more comprehensive cyberspace strategy.

Chapter 3 shifts the focus toward the potential consequences of adopting a strategy of promoting Internet freedom. First, the chapter examines the consequences of helping the oppressed overcome their oppressors. The historical records indicate that this process is rarely peaceful. So, it explores the nature of revolutions and how modern information technology may either help or hinder their success. Second, it describes how increasing the ability for populations to connect to information through modern ICT, if not done carefully, may make them more vulnerable to the dictates of oppressive regimes. For example, putting more people online may increase their susceptibility to monitoring or attribution. Finally, policy makers must realize that simply having freedom does not necessarily make one virtuous. The view held by many proponents of Internet freedom—that people are generally more good than evil—does not imply that evil will not be done. Therefore, the chapter examines some of the negative outcomes that are likely to accompany the positive ones.

The final chapter offers a series of recommendations for policy makers, particularly those within the DOD, to help implement an Internet freedom strategy. It covers a range of topics, including doctrinal changes, training, strategic communication and cooperation with other stakeholders. Hopefully, by implementing these recommendations the US government will be able to present a more unified and consistent approach to promoting freedom and democracy throughout the world.

Ultimately, the fundamental assumptions of this thesis are that the freedom inherent in the United States is one of its greatest strategic strengths and that the Internet serves to enhance this advantage. This work views attempts to control freedom in the modern information

technology environment as a strategic vulnerability of authoritarian regimes because, as Wriston stressed, "Draconian systems for controlling the flow or use of information tend to destroy or waste it."[13] By appropriately applying this strategic strength against the strategic vulnerabilities inherent in authoritarian governments, the US can expand the sphere of freedom and enhance global peace. The US must protect information freedom so its benefits are not destroyed or wasted.

[13] Wriston, *The Twilight of Sovereignty*, 35.

Chapter 1

Censorship and Circumvention

Freedom's untidy, and free people are free to make mistakes and commit crimes and do bad things. They're also free to live their lives and do wonderful things, and that's what going to happen here.
– Donald Rumsfeld

In a fair fight, truth wins.
– Kristin Lord

Due to the very nature of cyberspace, when people think about online censorship, their initial focus tends to be on the technical mechanisms for control and the corresponding technical mechanisms for circumvention. The terms censorship and circumvention conjure up notions of a cat-and-mouse battle between government controlled firewalls and packet sniffers and citizens encrypting their communication and anonymizing their activities through proxies. This, most certainly, is a significant part of controlling behavior online, but technical methods alone do not present the full spectrum of regulation.

To overcome this narrow perspective on censorship and circumvention, this chapter examines information control in a more comprehensive manner. While it does describe many of the technical capabilities in detail, it broadens the aperture by also reviewing legal, social and market forces that either constrain or promote different types of behavior. To guide the reader through the complex and interconnected array of methods that states use to regulate the online behavior of their citizens, this chapter is organized around answering a series of relevant questions: What kinds of information do states typically regulate? How has government regulation of cyberspace evolved over time? How is information regulated in cyberspace? And, finally,

what can be done to promote information freedom in the face of these constraints?

What Kinds of Information Do States Typically Regulate?

An important first step in understanding Internet freedom is to recognize the different types of content that states seek to regulate. Analysis done by the OpenNet Initiative (ONI) provides many details. In addition to categorizing the different types of restricted content, the ONI research probes the rationale for why states block particular classes of information. According to Robert Faris and Nart Villeneuve, who helped coordinate and conduct the ONI research on the topic, there are essentially six categories of information that are being filtered around the world: 1) *political content*, 2) *social content*, 3) *information related to conflict and security*, 4) *intellectual property*, 5) *economic interests* and 6) *Internet tools.*[1]

The first category deals with censoring political topics and it has been around for as long as there have been governments. The fear of losing control over their populace, leads many governments to suppress political opposition and dissent. Faris and Villeneuve contend, "Politically motivated filtering is characteristic of authoritarian and repressive regimes."[2] Political filtering typically includes stifling freedom of speech for both individuals and the media; suppressing political transformation and opposition parties; and preventing attempts to reform the political, legal or governance mechanisms of the state. Political censorship often strikes at the heart of individual liberty and self-determination.

[1] Robert Faris and Nart Villeneuve, "Measuring Global Internet Filtering," *Access Denied: the Practice and Policy of Global Internet Filtering*, Ronald Deibert et al., eds. (Cambridge, MA: The MIT Press, 2008), 9,12.
[2] Faris and Villeneuve, "Measuring Global Internet Filtering," 9.

The second category, social filtering, aims to prevent access to content deemed objectionable to the values, norms and morals of society. Most countries engage in this form of filtering to some degree, even democratic ones. The list of topics in this category generally includes racism, pornography, gay/lesbian content, gambling, alcohol and drugs, religious content, public health, sensitive or controversial history and women's rights.[3]

Conflict and threats to national security comprise the third category for state censorship. In some ways this category often overlaps with the first category, politics. Authoritarian states often perceive opposing political speech as threats to national security, even if their version of national security only reflects their own desire for self-preservation. Setting aside the purely political and generally non-violent activities described in the first category, threats to national security that may be filtered include information related to militant groups, extremists, separatists or terrorists; foreign relations and militaries; and external sources of information deemed contrary to the interests of the safety and security of the state.[4]

Protecting intellectual property represents a fourth category over which nations assert a form of censorship. This category is more closely related to content regulation than it is to censorship, but the methods employed to enforce those regulations are often similar. Western Europe and North America are most active in developing both legal and technical mechanisms to protect intellectual property rights.[5] Examples include the Digital Millennium Copyright Act (DMCA), Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PIPA) and the Stop Online Piracy Act (SOPA). Each of these laws aims to

[3] Faris and Villeneuve, "Measuring Global Internet Filtering," 7.
[4] Faris and Villeneuve, "Measuring Global Internet Filtering," 7.
[5] Faris and Villeneuve, "Measuring Global Internet Filtering," 9.

curtail the theft of intellectual property, either through threat of prosecution or through blocking and filtering.

The fifth category is protecting economic interest. While this category relates in some ways to the previous one, it is generally more concerned with protecting favorable commercial activity within a state or between states. For example, Faris and Villeneuve highlight how some states block low-cost international telephone services that use Voice Over Internet Protocol (VOIP). Since VOIP services offer a cheaper alternative to traditional telephony services, the customer base for large telecommunications companies are dwindling, which in turn threatens their lucrative, monopolistic business models.[6] States may censor particular types of international economic information in parallel with the trade regulations to support the domestic economy and protect markets, jobs and other financial interests.

The final category is Internet tools. This category is different from the previous ones because it aims to block access to the means for obtaining information rather than blocking access to the ends—the information itself. Blocking particular classes of Internet tools and services prevents users from obtaining the ability to access or produce information in the other categories. In this sense, this category is a more indirect method of censorship. It inhibits the enablers, rather than obstructing content directly. Some of the Internet capabilities that nations block are translation tools, anonymizers, blogging services, social media sites, web proxies, open source software, encryption services and archiving sites.[7]

The research done by the ONI suggests that not all content filtering is inherently malevolent. For example, there is nearly universal support

[6] Faris and Villeneuve, "Measuring Global Internet Filtering," 12.
[7] Faris and Villeneuve, "Measuring Global Internet Filtering," 9.

for stopping the promotion of mass atrocities or the exploitation of minors. Obviously, these forms of censorship are not the target of Internet freedom strategies. Instead, strategies aimed at promoting freedom to communicate should target censorship in the political and Internet tools categories. They should also strive to circumvent attempts to suppress information in the conflict and security category when efforts to suppress information in that category hinder a population's ability to achieve a better form of government, a better education or a better way of life.

How Has Government Regulation of Cyberspace Evolved Over Time?

The ONI has been researching access controls on the Internet since 2007. They have documented the censorship capabilities in 70 states, probed nearly 300 Internet Service Providers (ISP) within those states and tested access to almost 130,000 websites from within each state. Their research has led them to conclude that cyberspace regulation has evolved through four distinct phases: 1) *Open Commons*, 2) *Access Denied*, 3) *Access Controlled*, and 4) *Access Contested*. [8]

Open Commons Era

The first era, *Open Commons*, began in the 1960s and ran through the year 2000. During this period, the Internet was essentially wide open. Its users made sweeping libertarian declarations about the new medium. Some, like former lyricist for the Grateful Dead and co-founder of the Electronic Frontier Foundation, John Perry Barlow, took aim at government regulation by writing "A Declaration of the Independence of Cyberspace." In it, Barlow wrote, "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us

[8] Ronald Deibert, John Palfrey, Rafal Rohozinski and Jonathan Zittrain, "Access Contested: Toward the Fourth Phase of Cyberspace Controls," *Access Contested: Security, Identity, and Resistance in Asian Cyberspace Information Revolution and Global Politics*, Ronald Deibert et al., eds. (Cambridge, MA: The MIT Press, 2012), 6.

alone. You are not welcome among us. You have no sovereignty where we gather."[9]

In a similar fashion, Rick Levine, Christopher Locke, Doc Searls and David Weinberger published "The Cluetrain Manifesto" as a call to action to businesses and markets. They wrote the manifesto in a manner resembling Martin Luther's "95 theses," which fostered the Protestant Reformation. Levine and his co-authors hoped to show how the Internet would usher in a new era of commerce that would break down traditional organizational models and be dominated by human to human interaction. They expressed their view of Internet liberty as follows:

> We embrace the Web not knowing what it is, but hoping that it will burn the org chart -- if not the organization -- down to the ground. Released from the gray-flannel handcuffs, we say anything, curse like sailors, rhyme like bad poets, flame against our own values, just for the pure delight of having a voice. And when the thrill of hearing ourselves speak again wears off, we will begin to build a new world. That is what the Web is for.[10]

Governments, on the other hand, mostly ignored electronic communications or only mildly regulated the content.[11] The Internet was in its infancy. Despite the fervor of those who were a part of the early Web, there were simply not that many people online and there were even fewer politicians who understood the technology in a manner that would have allowed them to regulate it. At the time, there seemed to be many more pressing issues than worrying about a niche collective of enthusiastic "netizens."

---

[9] John P. Barlow, "A Declaration of the Independence of Cyberspace," 8 February 1996, https://projects.eff.org/~barlow/Declaration-Final.html (accessed 22 February 2012).
[10] Rick Levine et al., "The Cluetrain Manifesto: The End of Business as Usual" (Da Capo Press, 2001), 45. Bob Seidensticker, *Future Hype: the Myths of Technology Change* (Berkeley, CA: Berrett-Koehler Publishers, 2006), 39.
[11] Deibert, Palfrey, Rohozinski and Zittrain, "Access Contested," 6.

Not only was the threat posed by the Internet relatively confined, but even if states had wanted to regulate it, there were practical reasons impeding their ability to do so. Lawrence Lessig asserts that the fundamental design of the Internet prevented states from regulating behavior because it was not possible to know 1) who someone was, 2) where they were or 3) what they were doing.[12] The very architecture of cyberspace in this first era precluded its regulation. As the earlier quotes attest, many early online participants viewed the Web through libertarian eyes. Most believed that the government could never regulate the Internet and that it was beneficial that they did not.[13]

Access Denied Era

The relatively pristine openness of digital communications changed between the year 2000 and 2005 as cyberspace moved into the *Access Denied* era. According to Internet World Stats, the number of Internet users exploded from 16 million in 1995 to over 300 million in 2000.[14] Governments began taking serious notice of the rapidly growing percentage of their populations communicating online. Many states felt compelled to curtail objectionable Internet activity and began implemented filtering and blocking mechanisms. The attitudes of the public also changed as they felt the effects of a completely unregulated digital domain and reality began to set in. Most people realized they would have to accept some forms of regulation to successfully prevent problems ranging from relatively benign nuisances, such as spam, to more nefarious activity, such as identity theft, copyright infringement and especially the sexual exploitation of minors.[15]

---

[12] Lawrence Lessig, *Code: Version 2.0*, 2nd ed. (New York: Basic Books, 2006), 23.
[13] Lessig, *Code: Version 2.0*, 27.
[14] "Internet Growth Statistics," http://www.internetworldstats.com/emarketing.htm (Accessed 15 Feb 2012).
[15] Lessig, *Code: Version 2.0*, 27.

The methods for regulating content in this phase were largely technical in nature and not generally very sophisticated. Savvy users who understood the censorship mechanisms could bypass them with relatively little difficulty. In general, though, this was not a significant problem for regulators because the preponderance of users would never do so and the regime's filtering mechanisms would be predominantly effective despite the workarounds.[16] This era was dominated by what Ronald Deibert and Rafal Rohozinski call *first-generation controls*. These types of controls "focus on denying access to specific Internet resources by directly blocking access to servers, domains, keywords, and IP addresses. This type of filtering is typically achieved by the use of specialized software or by implementing instructions manually into routers at key Internet choke points."[17]

States often begin their censorship efforts under popular mandates for blocking specific types of content that are widely perceived as objectionable. Once they justify the initial investment and put the capabilities to censor in place, the state often finds that the barriers to blocking other forms of content are less difficult to overcome. For example, the same mechanisms for filtering access to sexually explicit content are often no different than those used to filter the content from a political opposition party. Technically, it is usually only a matter of changing the key words to be filtered or modifying the list of blocked uniform resource locators (URL) or Internet protocol (IP) addresses.

Lessig cautions citizens to understand the long-term effects of digital censorship, even when the initial case for censorship is widely seen as a public good. He states, "Liberty depends on the regulation remaining expensive. Liberty comes with friction. When it becomes easy

[16] Deibert, Palfrey, Rohozinski and Zittrain, "Access Contested," 10.
[17] Ronald Deibert and Rafal Rohozinski, "Control and Subversion in Russian Cyberspace," *Access Controlled: the Shaping of Power, Rights, and Rule in Cyberspace*, Ronald Deibert et al., eds. (Cambridge, MA: The MIT Press, 2010), 22.

or cheap to regulate, however, this contingent liberty is at risk."[18] This slippery slope of censorship helps perpetuate the practice with even greater effect in the subsequent phases of control.

Access Controlled Era

The next phase of cyberspace regulation, *Access Controlled,* lasted from 2005 to 2010. This phase was marked by a two-pronged strategy for asserting more government control over the Internet. The first method was to improve the technological sophistication for filtering and blocking unacceptable content. The censorship technologies that emerged during this era were more dynamic, timelier and more difficult to circumvent. Even though these technologies were more capable, they were still driven from the top down. To overcome this limitation, governments began incentivizing self-censorship by enacting logging, registration, licensing and identity requirements on both people and providers. During the *Access Controlled* phase, governments took advantage of the fact that when people know they can be identified and their behavior monitored, they are less likely to break the law.

Deibert and Rohozinski describe the censorship techniques used in the *Access Controlled* phase as follows:

> Second-generation controls aim to create a legal and normative environment and technical capabilities that enable state actors to deny access to information resources as and when needed, while reducing the possibility of blowback or discovery. Second-generation controls have an overt and a covert track. The overt track aims to legalize content controls by specifying the conditions under which access can be denied. Instruments here include the doctrine of information security as well as the application of existent laws, such as slander and defamation, to the online environment. The covert track establishes procedures and technical capabilities that allow content controls to be applied "just in time," when the information being targeted

[18] Lessig, *Code: Version 2.0*, 310.

> has the highest value (e.g., during elections or public demonstrations), and to be applied in ways that assure plausible deniability.[19]

Access Contested Era

The final era of cyberspace regulation, *Access Contested*, is the one we are living in today. All of the previous methods for censoring information remain, but a very public battle is emerging over who should control the medium. Citizens, organizations, corporations and governments are all vying for the right to exercise power openly in cyberspace. Examples abound—the Iranian Green Revolution, the Egyptian Revolution and the Jasmine Revolution in Tunisia. A Bollywood studio in India has even contracted with a cybersecurity firm to perform a Distributed Denial of Service (DDoS) attack on sites that offered its films for download.[20] Evidence of this period in Internet history can also be found in the recent backlash in the US against two pieces of proposed legislation, SOPA and PIPA. US citizens took to the Web to voice their opinions and many websites either "went dark" in protest (most notably Wikipedia), or prominently objected to the legislation on their home pages.[21]

In the *Access Denied* and *Access Contested* phases, populations fought for a right to speak, to express their opinions and demonstrate their support for a particular cause. In the *Access Contested* phase, government ideas increasingly have to compete against those of their own populations and even the populations and governments of other states. The struggle is shifting from a fight over speech to a battle for attention. Some are allowing democracy to decide, while other more authoritarian governments are enhancing their electronic propaganda

[19] Deibert and Rohozinski, "Control and Subversion in Russian Cyberspace," 24.
[20] Deibert and Rohozinski, "Control and Subversion in Russian Cyberspace," 34.
[21] Dylan Stableford, "As Wikipedia Goes Dark to Protest SOPA, Media Offer Support," *Yahoo! News*, 18 January 2012. http://news.yahoo.com/blogs/cutline/wikipedia-goes-dark-protest-sopa-media-offer-support-154353847.html (accessed 20 April 2012).

efforts to combat or suppress contrarian ideologies. For example, China has reportedly hired propagandists, known as the Fifty Cent Party, to patrol chat rooms and online forums. They are paid to post information favorable to the government and castigate anything they find objectionable.[22]

In addition to propaganda, controls in the *Access Contested* phase are characterized by more sophisticated and proactive technical capabilities. Rather than simple blocking and filtering, governments are engaging in denial of service attacks, malware distribution, Trojan horse emplacement, identity forgery and offline harassment.[23] Many of these tools even allow a government to attack content outside its own borders. Even when a state cannot force a site to take down objectionable material through direct legal action, it still has offensive, technical options to achieve similar ends.

Deibert and Rohozinski describe the techniques used in the modern phase as *third-generation tools*, and provide the following overview of their characteristics:

> Unlike the first two generations of content controls, third-generation controls take a highly sophisticated, multidimensional approach to enhancing state control over national cyberspace and building capabilities *for competing in information space* with potential adversaries and competitors. The key characteristic of third-generation controls is that the focus is less on denying access than successfully *competing* with potential threats through effective counterinformation campaigns that overwhelm, discredit, or demoralize opponents. Third-generation controls also focus on the active use of surveillance and data

[22] Deibert, Palfrey, Rohozinski and Zittrain, "Access Contested," 12-13.
[23] Hal Roberts, Ethan Zuckerman, and John Palfrey, "Interconnected Contests," *Access Contested: Security, Identity, and Resistance in Asian Cyberspace Information Revolution and Global Politics*, Ronald Deibert et al., eds. (Cambridge, MA: The MIT Press, 2012), 135.

> mining as means to confuse and entrap opponents.[24] [emphasis in original]

How is Information Regulated in Cyberspace?

For most people, cyberspace censorship typically equates to the technical means for controlling information, such as firewalls or content filters. While technological methods are the predominant means of censorship, there are many other constructs for regulating information. As Zittrain and Palfrey describe, "When states decide to filter the Internet, the approach generally involves establishing a phalanx of laws and technical measures to block their citizens from accessing or publishing information online."[25] Lessig goes beyond legal and technical methods by identifying four modalities that constrain behavior on the Internet—*the law, social norms, the market,* and *architecture.*[26] The law regulates by shaping behavior, often through threat of prosecution for violations. Societal norms also regulate online behavior by establishing either a positive recognition or a stigma from one's peers toward certain actions. The market regulates behavior through pricing structures, scarcity, barriers to entry and other economic factors. Finally, the technical architecture of cyberspace, its software and hardware, provide explicit controls on what kinds of behavior are possible.[27] Each of these four modalities will be examined in detail so that the reader can see the full range of ways that regulation can occur.

Legal Regulation

Zittrain and Palfrey describe five levels of legal regulation that states employ to constrain online behavior.[28] The first level is to enact content restrictions aimed at prohibiting citizens from publishing or accessing certain types of information online. These laws form the legal

[24] Deibert and Rohozinski, "Control and Subversion in Russian Cyberspace," 27.
[25] Zittrain and Palfrey, "Internet Filtering," 32.
[26] Lessig, *Code: Version 2.0*, 123.
[27] Lessig, *Code: Version 2.0*, 124.
[28] Zittrain and Palfrey, "Internet Filtering," 32-33.

basis for implementing technical censorship mechanisms and define the types of content to be filtered.

The second form of legal control is establishing licensing requirements for intermediaries, such as ISPs or social media websites, to carry out logging, filtering or surveillance of user activity. Licenses can also stipulate the permissibility of different types of content. Licenses provide authorities with a tool for exerting control over private service providers. If companies wish to operate and generate revenue in the sovereign territory of the host government, then they must comply with the requirements of the license or risk being shut down.

The third method is to make intermediaries liable for activity that crosses their infrastructures. These laws make no distinction between those who generate the content and those who act as a mere conduit for it. This method induces a form of "self-discipline"[29] into the system by forcing providers to police the content that either flows across or resides within their services. By enacting intermediary liability laws, the government effectively distributes the burden of censorship and surveillance to the private sector.

Fourth, states can enact registration requirements to gather data about citizens who access the Internet. The laws can require ISPs, websites, Internet cafes and other content access points to ensure they know the physical identify of their users. Users may be required to present state-issued identification codes before being allowed to access Internet services.[30] Registration requirements help establish a link between an online persona and a physical person. In doing so, they

[29] Rebecca MacKinnon, "Corporate Accountability in Networked Asia," *Access Contested: Security, Identity, and Resistance in Asian Cyberspace Information Revolution and Global Politics*, Ronald Deibert et al., eds. (Cambridge, MA: The MIT Press, 2012), 197.
[30] Pirongrong Ramasoota, "Internet Politics in Thailand after the 2006 Coup," *Access Contested: Security, Identity, and Resistance in Asian Cyberspace Information Revolution and Global Politics*, Ronald Deibert et al., eds. (Cambridge, MA: The MIT Press, 2012), 98.

enhance a government's ability to attribute illegal behavior to particular individuals and facilitate their prosecution. They also help content providers discern valid users. For example, a requirement to provide valid age information may help content providers restrict access to material that is inappropriate for minors.

Finally, states can establish laws that encourage citizens to be self-policing by heightening the perception, whether true or not, that the government has the capability to monitor what they do online. If citizens believe their actions online are both transparent and non-repudiable then they are less likely to engage in illegal behavior. These laws effectively "put citizens on notice that they should not publish or access content online that violates certain norms and to create a sense that someone might be paying attention to their online activity."[31]

Social Norms

Social norms constrain differently than legal norms. They are not imposed by the organized or centralized actions of a state, but through the many slight, but sometimes forceful, sanctions that members of a community exert on each other.[32] While social norms are sometimes also codified into law to promote additional awareness, deter behavior and legitimize the penalties, many are not. For example, smoking in public may be legal in many places, but it may be received with scorn by those in proximity to the smoker. Social norms also drive conformity in everything from proper hygiene to acceptable manners. Lessig describes how:

> Ordinary life is filled with such commands about how we are to behave. For the ordinarily socialized person, these commands constitute a significant portion of the constraints on individual behavior. Norms, like law, then, are effective rules. What makes norms different is the mechanism and

[31] Zittrain and Palfrey, "Internet Filtering," 36.
[32] Lessig, *Code: Version 2.0*, 340.

> source of their sanction: They are imposed by a community, not a state. But they are similar to law in that, at lease objectively, their constraint is imposed after a violation has occurred.[33]

While laws define the difference between what is legal and illegal, norms define the difference between what is moral or ethical and what is immoral and unethical. In describing a framework for ethical decision-making, Rushworth Kidder articulates a series of questions that people should generally ask before they engage in a particular activity. In addition to asking, "Does this activity break the law?" Kidder contends that three other questions are necessary to determine if a particular behavior violates social or moral norms. The first is, "Does this activity pass the stench test?" This is a gut-level determination dealing with a person's intrinsic moral character. The second question asks "How would you feel if what you are about to do showed up tomorrow morning on the front pages of the nation's newspapers?" This question deals with how publicity can modify behavior. The final question asks, "If I were my mother, would I do this?" Asking the last question forces someone to evaluate their behavior from the perspective of another person—one whom they respect and admire.[34]

The point of examining Kidder's questions is to highlight how social pressures can shape behavior, even if the issue is not covered by a legal restriction. The *Stench Test* is a reflection of personal moral values, which are shaped by society and culture. The *Front Page Test* demonstrates how behavior is tempered depending on whether the matter is kept private or made public. The fact that publicity moderates behavior is a reflection of the power of social pressure. Finally, the *Mom Test* also shows the power of other people's opinion in regulating activity.

---

[33] Lessig, *Code: Version 2.0*, 341.
[34] Rushworth M. Kidder, *How Good People Make Tough Choices Rev Ed: Resolving the Dilemmas of Ethical Living* (Harper Perennial, 2009), 182-183.

Recognition by one's peers for exhibiting laudable behavior can reinforce the positive. Likewise, the social stigma associated with conducting unacceptable behavior can equally inhibit the negative.

Cultural norms are powerful regulators and the effect of cyberspace on developing and applying social pressures is evolving. While the *Stench Test* and *Mom Test* exert their normative pressures in a relatively timeless fashion, cyberspace has changed the character of the *Front Page Test,* which might be better described as the *Facebook* or *YouTube Test* in the modern context. The ability to locate and distribute information on an unprecedented scale combined with the permanence of information in cyberspace often leave little room for forgiveness from someone's past once behavior hits the "front page" of cyberspace.

The concept of cyberspace shaping and being shaped by cultural and social norms is often associated with the term "meme." The term attempts to capture the illusive notion of how culture is propagated through society by discrete packets of information.[35] Memes are generally thought of as particular pieces of information on the Web that becoming extremely popular and broadly distributed. They can be seen by millions of people in an extremely short period of time and once they are, there is no way to erase them. Fortunately, most people's activities do not end up "going viral," but at the same time it is very difficult to predict which ones will. The potentially enormous consequences of socially unacceptable behavior showing up online are exerting a new level of social pressure to regulate behavior in historically unprecedented ways.

Market Regulation

Market regulation is the third modality of regulation described by Lessig. Economic constraints are imposed on actors by the cost of

[35] James Gleick, *The Information: a History, a Theory, a Flood* (New York: Pantheon, 2011), 312-314.

performing a particular action. These constraints exist as a result of the confluence of laws and norms defining what goods and services can be bought and sold, as well as the rules defining property rights and contracts.[36] Modern information technologies have dramatically reduced the costs of communication, allowing for an increasing number of actors to participate in the act of communicating. Historically, communicating across great distances or to a large number of people simultaneously was reserved for a select few with access to the resources to participate in such activity. Today, these services are available to consumers almost for free. While it is not the purpose of this thesis to study the economic forces that facilitated the reduction in cost of these technologies, it is important to realize that these low costs are the primary enabler for a strategy of promoting Internet freedom. The low barrier to accessing modern information technology is the key factor disrupting the monopoly that authoritarian regimes once exerted over information.

Market constraints are one of the most important factors in how all power has been historically wielded by the few over the many. The traditional cost and complexity of attaining and operating military capabilities has precluded such systems from the hands of all but the most powerful. Those unfortunate enough to live in oppressed societies often had little choice but to accept their fate at the hands of a despotic few. Once despots assumed control over sophisticated weaponry, there was little opportunity for resistance. In 1945, George Orwell described the situation as follows:

> I think the following rule would be found generally true: that ages in which the dominant weapon is expensive or difficult to make will tend to be ages of despotism, whereas when the dominant weapon is cheap and simple, the common people have a chance. Thus, for example, tanks, battleships and bombing planes are inherently tyrannical weapons, while

[36] Lessig, *Code: Version 2.0*, 341.

> rifles, muskets, long-bows and hand-grenades are inherently democratic weapons. A complex weapon makes the strong stronger, while a simple weapon — so long as there is no answer to it — gives claws to the weak.[37]

At the time, he was writing about the atomic bomb and his fear that it had the potential to foster even more tyranny, but his words have new meaning in today's context. As opposed to tanks, battleships and bombers, modern information technologies are low cost, generally easy to use and readily available to large segments of the population. In this sense, cyberspace could be considered the ultimate "democratic weapon" as it poses a fundamental challenge to authoritarian regimes by giving "claws to the weak."

Architectural Regulation

The final modality for regulating behavior is architecture. In cyberspace, the architecture is the actual technical implementation of the medium itself—the software and hardware. Cyber theorist Martin Libicki explains how cyberspace consists of three layers: a semantic layer, a syntactic layer and a physical layer. The semantic layer contains information that is meaningful to people and machines. The syntactic layer defines the format of information, regulates its flow and manages its security. It also sets controls and provides instructions for the physical layer. The physical layer is all of the tangible aspects of cyberspace—the routers, servers, smartphones, wires, spectrum, etc.[38] The three previous regulatory modalities reside at the semantic layer of cyberspace because they deal primarily with information content. The architectural level is less concerned with the information content than it is with the transportation mechanisms that enable the flow of that

[37] George Orwell, "You and the Atom Bomb," *Tribune*, 19 October 1945.
David J. Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy For Cyber-Power*, Kindle Ed. (New York: Routledge, 2012), location 2652.
[38] Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York, NY: Cambridge University Press, 2007), 8-9.

content. In Libicki's model, architectural regulation occurs at the syntactic and physical layers.

Modifications to the architecture have been the primary means of government regulation since the dawn of the *Access Denied* phase of censorship in cyberspace. Regulating behavior by controlling the architecture is direct and often measurable. Governments can pass a law and force a change. Specific examples of this will be provided shortly, but before moving into the specifics of how this occurs, it is important to understand a few key aspects of how the four modalities relate to one another and why the architectural layer lends itself to being a particularly lucrative target for government regulators.

The first factor is enforcement. Legal, social and market forces require an external mechanism to administer control. The architecture does not. It is "self-executing" according to Lessig. In one sense, the architecture of cyberspace is analogous to the laws of physics in the real world. It defines what can and cannot be done. As Lessig explains:

> Laws need police, prosecutors, and courts to have an effect; a lock does not. Norms require that individuals take note of nonconforming behavior and respond accordingly; gravity does not. The constraints of architecture are self-executing in a way that the constraints of law, norms, and the market are not. This feature of architecture—self-execution—is extremely important for understanding its role in regulation.[39]

A second factor that differentiates the architectural layer from the previous modalities is that its effects are automatic. The effects of regulation at the architectural layer are immediate and they are not subject to human judgment. If an actor violates the law or an established social norm, they will not feel the consequence of that action until after the act is committed. In some cases, the actor may be able to

[39] Lessig, *Code: Version 2.0*, 342.

skirt the penalty for illegal or objectionable behavior entirely if they are not caught or if law enforcement or society decides not to punish the offender for their actions. Market regulation operates somewhat similarly in that the rules are applied at the time of the action, although market regulation can be subject to more judgment than the cold precision of software and machines. Lessig writes, "Law, norms, and the market are constraints checked by judgment. They are enacted only when some person or group chooses to do so. But once instituted, architectural constraints have their effect until someone stops them."[40]

The final unique aspect of regulation by architecture is the actor's knowledge of the constraints that are being applied. Governments are increasingly learning to use this important quality of cyberspace regulation. As discussed earlier, second-generation controls often include covert mechanisms for either monitoring or blocking the flow of information in cyberspace. Again, Lessig offers important insight into this aspect of cyberspace regulation. To successfully operate, laws, norms and markets must ensure:

> The person constrained [knows] of the constraint. A law that secretly punishes people for offenses they do not know exist would not be effective in regulating the behavior it punishes. But this is not the case with architecture. Architecture can constrain without any subjectivity… Architectural constraints, then, work whether or not the subject knows they are working, while law and norms work only if the subject knows something about them.[41]

Technical Censorship

Given the fundamental technical nature of cyberspace, architectural regulation requires some additional discussion. Before proceeding into how the architecture regulates behavior we must first briefly describe how the Internet was designed to operate. This

[40] Lessig, *Code: Version 2.0*, 343.
[41] Lessig, *Code: Version 2.0*, 344,345.

background on how the Internet is supposed to work will help the reader better understand how censorship and circumvention are actually employed. Censorship efforts, in general, break the communications architecture of the Internet at key points. Circumvention efforts help put those broken points back together.

Fundamentals of Internet Architecture

To understand the underlying mechanisms of the Internet, we turn to the five-layer Internet Protocol Stack defined by James Kurose and Keith Ross shown in Figure 1.[42] It provides more technical insight into the semantic and physical layers of Libicki's model and therefore it is more useful for describing how censorship and circumvention operate.

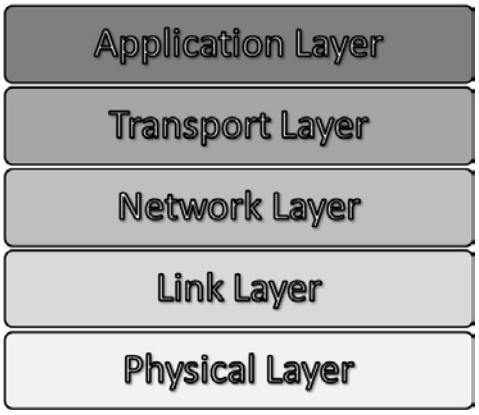

Figure 1. Five-Layer Internet Protocol Stack

Source: James F. Kurose and Keith W. Ross, Computer Networking: a Top-Down Approach, 5th ed. (Boston: Addison Wesley, 2010), 51

The Internet protocol stack represents the architecture of the Internet. Each layer has unique responsibilities for managing and moving data. The bottom of the stack represents all of the physical components of the Internet, such as the routers, servers, cables and spectrum. The *physical layer* contains all of the "real world" components of cyberspace. The layer immediately above the physical layer is the *link*

[42] James F. Kurose and Keith W. Ross, *Computer Networking: a Top-Down Approach*, 5th ed. (Boston: Addison Wesley, 2010), 51.

layer. This layer manages how data moves between physical machines connected by physical links, either wired or wireless. These first two layers are highly localized and generally independent of the data flowing across them. Therefore, most of the blocking and filtering efforts associated with first-generation tools occur at the top three layers. The top layers logically separate the locations of information on the Internet, manage how that information is allowed to move around and how it is presented to either machines or people.

The *network layer* provides the glue that binds the physical components of the Internet to logical IP addresses. It ensures that two physical machines can communicate across the vast array of intermediary networks between them. The network layer works in a similar fashion to the post office. When someone puts an envelope in the mail, all they need to worry about is the address of the recipient and their own return address. The post office figures out how best to route the mail along all of the roads between the two addresses. This information is abstracted away from both the sender and receiver. On the Internet, each user and website is associated with a particular IP address, analogous to how people or businesses are associated with a particular mailing address in the real world. Users and websites exchange information by including both the sender's and receiver's IP addresses within the packets of data they generate. The network layer, like the post office, uses the IP address to choose the path those packets take along the way.

The *transport layer* is responsible for the reliability of the connection between two end-points on the Internet. One of the primary protocols for this purpose is the Transmission Control Protocol (TCP). TCP creates a logical connection between two end-points that exists for the time the two points need to communicate. Having a logical connection facilitates communication by enabling important features

such as error correction, bandwidth throttling or encryption. The transport layer also manages something called "ports." Ports are numeric identifiers that differentiate the type of information flowing across a connection. For example, ports 80 and 443 are generally reserved for communicating webpages, while port 21 is reserved for sending files via the File Transfer Protocol (FTP).

The highest layer of the Internet protocol stack is the *application layer*. This layer is the closest layer to end users and has the most information about the actual content of the data transmitted between end-points on the Internet. For example, the application layer is responsible for defining how e-mail is transmitted between servers using a protocol called Simple Mail Transfer Protocol (SMTP). It also manages how webpages are transmitted through the Hypertext Transport Protocol (HTTP) and how people-friendly domain names, such as "www.google.com," are bound to their corresponding numeric IP addresses through the Domain Name System (DNS).

First-Generation Controls

With this information in mind, we turn to how governments can leverage these protocols to censor the Internet. The first and most basic filtering technique is called *IP header filtering*.[43] This filtering technique targets the network layer. It works by identifying the IP addresses of the sites to be censored and then ensuring that packets will not route to or from the sites. Governments can implement this method either in a centralized or decentralized manner. Implementing the centralized method requires that the government control the intermediary routers between the users and the target websites. If they do, then they can instruct the operators of the routers to drop any packet associated with

[43] Steven J. Murdoch and Ross Anderson, "Tools and Technology of Internet Filtering," *Access Denied: the Practice and Policy of Global Internet Filtering*, Ronald Deibert et al., eds. (Cambridge, MA: The MIT Press, 2008), 59.

blacklisted IP addresses. This method is viable when countries control the ISPs that service users within their borders. The decentralized approach is implemented by mandating that users install client-side filtering software.

The transport layer can also be targeted through *TCP header filtering*. This method is often used in conjunction with IP header filtering to enhance its accuracy.[44] For example, if a state only wishes to block file transfers to and from a particular address, then it can blacklist port 21. This would still allow Internet traffic to flow across port 80.

Another method is called *DNS Tampering* and it targets the application layer of the Internet Protocol Stack. As mentioned earlier, DNS is responsible for binding IP addresses, used by routers to direct packets between end-points, to more familiar and memorable domain names. After a user types a domain name into a web browser their machine queries a DNS server to retrieve the corresponding IP address for that site. DNS tampering works by modifying the information the DNS server would normally return to the client. Governments can filter information by mandating that the DNS servers respond to requests for blacklisted websites with either no response or an alternative response.[45] Without the correct IP address, users will be unable to access the target website.

Each of the previous controls relies on filtering based on the source and destination. These rather crude methods often lead to overblocking since websites can host many different types of content at a single IP address.[46] For example, imagine that a government wished to block access to news stories about a particular protest movement and that information was hosted on the Cable News Network (CNN) website. The

[44] Murdoch and Anderson, "Tools and Technology of Internet Filtering," 59.
[45] Murdoch and Anderson, "Tools and Technology of Internet Filtering," 61.
[46] Zittrain and Palfrey, "Internet Filtering," 46.

above tools only provide an all-or-nothing solution to the problem, since the government would have to block access to all traffic hosted at the site.

To overcome the imprecision of address-based filtering mechanisms, regulators may instead implement *content filtering*. This method is also known as "deep packet inspection," and it permits filtering based on the information itself. The blacklist in this case is not IP addresses or domain names, but specific keywords or phrases that the controller deems objectionable. This form of control allows for more precise filtering than the previous examples. Rather than blocking all of cnn.com, a government could look for keywords related to the protest movement and deny only those transfers that contained the banned words. This form of censorship is costly though, and often difficult to implement. Content filtering requires significant processing capacity to dissect each packet traversing the Internet, detailed knowledge about how to parse multiple communications protocols and the ability to cope with reconstructing content from its packetized form.[47]

The final first-generation control tool covered here is *proxy filtering*. As opposed to dictating that ISPs modify their routing tables or that clients install software, governments might mandate that all users interact with the Internet through proxy servers. This would facilitate inspection and blocking by forcing all traffic to and from the users to flow through centralized focal points.[48] All of the filtering efforts could be concentrated on these choke points allowing for much greater control over which data is and is not permitted to traverse the Internet. Proxies give the regulator the greatest flexibility, allowing blocking by both address and by content.[49] The drawback to proxy filters is often their

[47] Murdoch and Anderson, "Tools and Technology of Internet Filtering," 59-60.
[48] Murdoch and Anderson, "Tools and Technology of Internet Filtering," 61.
[49] Murdoch and Anderson, "Tools and Technology of Internet Filtering," 67.

performance. Since all of the traffic needs to be routed and processed at these central locations, performance tends to suffer because of insufficient communications bandwidth and processing capacity to handle the task.

Second-Generation Controls

With the exception of some rudimentary content filtering, first-generation controls are largely based on blocking addresses. These tools are relatively static and are implemented through automation. Second-generation tools are more sophisticated and dynamic. They are more sophisticated because they incorporate more semantic knowledge into their filtering criteria. There is more judgment and nuance, in addition to automation, associated with these methods. They are adaptive to changing circumstances. They are also increasingly refined and enhanced to prevent the right information at the right time. Second-generation controls can be characterized by three main technical enhancements over their predecessors: surveillance, security and offense.

The first enhancement is surveillance. In addition to simply blocking and filtering, second-generation tools allow governments to log, monitor and track online activity. Surveillance helps add a layer of judgment to cyberspace that the automation of simple blocking lacked. This is because behavior that is not blocked in real time can be sifted through after the fact to deduce who did what and when. This improvement arises from the confluence of lower technology costs and new laws. As described in the section on regulation, many states are implementing registration requirements for Internet users as well as licensing requirements for ISPs and websites. Low-cost access to greater processing, storage and bandwidth combined with these legal reforms are allowing governments to improve their ability to monitor behavior online. If a government publicizes its ability to monitor behavior, this will

discourage its citizens from attempting to access banned content, even if the technical measures for preventing it are inadequate.[50]

The second enhancement is an improvement in security. Governments increasingly have the capacity to conduct online censorship by covert means. For example, first-generation DNS filtering may have returned a link to a website letting the user know that their request was blocked. Second-generation tools may return a link to a replica of the requested page that has been scrubbed free of objectionable content. If the alternative webpage is sufficiently similar to the original, then the user may not know that they are not on the actual site.[51] Additionally, as technology becomes cheaper, the lag time for performing deep packet inspection or running proxy servers is decreasing dramatically. Over time, users may become complacent with these methods because they don't impose any observable decline in performance. As they become acclimatized to surveillance, they will likely tend to forget it even exists, giving a government more freedom to promote its own agenda online.

The third enhancement is the addition of offensive and proactive capabilities to the suite of options available to government regulators. By employing these tools, governments can even block access to content providers that exist outside their legal jurisdiction. An especially important form of this capability is called the *Denial of Service (DoS)* attack.[52] There are many forms of DoS attacks, so only the more common ones will be covered here.

Most DoS attacks work by overwhelming the connection of the target site with more data than it can handle. If a government controls a single resource with sufficient processing power and bandwidth, then it

[50] Murdoch and Anderson, "Tools and Technology of Internet Filtering," 65.
[51] Murdoch and Anderson, "Tools and Technology of Internet Filtering," 69.
[52] Deibert and Rohozinksi, "Control and Subversion in Russian Cyberspace," 26.

can flood the target with enough packets to ensure that no other users can gain access to the site. A more common approach is to distribute the attack so that it originates from multiple machines. Once called to action, their collective output overpowers the target's capacity. When this attack employs multiple computers it is known as a Distributed Denial of Service (DDoS). The attacker may or may not own the machines it uses to carry out the attack. It may infect them with viruses or malware turning them into a "botnet" capable of being controlled remotely.[53] Users who wish to promote this form of attack may even volunteer their machines to support the suppression of the offending site.[54]

The most convenient aspect of a DoS-style attack is that it does not require any form of legal control over the offending site or the intermediate pathways to be implemented. Also, DoS attacks do not have to be in place before the objectionable material goes online. Once a machine with sufficient capability is in place, or a botnet is on call, then the controller only needs to identify the target and commence the interruption. DoS attacks generally do not leave lasting damage, so their effects can be tailored to merely degrade the service for only as long as the attacker needs the service offline. This "just-in-time" form of censorship provides the attacker with a tremendous amount of control. Deibert et al. suggest, "Disabling or attacking critical information assets at key moments in time—during elections or public demonstrations, for example—may be one of the most effective tools for influencing political outcomes in cyberspace."[55] The source of these forms of attack is also relatively easy to deny or hide. Deibert et al. go on to describe that

[53] Ed Skoudis with Tom Liston, *Counter Hack Reloaded: a Step-by-Step Guide to Computer Attacks and Effective Defenses*, 2nd ed. (Upper Saddle River, NJ: Prentice Hall, 2006), 569.
[54] Saki Knafo, "Anonymous And The War Over The Internet," *The Huffington Post*, 30 January 2012. http://www.huffingtonpost.com/2012/01/30/anonymous-internet-war_n_1233977.html (accessed 20 April 2012).
[55] Deibert, Palfrey, Rohozinski and Zittrain, "Access Contested," 13.

"information is disabled at key moments only, thus avoiding charges of Internet censorship and allowing for the perpetrators' plausible denial… just-in-time blocking can be easily passed off as just another technical glitch with the Internet."[56] This supports the ability to employ many second-generation tools covertly.

Third-Generation Controls

Third-generation controls are the most complex and multidimensional of all of the approaches described so far. In addition to all of the technical capabilities described in the previous sections, these tools take aim primarily at the semantic layer of the Internet. The objective of states that employ third-generation tools is to overpower opposing viewpoints in the information sphere. In addition to blocking and filtering information, states are increasingly obstructing perceived threats through propaganda and counter-information campaigns to "overwhelm, discredit, or demoralize opponents."[57] Third-generation controls are also more manpower intensive and tend to be less easily automated.

Third-generation tools employ advanced surveillance and data mining techniques to coax questionable behavior out of the massive amounts of information online. Other methods may include state-sponsored information campaigns that interact directly with dissidents via blogs, social media, e-mail or other information services in cyberspace. They may employ "Internet brigades" to engage, confuse, discredit or harass individuals, post propaganda, distribute disinformation, skew online polling data or make, or threaten to make, personal information available publically. States may also take physical action to disrupt target groups or networks. Their aim is primarily physiological. As Deibert and Rohozinski explain, "The intent of these

[56] Deibert, Palfrey, Rohozinski and Zittrain, "Access Contested," 13.
[57] Deibert and Rohozinski, "Control and Subversion in Russian Cyberspace," 7.

campaigns is to effect cognitive change rather than to deny access to online information or services."[58] Third-generation tools mean that the technical game of cat-and-mouse that was a hallmark of the first two generations of control is now spilling over into a war of ideas for control of the mind rather than simply the medium.

What Can Be Dne to Promote Information Freedom in the Face of These Constraints?

This chapter has examined many methods for regulating behavior online. Not all of them are technical, but the technical methods often provide law makers and those who wish to circumvent the law, with the most direct means of achieving their objectives. The final section of this chapter deals with specific methods for circumventing censorship. The goal is to provide policy makers with an understanding of what options are available to them should they decide it is in the US interest to promote freedom to communicate online in the face of authoritarian laws that aim to prevent those very freedoms. It looks at each of the generation of censorship tools presented throughout this chapter and explains methods for how they can be bypassed.

Circumventing First-Generation Controls

First-generation censorship tools aim to blacklist specific websites, and potentially keywords or phrases, primarily through static, technical means. Developing and maintaining blacklists are the primary weaknesses of first-generation controls. The sheer volume of websites on the Internet makes this an exceptionally daunting task even if no active circumvention techniques were available. As of February 2012, Worldwidewebsize.com estimates there are 7.92 billion pages on the

[58] Deibert and Rohozinski, "Control and Subversion in Russian Cyberspace," 28.

Internet.[59] Steven Murdoch and Ross Anderson describe the problem facing those building blacklists as follows:

> Building this list is a considerable challenge and a common weakness in deployed systems. Not only does the huge number of Web sites make building a comprehensive list of prohibited content difficult, but as content moves and websites change their IP addresses, keeping this list up-to-date requires a lot of effort. Moreover, if the operator of the site wishes to interfere with the blocking, the site could be moved more rapidly than it would be otherwise.[60]

Despite the inherent difficulties of maintaining and executing blacklists in aggregate, some content providers may still be picked among the unlucky few to be targeted for censorship. These providers still have options. The most direct way to overcome IP filtering is to simply change their IP address. This solution is likely to be temporary since once the blacklist managers find out about the change, they can update the list. This option might not be acceptable to some major providers whose IP addresses are well established. A provider, such as Google or Yahoo!, simply cannot modify their own addresses without significant repercussions to the existing infrastructure of the Internet. An alternative solution is to provide users with a proxy server hosted at an IP address that is not blacklisted. Users communicate through the proxy, which may be outside of the jurisdiction or control of the censoring state. The IP filters will only see data flowing between the user and the proxy and without additional checks they will not recognize that the user is actually communicating with a forbidden site. Proxy solutions are likely to be temporary since the controlling government may realize what is happening and add the address of the proxy server to its blacklist. To this end, circumvention providers may have to routinely update the address of the proxy servers and find ways to communicate

[59] http://www.worldwidewebsize.com/ (accessed 23 February 2012).
[60] Murdoch and Anderson, "Tools and Technology of Internet Filtering," 59.

the new address to users. Search engines, online listings or e-mail subscription services are useful tools for providing up-to-date information about available proxy servers.[61]

TCP header filters can be circumvented in a similar fashion by manipulating the choice of ports that processes use to communicate information. There is no technical reason why a website could not host its content on any other port besides port 80. Port 80 is reserved for website related traffic by convention, but users could bypass filtering on port 80 by pre-arranging a different port number and updating the settings in the client's browser.

DNS tampering is also relatively easily circumvented since machines only need to know IP addresses to communicate. Once a domain name is resolved to its IP address the domain name is no longer needed to create a data connection. Users can avoid DNS tampering by knowing the IP address ahead of time or by obtaining it from an alternative source. Local DNS caches also provide the user with a means of avoiding this form of filtering assuming the local DNS cache already knows the association between the domain name and the IP address of the target site. Also, if the user has control of their local settings, then an alternative, trusted DNS service could be selected to resolve the target site accurately.

Content filtering is more difficult to overcome since it deals directly with the same words and phrases that are likely to be important to the users. However, there are still many ways to avoid keyword blocking. One creative method is to employ "leet speak." Leet speak is essentially an alphabetic substitution mechanism that replaces the original letters with visually similar symbols. For example, the average person would

[61] Radio Free Asia, "Getting Around Internet Blockage" http://www.rfa.org/english/about/help/web_access.html (accessed 13 March 2012).

recognize the word "HELLO" even if it were presented as "H3LL0." A machine that wasn't programed with this form of the greeting in its blacklist would likely allow the content to pass through its filter. A stronger form of protecting against keyword filtering is to use cryptographically secure encryption algorithms, such as Pretty Good Privacy (PGP), Secure/Multipurpose Internet Mail (S/MIME) or Secure Shell (SSH).[62] Encryption will be discussed in more detail below in the section covering circumvention of second-generation controls.

Proxy filtering is essentially a centralized way of implementing any of the first-generation censorship tools. Therefore, it can often be overcome with similar techniques. If the client machines are locked down such that user-supplied software cannot be installed or connection settings changed, then the user may be able to bypass the proxy by choosing an entirely different form of communication. For example, the cable Internet provider may be required to lock down the choices available to users, but the user may be able to exchange information through a dial-up connection instead. That connection may even only be available via an international number or via a satellite phone, but the capability exists if there is sufficient will to bypass the censorship.

A significant difficulty facing the circumventor is the need to educate users on the techniques. Much of the architecture of cyberspace is a proverbial "black box" to most of its users. For example, trying to explain how to reconfigure a browser so that it points to a different DNS server may be a particularly daunting task to the uninitiated. A second problem is that governments often censor sites that host circumvention tools or provide information about circumvention techniques. This means that circumventors will have to find alternative methods of distribution for both the tools and their configuration details. A third

[62] Skoudis, *Counter Hack Reloaded*, 76.

problem is that attempting to find circumvention capabilities puts the people who look for them at risk since there may be little justification for searching for circumvention techniques outside of trying to skirt the law. US policy makers who wish to support circumvention technologies in oppressed nations will have to overcome these challenges.

Circumventing Second-Generation Controls

The methods for overcoming second-generation controls are less direct than those for overcoming first-generation controls. In addition to the technical methods, second-generation controls employ legal and social pressures to curtail behavior. This makes circumvention more difficult. If laws are passed that make certain behavior illegal, then citizens will have to feel sufficiently protected by the circumvention measures before they are likely to engage in the activity. Being denied access to a particular piece of information is one thing, but the threat of financial penalties or jail time is quite another. Overcoming second-generation tools requires a deeper commitment on behalf of the actor and therefore the benefits of the action will have to outweigh the risks. The promise of freedom will have to be real and the benefits of achieving success will have to stand up in the face of the consequences of failure.

Emphasis on identification and surveillance are hallmarks of second-generation controls. Second-generation techniques are more than simply controlling the supply of information; they also aim to control the demand through fear of reprisal. This means that in addition to the methods for circumventing first-generation controls, users who wish to withhold their identity or keep their communications secure will have to enhance their ability to use anonymizing services and cryptography.

One of the more common tools for providing anonymity online is called The Onion Router (Tor). Tor is a community-based anonymizing

service that allows users to both protect their identity as well as bypass many forms of filtering and surveillance. Rather than transfer data through typical routing paths, information requested through Tor is routed through servers hosted by volunteers. At the simplest level, Tor is a proxy server capable of circumventing many IP blacklist filters because the addresses associated with the Tor network fluctuate making it difficult to effectively blacklist. More importantly though, Tor intentionally passes communications through multiple, random nodes between the user and the target site and modifies the source IP addresses along the way to scramble the identity of the originator. In addition, it encrypts the traffic between Tor nodes to ensure that even the volunteers cannot see the data flowing through their systems. All of these features of the Tor network make it extremely difficult to trace communications and discover the identity of the communicator. The Tor's website states, "Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location."[63]

Secure communication is another critical aspect of circumventing second-generation controls. In this context, for communication to be secure it must have at least the following three qualities: *confidentiality*, *end-point authentication*, and *message integrity.*[64] Confidentiality involves ensuring that only the intended sender and receiver are able to access the contents of the data. It is generally achieved by encrypting the data using a cryptographically secure algorithm and a key available only to the sender and receiver.

[63] Tor, "Anonymity Online," https://www.torproject.org/ (accessed 23 February 2012).
[64] Kurose, *Computer Networking*, 688-689.

While their IP addresses can be masked by anonymizing services like Tor and the communication path can be secured with encryption, users must still be cautious that recipients are actually who they claim to be. This is where end-point authentication comes in. It refers to the ability of the sender and receiver to verify that the person or machine on the other end is indeed the intended recipient of the data. This is especially important and often especially difficult online. Much of the end-point authentication on the Internet is done through digital certificates that have been cryptographically signed by both by the content provider and by trusted third parties. For most types of Internet traffic, the cryptographic signatures only apply to the server and not the client. This leaves the client in a position to maintain anonymity while still ensuring the identity of the server.

The mathematical details of that signature are beyond the scope of this thesis, but from a functionality perspective, it suffices to say that these signatures provide a secure method of positively identifying end-points on the Internet. For example, validated websites that use end-point authentication will often be accompanied by a graphic of a padlock symbol displayed in the user's web browser. When users see the padlock, they know the communication path is encrypted and that the site on the other end is not a forgery trying to harvest sensitive information.

Finally, the sender and receiver should be able to tell if the data has been manipulated. This property of secure communication is known as *message integrity.* Again, digital certificates provide a means of ensuring the integrity of the end-points. If users get notifications that these certificates have errors, then they should be extremely cautious before communicating. Cryptographic hashes also provide a means to validate that information has not been tampered with. Hashes are like fingerprints for digital data. For example, users can run a file through a

hashing algorithm and verify the output against the known value associated with a valid version of the file. Any discrepancies between the two values indicate that the file has been modified in some fashion. In the worst case scenario, any signs of unintended modification could point to the presence of viruses, malware or Trojan horses that could undermine the security of the communication.

Second-generation controls emphasize identification and surveillance to coerce a populace to conform to standards deemed acceptable by the regime. Therefore, second-generation circumvention must place equal or even more emphasis on combating the pressures of that coercion through secure communication and anonymity services. Combining these techniques helps facilitate information freedom by making information exchange trusted, confidential and anonymous. These factors are often critical for helping users overcome the fear of punishment for engaging in behavior their government deems objectionable.

Circumventing Third-Generation Controls

Most of the techniques employed to both censor and circumvent information in the first and second generations dealt with the physical and syntactic layers of cyberspace. Censorship efforts involved either eliminating the supply of information or monitoring user activity and threating reprisal for objectionable behavior. Circumvention efforts aimed to reintroduce the supply of information and lower the threat of reprisal for accessing or exchanging that information. By contrast, third-generation censorship and circumvention are focused on the message itself. They operate at the semantic layer of cyberspace, where the modern battle over information is being fought. It is not simply a fight to block or provide information, but a battle for cognitive influence.

This makes third-generation circumvention more difficult. Not only do circumventors need to provide means to access the information, but they must also craft the information in ways that influence the content consumers. The information is no longer exogenous to the implementation characteristics of censorship and circumvention. In the third generation, the information is the most critical component of the process. Circumvention involves winning over the "hearts and minds" of the population rather than simply defeating the control mechanisms of the regime. It is less technical and more psychological, requiring a different skill set for its practitioners.

Circumventing third-generation controls requires a team approach to merge the efforts of both technical and informational experts. The technical experts still provide the basis for circumventing first- and second-generation controls that persist in the third generation. They also help tailor the information campaign in the context of modern technology-focused media and assist the information experts in placing the message in cyberspace in ways that maximize its effect. The second half of the team is responsible for content generation. These third-generation members must be capable of articulating the strategic message while discrediting the message of the controlling regime. The most effective message will be factual, authentic and capable of standing up to the regime's counter-information efforts.

The fight against global terrorism and terrorist organizations provides interesting parallels and examples of similar ideological struggles. Terrorist organizations, such as Al Qaeda, have been extremely successful in using modern information technology to promulgate their message. They leverage the Internet and mass media to ensure their "propaganda by deed" spreads nearly instantaneously around the globe. In addition to their actions, they radicalize recruits, solicit for funding, perform tactical planning and execute missions

online.[65] As counter-terrorism efforts evolve they increasingly resemble the *Access Contested* phase of cyberspace.

As General John Abizaid, former commander of the United States Central Command, said, "You can destroy the people in Al Qaeda, but you can't destroy the idea of Al Qaeda. The idea of Al Qaeda needs to be attacked."[66] Just as information controls in the first two generations attacked the supply of information, early counter-terrorism efforts focused primarily on the supply of terrorists. Counter-terrorism strategies and third-generation circumvention methods are unified by their shift to curtailing demand for a particular ideology. For example, terrorist actions often undermine their objectives. International strategic communication efforts to invalidate terrorist ideology seized on terrorist attacks that killed civilians or committed other atrocities. According to Mark Pfeifle, the deputy national security adviser for strategic communications and global outreach:

> The main goal was to create a constant drumbeat of anti-Al Qaeda information that was factual, directly quoted, and heavily sourced with credible, direct links to verify. We put a priority on using photos and video to tell the story with the theme throughout being Al Qaeda and its supporters are killing, maiming innocent Muslims, including women and children.[67]

The United States government is far from the only entity challenging distorted ideology. Other governments are also engaging the contested information space. For example, both the Netherlands and Pakistan have employed counter-recruiting strategies tailored to ensure disaffected youths are given alternatives to radicalization. Saudi Arabia has also enlisted hundreds of Islamic scholars to fight terrorist influence

[65] Eric Schmitt and Thom Shanker, *Counterstrike: the Untold Story of America's Secret Campaign Against Al Qaeda* (New York: Times Books, 2011), 133.
[66] Schmitt and Shanker, *Counterstrike,* 160.
[67] Schmitt and Shanker, *Counterstrike*, 167.

online by challenging extremist interpretations of the Koran in social media.[68] There is also a host of grass roots organizations opposed to combating violent extremism such as the Alliance of Youth Movements, Sisters Against Violent Extremism, Global Survivors Network and the Quilliam Foundation.[69]

Terrorism is far from the only repressive ideology that leaders must deal with in the *Access Contested* phase of cyberspace, but it highlights many characteristics of the prevailing trend in censorship and circumvention. The modern era is no longer simply a matter of taking direct action against the supply of data. Access to communication tools is too ubiquitous to truly control the flow of information. The new battle is about the message. It is about the demand for information. It is about influence. Participation in this fight is no longer limited to governments, although they still play an extremely important role. Now, however, businesses, non-government organizations and individuals all compete on a nearly even playing field. Circumvention at this stage requires a more long-term, indirect methodology centered on persuading the target audience to adopt a particular set of beliefs.

Conclusion

As this chapter has highlighted, censorship in cyberspace is much more than a technical endeavor. While technology has indeed played a key role in the history of Internet censorship, other factors, such as laws, social pressure and market forces also contribute to regulating behavior. As Morozov points out, "Most of the firewalls to be destroyed are social and political rather than technological in nature. The problem is that technologists who have been designing tools to break technological rather than political firewalls… are the ones who control the public

[68] Schmitt and Shanker, *Counterstrike*, 162.
[69] Schmitt and Shanker, *Counterstrike*, 170.

conversation"[70] Leaders who wish to circumvent the control mechanisms of authoritarian regimes must take all of these factors into account and plan for them accordingly.

Ultimately, for circumvention to be successful there must be a desire to access, publish or transmit the censored information. Put another way, circumvention will only work if there is a mismatch between legal regulation and societal norms. Specifically, the most just implementation of circumvention technologies will occur when a government is oppressing its population. Circumvention cannot be expected to lead to any useful result if the society has determined that its current form of government is the best one for its particular circumstances. Lessig examines this phenomenon from the perspective of free speech. If freedom of speech is shunned by society, then circumventing government attempts to enact a legal framework based on the same principles of suppression of speech are unlikely to yield any fruit. He provides the following analysis of the subject:

> [A] constitutional account of free speech that thought only of government would be radically incomplete. Two societies could have the same "First Amendment"—the same protections against government's wrath—but if within one dissenters are tolerated while in the other they are shunned, the two societies would be very different free-speech societies. More than government constrains speech, and more than government protects it. A complete account of this—and any—right must consider the full range of burdens and protections.[71]

[70] Evgeny Morozov, *The Net Delusion: the Dark Side of Internet Freedom* (New York: PublicAffairs, 2011), 111-112.
[71] Lessig, *Code: Version 2.0*, 233.

Chapter 2

Cyberspace Influence

It is my view that, at least so long as political repression remains a central feature of too many world governments, free governments should recognize a protected legal right to these technologies.

– Lawrence Lessig

We're trained to do D's: devastate, destroy, defeat, defend. Now we're asked to go into places and do R's—recover, reform, rebuild, renew. To do that, we'd have to know how to blow apart things in just the right way so we can later come in and rebuild them. Tell me, how the hell are we gonna do that?

– unnamed Air Force General (quoted in Atran)

In addition to architecting a framework for governing the United States, the Constitution is a *de facto* statement of American values. By specifying legal protections, particularly in the Bill of Rights, the Founding Fathers, and the subsequent congresses that contributed important amendments, made proclamations about what America holds dear. This thesis focuses on the First Amendment protection of free speech because cyberspace has profoundly changed the character of how people exercise that freedom. Yet, while the character has changed, the nature of free speech has not. As America's Founding Fathers recognized, people empowered with the ability to express and inform their own opinions will be more capable of creating a better and more legitimate form of government. Also, as Kant alluded to, there is reason to believe that governments based on democratic ideals are more likely to remain at peace with one another. Therefore, by holding freedom of speech as a fundamental value, the United States can more effectively govern domestically and by promoting that value internationally, the United States can encourage a more peaceful and prosperous global order.

In terms of political strategy, one could consider values as *ends*. As Harry Yarger explains:

> National values are expressions of collective visions about what people believe represents a good life. They are an ideal statement of a desired and esteemed social reality: beliefs about idealized ways of living and acting. As such they serve as a means of determining and judging actual behavior based on beliefs about what society and its members should be achieving. Society's values when applied to specific issues or circumstances in the international environment help define national interests, the end-state desired.[1]

The policies of US agencies define the *ways* and *means* of achieving those ends. The *ways* and *means* of policy aim to affect the behavior of both domestic and international actors so that they conform more closely to American values. Policy is best understood as guidance in regard to the end-state sought by strategy. In this sense, policy is a statement of how the US intends to influence others to promote American interests.[2]

Through this lens, this chapter examines US policy governing cyberspace and how it fosters the value of promoting freedom of speech in the Internet Age. As we will see, different agencies within the government approach the problem of influencing the behavior of international actors differently. Each has different ways and means, and therefore each uses a different approach to achieve the common objective of promoting American interest.

Values

The Declaration of Independence and the Constitution of the United States have already been covered as expressions of American values, but there are other important documents and declarations as well. Of particular relevance to Internet freedoms are passages contained

[1] Harry R. Yarger, *Strategy and the National Security Professional: Strategic Thinking and Strategy Formulation in the 21st Century* (Westport, CT: Praeger, 2008), 86.
[2] Yarger, *Strategy and the National Security Professional*, 4.

in two international sources and three domestic sources. The international documents are the *Universal Declaration of Human Rights* and the *International Covenant on Civil and Political Rights*. The domestic sources are the *National Security Strategy*, a recent declaration by the US Secretary of State Hillary Clinton on Internet freedoms and the *International Strategy for Cyberspace*.

In the aftermath of World War II, nations sought ways to find common ground between all peoples of the world. To do so, the fledgling United Nations (UN) established the Commission on Human Rights in 1946 to draft an international bill of rights. The task was assigned to a formal drafting committee from nine states selected with regard to geographical, political, cultural and religious diversity. Among the original drafters was Eleanor Roosevelt, the widow of former US President Franklin D. Roosevelt.[3] The *Universal Declaration of Human Rights* (UDHR) was adopted by the UN General Assembly in 1948. According to the UN website:

> The Universal Declaration of Human Rights is generally agreed to be the foundation of international human rights law… It represents the universal recognition that basic rights and fundamental freedoms are inherent to all human beings, inalienable and equally applicable to everyone, and that every one of us is born free and equal in dignity and rights… The UDHR has inspired more than 80 international human rights treaties and declarations, a great number of regional human rights conventions, domestic human rights bills, and constitutional provisions, which together constitute a comprehensive legally binding system for the promotion and protection of human rights.[4]

[3] United Nations, "History of the Document," http://www.un.org/en/documents/udhr/history.shtml (accessed 19 March 2012).
United Nations, "The Drafters Of The Universal Declaration Of Human Rights," http://www.un.org/en/documents/udhr/drafters.shtml (accessed 19 March 2012).
[4] United Nations, "The Foundation Of International Human Rights Law," http://www.un.org/en/documents/udhr/hr_law.shtml (accessed 19 March 2012).

Article 19 of the UDHR is especially relevant to Internet freedom. It states, "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[5] The framers of the UDHR recognized that freedom of expression should not be denied without a legitimate reason. At a time when the world was healing from the largest war in history and bracing itself for a new stalemate between the East and West, codifying universal principles was a colossal task and its achievement reflects the credibility of the principles it articulates. According to Mary Rundle and Malcolm Birdling, "The inclusion of a broad, unfettered guarantee of freedom of expression in such a weighty document is a clear statement of international acknowledgement of such a right."[6]

It took almost 30 years for the principles of the UDHR to receive a more binding legal status. Together with the UDHR, two subsequent Covenants—the *International Covenant on Civil and Political Rights* (ICCPR), and the *International Covenant on Economic, Social and Cultural Rights* (ICESCR)—make up the *International Bill of Human Rights*. These Covenants entered into force in 1976 and are binding on states that have ratified them.[7] The ICCPR is the more relevant to Internet Freedoms. To date, over 170 nations have become party to its provisions, including the United States.[8] Article 19 of the ICCPR is the most pertinent article with respect to Internet freedom. It states the following:

---

[5] United Nations, "The Universal Declaration of Human Rights," http://www.un.org/en/documents/udhr/index.shtml. (accessed 19 March 2012).
[6] Mary Rundle and Malcolm Birdling, "Filtering and the International System," *Access Denied: the Practice and Policy of Global Internet Filtering*, Jonathan L. Zittrain et al., eds. (Cambridge, MA: The MIT Press, 2008), 78.
[7] United Nations, "The Foundation Of International Human Rights Law," http://www.un.org/en/documents/udhr/hr_law.shtml (accessed 19 March 2012).
[8] United Nations, "Treaty Collection," http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en (accessed 19 March 2012).

> 1. Everyone shall have the right to hold opinions without interference.
>
> 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
>
> 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order, or of public health or morals.[9]

The Article restates the universality of the inherent right for individuals to express themselves freely and to "seek, receive or impart information of all kinds" through all types of media. Both the UDHR and the ICCPR establish freedom of expression as a key value applicable to all of humanity. Yet, the Article also acknowledges that the exercise of those rights carries with it "special duties and responsibilities" that may be subject to certain restrictions. Nations that are signatories to the ICCPR may engage in censorship and information filtering provided that they establish their practices in law and that the laws are necessary. For such laws to be deemed necessary, they must meet one of two criteria: 1) if access to or publication of a particular kind of information would disrespect the rights or reputations of others; or 2) if the information must be protected for national security or reasons of public order, health or morals.

As a charter member of the UDHR drafting committee, a key vote in its adoption by the General Assembly, and a signatory and ratifier of the ICCPR, the US is intimately associated with the values proclaimed in

[9] The Office of the United Nations High Commissioner For Human Rights, "International Covenant on Civil and Political Rights," http://www2.ohchr.org/english/law/ccpr.htm#art19 (accessed 19 March 2012).

these international sources. The fact that these sources reflect an international consensus on the universal right to expression and access to information is also important to the future of Internet freedoms. Not only are the UDHR and ICCPR a reflection of America's intrinsic values, America's presence alongside other nations in professing them reflects a deeper sense of international commitment to these values. The UDHR and the ICCPR form a platform for cooperation among nations toward this common good.

More recently, the United States has also upheld freedom of expression in domestic sources. The 2010 *National Security Strategy* (NSS) extols the extraordinary potential of cyberspace in promoting information freedom. It also ties this value to a belief that individuals will be able to form a more capable and peaceful democratic government when freedom is allowed to flourish. In the section titled *Marshalling New Technologies and Promoting the Right to Access Information*, the NSS declares the following:

> The emergence of technologies such as the Internet, wireless networks, mobile smart-phones, investigative forensics, satellite and aerial imagery, and distributed remote sensing infrastructure has created powerful new opportunities to advance democracy and human rights. These technologies have fueled people-powered political movements, made it possible to shine a spotlight on human rights abuses nearly instantaneously, and increased avenues for free speech and unrestricted communication around the world. We support the dissemination and use of these technologies to facilitate freedom of expression, expand access to information, increase governmental transparency and accountability, and counter restrictions on their use.[10]

Another key component of the 2010 NSS is contained in the section titled *Promote Democracy and Human Rights Abroad*. This section is reminiscent of Kant and it reflects America's belief in

[10] White House, "National Security Strategy of the United States of America," May 2010, 39.

Democratic Peace Theory since it is in America's interest that other nations adopt the values of freedom and democracy. Nations that do so will be "more just, peaceful and legitimate." The section declares the following:

> The United States supports the expansion of democracy and human rights abroad because governments that respect these values are more just, peaceful, and legitimate. We also do so because their success abroad fosters an environment that supports America's national interests. Political systems that protect universal rights are ultimately more stable, successful, and secure.[11]

Together, these two portions of the NSS signify important American values. By expanding access to information technologies and fostering a global, political climate favorable to freedom of expression and human rights, the United States can help promote a more peaceful and prosperous world order. The NSS also reflects the values held by the UDHR and the ICCPR and encourages American leaders to take action to uphold these values at home and abroad.

Another statement of freedom of expression as an American value comes from the Department of State. On 21 January 2010, speaking to an audience at the Newseum in Washington D.C., Secretary of State Hillary Clinton delivered a seminal speech outlining the importance of Internet freedoms. Her speech expanded on President Roosevelt's "Four Freedoms" speech delivered on 6 January 1941, and also highlighted the work done by Mrs. Roosevelt when she helped draft the UDHR. In 1941, the President looked forward to a world founded upon four essential human freedoms: *freedom of speech and expression, freedom of worship,*

[11] White House. "National Security Strategy of the United States of America," 37.

freedom from want, and *freedom from fear.*[12] Secretary Clinton added a fifth freedom to the list: *freedom to connect.*[13] Her speech was a formal acknowledgement of the prominent role the Internet would play in US foreign affairs for the foreseeable future.

Secretary Clinton made several key statements in the address that expressed US commitment to this value. She stated, "The Internet is a network that magnifies the power and potential of all others. And that's why we believe it's critical that its users are assured certain basic freedoms. Freedom of expression is first among them." She also warned authoritarian regimes about the intrinsic dangers of denying this right. "Countries that restrict free access to information or violate the basic rights of Internet users risk walling themselves off from the progress of the next century." Finally, she restated America's belief that cyberspace can help promote the ideal articulated in the NSS for all nations to be more just, peaceful and legitimate when she stated, "Even in authoritarian countries, information networks are helping people discover new facts and making governments more accountable."[14]

Secretary Clinton's address on Internet freedoms embodies the importance of promoting freedom of expression as a fundamental value applicable to all of humanity. It also highlights how modern information technologies have created the most favorable environment in history for promulgating such a value. As Secretary Clinton stated, "Now, in many respects, information has never been so free. There are more ways to spread more ideas to more people than at any moment in history."[15]

---

[12] Franklin Roosevelt, "Transcript of President Franklin Roosevelt's Annual Message (Four Freedoms) to Congress (1941)," 6 January 1941, http://www.ourdocuments.gov/doc.php?flash=true&doc=70&page=transcript (accessed 20 March 2012).
[13] Hillary Clinton, "Remarks on Internet Freedom," 21 January 2010, http://www.state.gov/secretary/rm/2010/01/135519.htm (accessed 20 March 2012).
[14] Hillary Clinton, "Remarks on Internet Freedom."
[15] Hillary Clinton, "Remarks on Internet Freedom."

President Obama also affirmed America's commitment to the principle of Internet freedom in the 2011 *International Strategy for Cyberspace*. This document seeks to unify America's approach to cyberspace by engaging with international partners toward promoting shared values and achieving common objectives. In it, the president established the following four threads aimed at promoting fundamental freedoms in a safe and secure manner through cyberspace:

> 1. Support civil society actors in achieving reliable, secure and safe platforms for freedoms of expression and association.
>
> 2. Collaborate with civil society and nongovernment organizations to establish safeguards protecting their Internet activity from unlawful digital intrusion.
>
> 3. Encourage international cooperation for effective commercial data privacy protections.
>
> 4. Ensure the end-to-end interoperability of an Internet accessible to all.[16]

The preceding section clearly demonstrated America's belief that information freedom is a fundamental value and that modern information technologies are crucial facilitators of that freedom. The United States sees this value as applying not only to its own citizens, but to all of humanity. In addition to viewing it as an inherent right, America believes that promoting this right globally is in the best interest of all nations because nations that are free, open and democratic are more likely to foster peace and prosperity. Therefore, America must take steps to influence others around the globe to also act according to this value.

Influence

Before examining the mechanisms by which US policy influences, we must first examine the theory of influence itself. For that we turn to

[16] White House, "International Strategy for Cyberspace," May 2011, 23-24.

B. F. Skinner's theory of *operant conditioning*, which describes how behavior can be either reinforced or reduced by an external stimulus. According to Skinner, the history of reinforcement and punishment either increases or decreases the likelihood of an agent exhibiting a particular behavior in the future. Therefore, by deliberately manipulating the consequences associated with a particular behavior, Skinner theorized that agent behavior could be shaped in deterministic ways.[17]

There are two kinds of reinforcement: positive and negative. *Positive reinforcement* consists of presenting a stimulus that strengthens the behavior upon which it is made contingent. An example of positive reinforcement is giving candy to a child after the child performs some action. *Negative reinforcement* consists of withdrawing something unpleasant to strengthen behavior. Shutting off a bright light or eliminating a loud noise as a result of some behavior are examples of negative reinforcement. Both positive and negative reinforcement can be used to promote behavior. In this sense, they are both rewards.[18] Contrary to popular perception, negative reinforcement is different from punishment, which we turn to next.

Punishment aims to shape behavior in exactly the opposite way. *Positive punishment* works by presenting an adverse consequence aimed at decreasing the behavior it follows. Putting someone in jail after a crime is an example of a positive punishment. On the other hand, *negative punishment* reduces the likelihood of a particular behavior by withdrawing something of value from the agent. For example, a parent may take a toy away from a child as a form of punishment following

[17] B.F. Skinner, *Science And Human Behavior* (Free Press, 1965), 65.
[18] Skinner, *Science And Human Behavior*, 73.

objectionable behavior. These four influence techniques are summarized in Figure 2.[19]

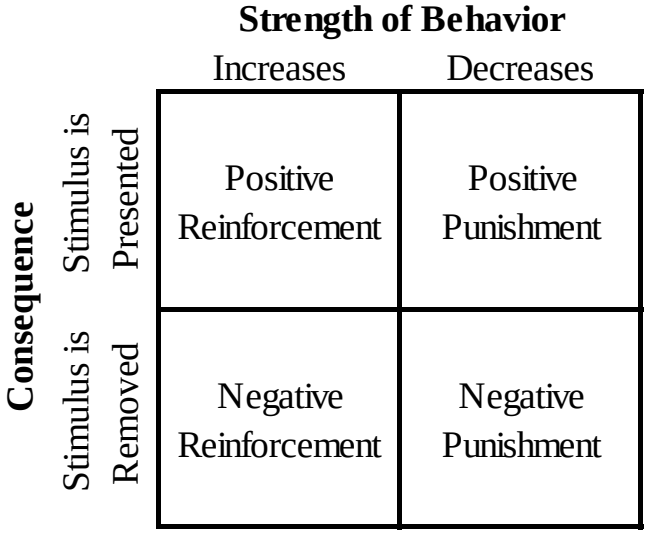

Figure 2. Quadrant of Influence

Source: Paul Chance, Learning and Behavior: Active Learning Edition, 6th ed. (Belmont, CA: Wadsworth Publishing, 2009), 209.

Figure 2 presents a framework that can be used to help understand how the policies of various US government agencies contribute to US influence. The rest of this chapter is devoted to this task, and as we shall see, different agencies approach influence in and through cyberspace in dramatically different ways.

Policy

Influence can only be achieved through appropriate and clear communications and signaling, yet the policies of various US agencies are conflicted in their approach to cyberspace. In some ways, the policy contradictions are understandable since using cyberspace has both positive and negative consequences. On one hand, modern information technologies facilitate democratic forms of government, fuel the globalized economy, enhance education and help create a more

[19] Paul Chance, *Learning and Behavior: Active Learning Edition*, 6th ed. (Belmont, CA: Wadsworth Publishing, 2009), 209.

connected society. They promote the values described earlier in ways never before seen in history. On the other hand, as governments, businesses and individuals become more reliant on information technology they potentially expose themselves to new forms of risk. According to Metcalf's Law, the value of a network is proportional to the square of the number of nodes in the network.[20] By this logic, the Internet becomes exponentially more valuable with each additional user. Yet, each new user also becomes a potential new threat to the network. The US is struggling to balance between these opportunities and vulnerabilities in cyberspace.

In conventional conflict, fortifications and armaments serve as powerful deterrents to aggression. Invaders can be kept out, aggression is attributable and violence is largely confined to nation-state actors. As the famous Prussian General Carl von Clausewitz described, defense has historically been the stronger form of war.[21] In this sense, defensive, conventional military forces map to Figure 2's *positive punishment* quadrant of influence because they impose costs on an aggressor. In the physical domains, the costs imposed by the defense often outweigh the potential benefits to be gained by offense. The cost equation associated with traditional forms of warfare help tilt the balance of power in favor of stability.

Offense and defense in cyberspace are different than they are in other domains. Traditional militaries, especially technologically advanced ones, require significant investments of resources and manpower. These high acquisition barriers keep conventional military forces largely in the hands of nation-state actors. Cyberspace activity, however, is characterized by much lower barriers to entry. For example,

[20] Carl Shapiro and Hal R. Varian, *Information Rules: a Strategic Guide to the Network Economy* (Boston, MA: Harvard Business Review Press, 1999), 184.
[21] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret, (Princeton, NJ: Princeton University Press, 1976), 84.

adversaries do not require the resources, or significant periods of time, to procure or acquire the cyber equivalent of jets, tanks or bombs. For little-to-no money and the time it takes to download code, an adversary can launch a sophisticated cyber attack with a relatively small chance of incurring any significant cost on their end. Often, the worst that happens is that the attack is unsuccessful and the aggressor is in no worse position than they were prior to the attack.

Low barriers to entry contribute to a much larger set of actors in cyberspace. These actors range from nation-states to individuals. The large number of actors makes international relations more complex. Attribution is also difficult, not only as a result of the multitude and diversity of actors, but also because of the fundamental nature of cyberspace itself. The 2011 *National Military Strategy* (NMS) summarized these factors when it declared, "The cyber threat is expanded and exacerbated by lack of international norms, difficulties of attribution, low barriers to entry, and the relative ease of developing potent capabilities."[22]

In the age of cyberspace, the cost equation associated with offensive action may no longer favor stability. In an effort to deny the benefits of aggression, organizations and individuals often employ firewalls, virus scanners, intrusion prevention systems, access management and encryption to remove the rewards of executing cyber attacks. Difficulties associated with attribution, political constraints, and other factors limit many organizations to using these tools of *negative punishment* as the primary form of influence to reduce cyberspace aggression.

In light of the challenges associated with aggression in cyberspace, a strategy based on promoting Internet freedom, which includes elements

[22] Department of Defense, "The National Military Strategy of the United States of America," 2011, 3-4.

of both *positive* and *negative reinforcement*, may seem counterproductive for many US agencies charged with keeping America safe from external threats. In this regard, US agencies do not speak with a common voice about cyberspace. There is a clear dichotomy between reinforcing favorable behavior on one hand and punishing objectionable behavior on the other. While all US agencies aim to protect American values, their approaches are dramatically different and their policies are often contradictory. For example, Evgeny Morozov points out that "nowhere is this chasm more obvious than in what the State Department says about Internet freedom and what the Department of Defense does about Internet Control."[23] The remainder of this chapter examines these differences in detail. It also examines the DHS, in addition to the DOD and State Department.

The DOD, acting under the control and authority of the President and Secretary of Defense, is the primary agency for inflicting *positive punishment* on America's adversaries. In accordance with the Laws of Armed Conflict, the DOD can impose costs through offensive military action with the goal of influencing an adversary's political will. The DOD is also responsible for protecting American interests from aggression and therefore its influence extends into the *negative punishment* quadrant. Through defensive military activity, the DOD can deny potential benefits to a would-be aggressor.

With respect to cyberspace, Joint Publication (JP) 3-13, *Information Operations*, highlights how the DOD will influence behavior in cyberspace through both *positive* and *negative punishment*. Both forms of influence are covered under the umbrella term, Computer Network Operations (CNO). CNO is divided into three basic forms of operations: Computer Network Attack (CNA), Computer Network Defense (CND), and Computer

[23] Morozov, *The Net Delusion*, 229.

Network Exploitation (CNE). CNA represents the offensive, or *positive punishment*, arm of the DOD operations in cyberspace, while CND represents the defensive, or *negative punishment*, portion of cyberspace operations. CNE is related to enabling operations and intelligence collection. It is not inherently a tool for influencing others. Rather it is a supporting function for obtaining situational awareness about the motivations and capabilities of others. Therefore it is not covered in detail here.

CNA consists of "actions taken through the use of computer networks to disrupt, deny, degrade or destroy information resident in computers and computer networks, or the computers and networks themselves."[24] This quote is one of the many uses of the "Four D's"—disrupt, deny, degrade or destroy—seen so often in military doctrine. The Four D's are negative objectives in that they influence behavior through the threat or actual imposition of cost.

CND involves "actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks."[25] Whereas CNA is directed against the adversary, CND activities operate on friendly networks. Their purpose is to eliminate the rewards associated with adversarial activity directed toward military networks. The DOD mandate for CND is restricted to the .mil domain, also known as the Global Information Grid (GIG), "through a combination of detection, deterrence, denial and multi-layered defense."[26]

Cyberspace operations contribute to the DOD goal of gaining *superiority*. Air Force Doctrine Document (AFDD) 3-12, *Cyberspace Operations*, defines cyberspace superiority as "The operational advantage

[24] Department of Defense, "Joint Publication 3-13: Information Operations," 13 February 2006, II-5.
[25] Department of Defense, "Joint Publication 3-13: Information Operations," II-5.
[26] Department of Defense, "The National Military Strategy of the United States of America," 19.

in, through, and from cyberspace to conduct operations at a given time and in a given domain without prohibitive interference." To achieve cyberspace superiority, the document goes on to say that "commanders should determine the minimum level of control required to accomplish their mission and assign the appropriate level of effort."[27]

As the earlier quote from Morozov alluded to, the DOD seeks control over the domain as the primary way to achieve its mission. Neither JP 3-13, nor AFDD 3-12, mention options related to *positive* or *negative reinforcement*. These public statements, which demonstrate American resolve to employ offensive and defensive capabilities in cyberspace, only represent the negative consequences of aggression toward the United States. They do not provide a strategy for establishing a commensurate benefit to the aggressor for taking favorable actions. The closest the DOD comes in this regard is contained in the 2011 *Strategy for Operating in Cyberspace*, which affirms the DOD's commitment to international engagement in support of the *International Strategy for Cyberspace* and to "the President's commitment to fundamental freedoms, privacy, and the free flow of information."[28] While this declaration is encouraging, DOD doctrine does not provide sufficient specific guidance to the military on how it will implement this commitment.

This is not to say that the DOD does not use *reinforcement* strategies at all. It has a long history of employing humanitarian assistance, disaster relief, foreign internal defense (FID) and counterinsurgency (COIN) operations. Humanitarian assistance and disaster relief are *negative reinforcement* tools in that they help eliminate suffering. FID and COIN operations provide foreign governments, who

[27] United States Air Force, "Air Force Doctrine Document 3-12: Cyberspace Operations," Change 1, 30 November 2011, 2.
[28] Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," July 2011, 9-10.

act according in the US and international interests, with support. These are *positive reinforcement* tools. Despite evidence of a more comprehensive approach to exercising influence across other missions of the DOD, the same cannot be said yet of cyberspace operations.

The Department of Homeland Security also plays a key role in influencing the behavior of cyberspace actors, but its tools of influence are more limited than those of the DOD. It does not have the authority to implement *positive punishment* approaches on international aggressors as directly as the DOD. Short of requesting military intervention, DHS can only impose costs on international cyberspace aggressors through cooperative law enforcement agreements with other nations. While its tools of *positive punishment* are limited, it does have the primary responsibility for defending the .gov networks of the United States and for coordinating the protection of critical infrastructure. Therefore, its primary tools relate to *negative punishment* by denying adversaries any benefit from conducting hostilities in cyberspace. This strategy is reflected in many key DHS documents including the 2003 *National Strategy to Secure Cyberspace*, the 2009 *National Infrastructure Protection Plan* and the *Quadrennial Homeland Security Review.*

The DHS issued the 2003 *National Strategy to Secure Cyberspace* under its responsibility for developing a comprehensive national plan for securing the key resources and critical infrastructure of the United States. It acknowledges the vital importance of cyberspace and goes so far as to call it the "nervous system—the control system of our country."[29] The strategy articulates three strategic objectives for securing cyberspace: 1) Prevent cyber attacks against our critical infrastructures; 2) Reduce national vulnerabilities to cyber attack; and 3) Minimize the damage and recovery time from cyber attacks that do

[29] Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," vii.

occur.[30] *Preventing*, *reducing* and *minimizing* are essentially negative objectives, in that they aim to decrease harm, rather than increase benefits through positive objectives such as promoting growth and developing new capability.

The 2009 *National Infrastructure Protection Plan* is a more comprehensive document than the *National Strategy to Secure Cyberspace* in that it provides guidance for securing all of America's critical infrastructure. The document defines 18 *critical infrastructure and key resources* and cyberspace is largely covered under one of these; the *information technology* sector. The guidance for protecting all 18 sectors revolves around protection by enhancing security, improving defenses, fostering resiliency and promoting education. For example, the document states:

> Protection can include a wide range of activities, such as improving security protocols, hardening facilities, building resiliency and redundancy, incorporating hazard resistance into facility design, initiating active or passive countermeasures, installing security systems, leveraging "self-healing" technologies, promoting workforce surety programs, implementing cybersecurity measures, training and exercises, business continuity planning, and restoration and recovery actions.[31]

Finally, in 2010, the DHS issued the inaugural *Quadrennial Homeland Security Review*. This document establishes three key concepts though which the DHS intends to form a foundation for comprehensive homeland security: *Security*, *Resilience* and *Customs and Exchange*. Security will be provided by "identifying and interdicting threats, denying hostile actors the ability to operate within [America's] borders, and protecting the nation's critical infrastructure and key

[30] Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," 13-14.
[31] Department of Homeland Security, "National Infrastructure Protection Plan," 2009, 1.

resources."[32] Resiliency is achieved by "foster[ing] a society that is robust, adaptable, and has the capacity for rapid recovery."[33] The final concept is related to maintaining lawful trade, travel and immigration.[34] Again, each of these concepts, while of vital importance, only provides for influence through denying benefits. Even resiliency, while positively influencing America's domestic population, still only serves to negatively influence adversaries. Resilience effectively denies an adversary the potential advantages of inflicting harm on the US since a resilient population and durability in its underlying support system will help keep America functioning even after an attack.

This short review of key DHS documents reveals that both the objectives and the means for achieving those objectives are defensive in nature. Like the DOD, the DHS is focused primarily on threats and not on the commensurate benefits of cyberspace. The organizational focus is not surprising since both agencies are responsible for different aspects of US national security. The culture of these organizations naturally inclines them to look toward defensive, *negative punishment* strategies and, in the case of the DOD, also *positive punishment* strategies when required. Ultimately, as Figure 2 shows, punishment strategies alone do not form a complete picture of influence. Both organizations may be able to enhance security by expanding their focus to include an assessment of the opportunities associated with cyberspace. This would lead to developing more comprehensive influence capabilities that include not only *punishment*, but also *reinforcement.* To examine, what a reinforcement strategy might look like, we turn to the Department of State and its stance on Internet freedom.

[32] Department of Homeland Security, "Quadrennial Homeland Security Review," February 2010, 15.
[33] Department of Homeland Security, "Quadrennial Homeland Security Review," 15.
[34] Department of Homeland Security, "Quadrennial Homeland Security Review," 16.

Secretary of State Clinton's speech on Internet freedom in 2010 discussed earlier not only expressed America's commitment to universal freedom of expression, it also outlined several specific methods through which the US would promote this objective. In it she highlighted how the State Department was already working in more than 40 countries to help individuals silenced by oppressive governments.[35] She went on to say:

> We are also supporting the development of new tools that enable citizens to exercise their rights of free expression by circumventing politically motivated censorship. We are providing funds to groups around the world to make sure that those tools get to the people who need them in local languages, and with the training they need to access the Internet safely… Both the American people and nations that censor the Internet should understand that our government is committed to helping promote Internet freedom.[36]

Secretary Clinton committed to working with partners in industry, academia and nongovernmental organizations to "establish a standing effort that will harness the power of connection technologies and apply them to our diplomatic goals."[37] As companies, especially those involved in social media, expand internationally, they are increasingly being pressed to filter and block various forms of content.[38] Therefore, Secretary Clinton included an appeal to private organizations to become more proactive in challenging foreign demands for censorship and surveillance. To help, she revitalized the Global Internet Freedom Taskforce as a forum for addressing global threats to Internet freedom and encouraged voluntary efforts by technology companies, such as the work done by the members of the Global Network Initiative.

On 8 December 2011, the State Department issued a factsheet describing its Internet freedom programs. The document highlighted six

---

[35] Hillary Clinton, "Remarks on Internet Freedom."
[36] Hillary Clinton, "Remarks on Internet Freedom."
[37] Hillary Clinton, "Remarks on Internet Freedom."
[38] Global Network Initiative, "Frequently Asked Questions," https://www.globalnetworkinitiative.org/faq/index.php (accessed 26 March 2012).

programming areas important to protecting freedoms online: *counter-censorship technology, secure mobile communications, digital safety training, emergency funding for activists, Internet public policy,* and r*esearch on Internet repression.* It also stated, that since 2008, the US Congress has appropriated $70 million to fund these efforts. As a result, the State Department, in concert with its partners, now has a portfolio of over 20 circumvention and secure communications tools. These tools help 1.9 million unique users per month and have received more than 115 million downloads. The State Department has also provided in-person training for over 7500 Internet activists in contested environments and made non-technical support materials available in over 10 languages to assist those in oppressed information environments.[39]

The Broadcasters Board of Governors (BBG) is one of the agencies partnered with the State Department to accomplish these objectives. The BBG is the independent federal government Agency that oversees all US civilian international broadcasting.[40] Its mission is to "inform, engage, and connect people around the world in support of freedom and democracy."[41] The BBG is known for its role in providing radio broadcasts over areas controlled by repressive regimes. The broadcast organizations include the Voice of America (VOA), Radio Free Europe/ Radio Liberty (RFE/RL), Office of Cuba Broadcasting (OCB), Radio Free Asia (RFA), Middle East Broadcasting Networks (MBN) and the International Broadcasting Bureau (IBB).[42]

---

[39] Department of State, "Factsheet: State Department Internet Freedom Programs," 8 December 2012, http://www.humanrights.gov/wp-content/uploads/2011/12/20111208-FactSheet-InternetFreedomPrograms.pdf (accessed 26 March 2012).
[40] Broadcasting Board of Governors, "Frequently Asked Questions," http://www.bbg.gov/about-the-agency/history/faqs/ (accessed 26 March 2012).
[41] Broadcasting Board of Governors. "BBG Strategic Plan 2012-2016," February 2012, http://www.bbg.gov/wp-content/media/2012/02/BBGStrategicPlan_2012-2016_OMB_Final.pdf (accessed 26 March 2012).
[42] Broadcasting Board of Governors, "Frequently Asked Questions."

As information technologies continue to change the way that people create and consume media content, the BBG has evolved into more than a collection of radio broadcasters. It has grown into a full-fledged multimedia news organization. The broadcasters "perform these vital tasks in places where extremism and authoritarianism are rampant, threats to press freedom persist, and governments censor Internet access, harass and imprison journalists and jam radio and television broadcasts." The BBG highlights its services as "one of the highest yielding, low-cost initiatives within public diplomacy."[43]

From a cyberspace perspective, one of the most important missions of the BBG, with the help of other public and private-sector organizations, is to underwrite Internet anti-censorship efforts. Specifically, the agency offers services such as the following:

- Daily e-mails with news summaries, instructions for bypassing government filters, and links to proxy or shadow sites

- Multimedia-capable, client-side proxy software customized for the BBG

- Short Message Service (SMS) delivery of proxy information, news and multimedia[44]

In addition to providing these types of technical services in partnership with agencies like the BBG, the State Department is also committed to employing its more traditional forms of influence to combat digital injustice. Through diplomatic efforts and strategic communication, the State Department is shedding light on repressive regimes who have imprisoned political dissenters. It has publically raised the cases of bloggers, journalists and other online activists to the

[43] Broadcasting Board of Governors. BBG 2009 Annual Report. 7. http://media.voanews.com/documents/09anrprt.pdf (accessed 26 March 2012).
[44] Broadcasting Board of Governors. Program Delivery Overview. July 2010. http://media.voanews.com/documents/Engineering_FactSheet_7_101.pdf (accessed 26 March 2012).

highest levels of government in countries ranging from Egypt and Tunisia to Azerbaijan, Syria and China.[45]

The Department of State is also supporting ways to strengthen democratic ideals and reinforce sound governance in other nations through information technologies. For example, in 2010, the department launched Civil Society 2.0 to "help raise digital literacy, strengthen the information and communications of NGOs, and amplify the impact of civil society movements." It is also working with local partners in Africa on an effort called Apps4Africa to connect communities on the continent and develop innovative solutions to shared problems.[46] These efforts aim to reinforce freedom of expression at the foundational level of emerging governments. If they are successful, they may be able to stop censorship before it starts.

The methods used by the State Department rely heavily on both *positive* and *negative reinforcement* strategies for influencing the behavior of other nations. Examples like Civil Society 2.0 and Apps4Africa *positively reinforce* transparency and principled governance abroad. The department's circumvention efforts *negatively reinforce* freedom of expression by providing individuals with a means to alleviate the harmful effects of information control. In contrast to the DOD's "Four D's"—disrupt, deny, degrade or destroy—the State Department is offering what could be called the "Two P's"—promote and provide. By *providing* funding and tools, and following a *reinforcement* strategy, the State Department is *promoting* the universal value of freedom of expression.

Conclusion

It is not possible to achieve a value as an end state in an absolute sense. It can only be continuously strived for. Professor Everett Dolman

[45] Department of State, "Internet Freedom," 15 February 2012, http://www.state.gov/r/pa/prs/ps/2011/02/156623.htm (accessed 26 March 2012).
[46] Department of State, "Internet Freedom."

from the School of Advanced Air and Space Studies called this "Pure Strategy." He advocated that "Strategy, in its simplest form, is a *plan for attaining continuing advantage*. For the goal of strategy is not to culminate events, to establish finality in the discourse between states, but to influence states' discourse in such a way that it will go forward on favorable terms."[47] [emphasis in original] Therefore, the US must view freedom of expression and, by extension, Internet freedoms as guiding principles that shape the policies and actions it takes. These activities should be coordinated such that each step along the way accumulates toward these ideals. They should guide and facilitate the development of policies and help prioritize a nation's limited resources. As Professor Dolman alludes to, strategy is less about the outcome of any particular action and more about the aggregate influence that all action has on the international strategic environment.

As we have seen, different agencies within the US have considerably different approaches when it comes to cyberspace influence. The DOD and DHS share a common threat-focused perspective that tends to limit their forms of influence to *punishment*. They both rely heavily on defensive, or *negative punishment,* capabilities aimed at denying the benefits of aggression. The DOD also has options for carrying out *positive punishment* at the President's request to impose costs on cyber belligerents. The State Department is more opportunities-focused, and largely falls on the opposite side of the influence quadrant shown in Figure 2. It has been developing capabilities in cyberspace aimed at rewarding those who strive to promulgate the value of freedom of expression. By promoting and providing tools to circumvent censorship, maintain anonymity and confidentiality, reinforce transparency and democracy, and share information about those who

[47] Everett Dolman, *Pure Strategy: Power and Policy in the Space and Information Age*, New ed. (New York: Routledge, 2005), 6.

engage in suppressing human rights, the State Department is influencing through *reinforcement*.

The goal here is not necessarily to favor one form of influence over another, since changing circumstances will dictate which form of influence is most appropriate for a given place and time. Rather, the point is to demonstrate that US agencies need a more comprehensive suite of influence options in and through cyberspace. They must take a balanced approach; one that is not all threat-focused or all opportunities-focused. They must also recognize that their individual policies and actions cannot be kept in isolation from one another. Instead, they must view their activities as key components of a perpetual campaign aimed at influencing others to adopt universal values.

Of course, promoting these values will not come without some difficulties. While modern information technology has changed the scope and scale of information exchange, the fundamental nature of freedom of expression is no different than it was when America's Founding Fathers established it as the first principle of the Bill of Rights. They understood that some actors would take advantage of this freedom in harmful ways. In spite of this reality, they held fast to a belief that in the aggregate the net benefit of a free society far outweighed the costs. This is the same belief that America must reaffirm in the Internet Age. Yet, it should not do so blindly. US policy makers must be ready to face both the positive and negative consequences of promoting freedom of expression. To that end, the next chapter outlines some of the problems that America may face even as it seeks to reap the rewards associated with these freedoms.

Chapter 3

Problems with Internet Freedom

The very technologies that empower us to lead and create also empower those who would disrupt and destroy.
– 2010 National Security Strategy

Freedom to browse whatever one wants is, of course, worth defending in its own right, but it's important to remember that, at least from a policy perspective, such freedoms would not necessarily bring about the revolutionary democratic outcomes that many in the West expect.
- Evgeny Morozov

History is replete with claims about how this or that invention would change the world for the better. Technologies that come the closest to achieving such a lofty assertion are often associated with improvements in communication. Guttenberg's printing press brought about widespread literacy and the knowledge of books to the masses. The telegraph enabled instantaneous, long-distance communication. Even major innovations in transportation, such as the automobile and airplane, serve a strong communicative purpose. They open up the world to new forms of interaction, globalize the economy and enhance the perception that it is indeed a small world. Yet, none of these advances have been as significant, as widespread, or as rapidly adopted as the Internet. There is no doubt it has transformed the scope and scale of information exchange around the world in historically unprecedented ways.

The emergence of the Internet also coincides with a particularly unique period in world history that helped facilitate its adoption. It arose at a point when societies around the world were becoming more open and individuals within those societies were looking for ways to take advantage of that freedom. The fall of the Soviet Union punctuated a historical trend toward freer societies as highlighted by the fact that

between 1950 and 2000 the number of democracies rose from only 22 to 120.[1] The confluence of advancements in technology and a global political climate more favorable to information exchange helped accelerate the expansion of the Internet.

For many, information technologies were not only shaped by the increase in freedom, but also helped shape the development of freedom around the world. Freedom of information goes hand in hand with democracy. Therefore, many people see the Internet, which facilitates that freedom better than any technology in history, as the ideal mechanism for pushing authoritarians into extinction. Evgeny Morozov labels these individuals *cyber-utopians*. They see the peaceful end of the Cold War as an unmistakable testament to the effectiveness of information technology for enhancing freedom. They believe the Internet favors the oppressed rather than the oppressor because it strikes at the heart of what authoritarians attempt to control.[2] If information control is the hallmark of authoritarian regimes, then the Internet should turn their traditional strength into a strategic vulnerability.

Morozov cautions the cyber-utopians that the Internet has a darker side. He chastises them for failing to see the broader political context surrounding information technologies and for underestimating the adaptability and sophistication of dictators.[3] In addition to the political problem highlighted by Morozov, Luke Allnutt sees similar challenges in the context of radicalism and crime. He declares that "Where the techno-utopianists are limited in their vision is that in this great mass of Internet users all capable of great things in the name of democracy, they see only a mirror image of themselves: progressive,

---

[1] Kristin M. Lord, *The Perils And Promise of Global Transparency: Why the Information Revolution May Not Lead to Security, Democracy, or Peace* (Suny Series in Global Politics), annotated edition ed. (Albany, NY: State University of New York Press, 2007), 6.
[2] Morozov, *The Net Delusion*, xiii.
[3] Morozov, *The Net Delusion*, xii.

philanthropic, cosmopolitan. They don't see the neo-Nazis, pedophiles, or genocidal maniacs who have networked, grown, and prospered on the Internet."[4]

The goal of this chapter is to examine the potential problems associated with Internet freedom. Leaders must be aware of both the good and bad consequences of promoting this ideal. With a solid understanding of the pros and cons, they will be able to make better decisions and be more prepared for the likely outcomes. Internet freedom, like all forms of freedom, must be approached in the aggregate. This is nothing new for democracies where freedom has historically been viewed as a net benefit to society, despite the problems that come with it.

Three potential problems are examined. The first problem is associated with the difficulty of predicting the political end-state. The foundation of the cyber-utopian movement is that self-determination is a fundamental right for all people and that freedom of expression is necessary for effectively determining what form of government a people desires. In addition to this fundamental assumption, there is a belief on the part of cyber-utopians that once empowered with free speech, people will desire, and be capable of achieving, a liberal democratic form of government. The first part of this chapter analyzes the likelihood of this outcome. It also examines the role of modern information technologies in either helping or hindering people achieve this desired end-state.

The second potential problem is how promoting access to the Internet may have the counterintuitive effect of strengthening the grip of an authoritarian regime on its society. As Chapter 1 highlighted, as more people communicate online, there is more opportunity for authoritarian regimes to intercept and monitor digital traffic. Also, as

[4] Luke Allnutt, "Twitter Doesn't Start A Revolution, People Do," *Christian Science Monitor*. 8 February 2010. http://www.csmonitor.com/Commentary/Opinion/2010/0208/Twitter-doesn-t-start-a-revolution-people-do (accessed 17 April 2012).

the population of Internet users increases, there are more opportunities for the authoritarian regime to propagandize its citizens. In the worst case scenario for cyber-utopians, authoritarian governments may actually be able to enhance their legitimacy by allowing the populace to perceive that their communication is free. To do so, authoritarian regimes may reduce their filtering and blocking efforts, while enhancing their surveillance and propaganda campaigns. Its populations see themselves as having a voice, while the regime exerts control and asserts power through less direct and less observable means.

The final potential problem is the likelihood that users empowered with information technology will decide to use their new-found freedom for personal reasons as opposed to political activism. Political activism, especially in oppressed societies, is risky. The reward of a better life requires a long-term term and often difficult commitment, and still a successful outcome is far from guaranteed. Personal use entails lower risk and the satisfaction is more immediate. The imbalance of risk versus reward favors a scenario where the majority of people will not be inclined to contribute to the political reforms desired by the cyber-utopian. Some of the users may even engage in criminal, violent or extremist behavior. Both forms of non-political behavior present problems to senior leaders who encourage Internet freedom. The challenges associated with nefarious activity are obvious, but the benign use cases are also problematic. As we saw in Chapter 2, the US congress has funded tens of millions of dollars toward Internet freedom campaigns. It may be difficult to sustain investments if the ways people use their freedom do not contribute to a better political end-state.

Problem 1: An Uncertain Political End-State

Ethan Zuckerman, a researcher at the Berkman Center for Internet and Society at Harvard University, wrote an essay in response to Secretary Clinton's Five Freedom's speech. In a piece entitled "Internet

Freedom: Beyond Circumvention," Zuckerman tackles the implications of a national policy aimed at global Internet freedom. He contests the prevailing assumptions that circumvention tools are the primary answer. While he recognizes their importance, Zuckerman challenges leaders to understand the practical limitations of deploying such tools *en masse* and he urges them to ask deeper questions about what they are hoping to achieve through providing Internet freedom.[5]

He contends that those engaged in promoting Internet freedom should start by asking the fundamental question, "How do we think the Internet changes closed societies?" He then offers three theories underlying the most common answers. He calls the first theory the "North Korea Theory," because it centers on a hope that "un-suppressed" information could provoke a popular uprising in heavily repressed nations. His second theory is the "Twitter Revolution Theory." It hinges on how citizens in closed societies use the power of the Internet to unite and overthrow their oppressors. Finally, the "Public Sphere Theory" describes how communication tools are long-term investments in freedom. While they may not spark revolutions immediately, they may create a new public sphere empowering the next generation of social actors to overcome the old regime.[6]

Zuckerman is a believer in the power of information, but for each of these theories he offers a cautionary tale. For the first, he highlights how simply having the ability to access information may only be a necessary, but not sufficient, condition for success. Second, tools such as Twitter and Facebook, while opening up new avenues to communicate, are easy to compromise, can be flooded with disinformation and are subject to government shutdowns. The third

[5] Ethan Zuckerman, "Internet Freedom: Beyond Circumvention," February 22, 2010. http://www.ethanzuckerman.com/blog/2010/02/22/internet-freedom-beyond-circumvention/ (accessed 6 April 2012).
[6] Zuckerman. "Internet Freedom: Beyond Circumvention."

theory suffers from its explicit long-term focus. It is difficult to test and it is hard to craft policy, and maintain clarity and commitment, over such long time horizons. Zuckerman's blend of theory and pragmatism can help cyber-utopians better understand the likely impact of information technology on closed societies. His approach helps clarify the ways and means of societal revolution through information technology, but it does not guarantee a positive end. The intermediate steps between oppression and freedom are often perilous and uncertain. Revolution is not something to be taken lightly.

So, when should senior leaders favor revolution as a viable solution to a political problem? First, the US is not interested in revolution for its own sake. Any support to revolutionaries should be tied directly to national security objectives. Second, a revolution should not be pursued if there is no reasonable prospect of a better situation following the turmoil of changing governments. This part of the answer comes with the strong caution that there is no guarantee of a favorable outcome and before engaging in support to revolutions senior leaders would be wise to heed the old adage that the devil you know may be favorable to the devil you don't. Finally, modern information technology raises new issues concerning how people mobilize for revolution. To help understand whether or not revolutions can result in a better future, we turn to Crane Brinton.

In 1938, Brinton first published his formative work entitled *The Anatomy of Revolution*. In it, he describes the conditions that precipitate revolutions, the roles and character traits of different individuals within a revolution and the phases that revolutions typically proceed through before a new order emerges. He uses four revolutions as a backdrop for his analysis: the English Revolution, the American Revolution, the

French Revolution and the Russian Revolution.[7] By reviewing Brinton's description of the historical pattern of revolutions, the cyber-utopian can form a better understanding of the outcomes, both positive and negative, that may result from Internet freedom campaigns.

In attempting to find uniformity across his historical case studies, Brinton determines that the precursory signs of a revolution are difficult to distinguish from the typical struggles and disagreements found in most modern societies. The difficulty in differentiating between ordinary political struggle and the kind that might lead to a change makes it hard for the cyber-utopian to determine if or when their efforts will produce results. This also makes measuring progress problematic. Without clearly defined measures of performance or an ability to measure advancement toward the desired end-state, cyber-utopians may struggle to maintain political support for continued investment in Internet freedom campaigns.

Brinton highlights government deficits, complaints over taxation, conspicuous governmental favoring of one set of economic interests over another and the separation of economic power from political power as all playing a part in establishing the conditions necessary for a revolution to occur. All of these factors can be seen in one degree or another in most states at any given time. Yet, despite the difficulties in distinguishing these characteristics from typical politics, Brinton concludes that what really precipitates revolutions is not simply the existence of these conditions, but a general, widespread sense of awareness about them. He asserts, "It must, however, be really in the air, and not simply in the mouths of professional seers or timid conservatives."[8] Other telltale signs include the loss of self-confidence among many members of the ruling class, the conversion of many members of that class to the belief that

[7] Crane Brinton, *The Anatomy of Revolution*, Revised ed. (New York: Vintage, 1965), 65.
[8] Brinton, *The Anatomy of Revolution*, 66.

their privileges are unjust or harmful to society and the refusal to pay taxes. These latter signs are likely to be more indicative of coming changes than the preceding ones.[9]

The first stage of a revolution is characterized by a surge of protests against government tyranny. Brinton shows that through pamphlets, plays, public addresses and other forms of expression, a demonstrable increase in organized opposition takes hold.[10] In the modern context, we could add spikes in protest-related keyword searches, increased "tweets" concerning problematic issues, more bloggers demanding change and a swell of membership in Facebook groups dedicated to government opposition. But, the real tipping point occurs when the existing regime fails to demonstrate its power to control such events. Either the opposition is too strong, resourceful, or virtuous or the regime is too half-hearted or inefficient to succeed.[11] At the end of this stage, the incumbent retains a nominal recognition of its status, but the revolutionaries increasingly wrest *de facto* control from the old regime. At the end of this phase, control of the state is split between two parties; the party of the old regime and the party of the revolution.[12]

Then comes the test of power. In each of Brinton's case studies there is a point, or several points, where the constituted authority is challenged by the illegal acts of revolutionaries and the existing regime resorts to force to maintain control. For a revolution to be successful, revolutionaries must prevail at this defining moment. If they do, then they will have shown themselves stronger and more capable of governing than the old regime.

---

[9] Brinton, *The Anatomy of Revolution*, 65, 78.
[10] Brinton, *The Anatomy of Revolution*, 68.
[11] Brinton, *The Anatomy of Revolution*, 68.
[12] Brinton, *The Anatomy of Revolution*, 79.

The cyber-utopian narrative often ends there, with the underdog having vanquished the oppressor. Unfortunately, the next phases of revolution are often marked by severe violence as the revolutionaries assert themselves as the new authority within the state. The responsibilities of managing the day-to-day affairs of government bureaucracy strain the original solidarity of the revolutionaries. Soon after the old regime falls, disagreements emerge over the details. Brinton calls the period following the fall of the old regime the "crisis" period because it can often result in a consolidation of power in the hands of radical idealists who seek to unify the new direction through fear and oppression. At this point, tyranny often takes hold and extremists exert their power through seizures of property, violent propaganda, discrimination, hostility toward religion, societal purges and other forms of overwhelming control. The "Reign of Terror" by both Robespierre and Stalin are defining examples of this possibility. Fortunately for the United States, the American Revolution proved an exception to the rule.

This reality presents a significant challenge for those who promote Internet freedom for the purpose of helping the oppressed achieve self-determination. As Jon Alterman asserts, "Revolutions, after all, are judged not by what they replace, but what they replace it with."[13] Cyber-utopians must account for the possibility that if the freedom leads to a revolution, then it might also result in a reign of terror as the new government struggles to consolidate and assert its authority. Accurately predicting whether a given population's uprising will result in either a reign of terror, an American style democracy, or something in between is extremely difficult.

[13] Jon B. Alterman, "The Revolution Will Not Be Tweeted," *The Washington Quarterly*, 34.4 (2011): 103.

Brinton's final stage of revolution is the "Thermador" period, which he characterizes as "a convalescence from the fever of revolution."[14] Eventually, the perpetrator of the reign of terror is vilified and his methods castigated by more moderate subsequent rulers. For example, in the Thermador period of the French Revolution, Robespierre was guillotined. Stalin's reign lasted until his natural death, but a successor to his seat at the head of the Soviet government, Nikita Khrushchev, decried his "cult of personality and its consequences." Much to the surprise of the Soviet establishment, he described the terrors, tortures and errors of Stalin's rule in a speech before the Soviet congress in 1956. This helped lead a wave of de-Stalinization across the Soviet Union.[15]

Successfully entering a Thermador period represents another challenge facing the cyber-utopian. The crux of this difficulty lies with the anonymizing qualities of the Internet. The ability to remain anonymous dramatically reduces the barriers to expression because a revolutionary can promulgate his or her message without significant risk of being identified and punished. The attribution problem dilutes the effectiveness of the existing regime to control or suppress the revolutionary message. While reducing these barriers helps, in theory, promote an environment favorable to revolutions, it also hinders those revolutions from implementing the accountability required for the rule of law to take hold when the new government takes over. As David Betz and Tim Stevens attest, "One major effect of cyberspace is that it makes it easier to subvert and harder to govern."[16]

Another difficulty facing post-revolutionaries in the Internet Age is the problem of transitioning from impulsive to planned behavior. As Morozov writes, "There are real dangers to substituting strategic and

[14] Brinton, *The Anatomy of Revolution*, 205.
[15] Walter A. McDougall, … *The Heavens and the Earth: A Political History of the Space Age* (Baltimore and London: Johns Hopkins University Press, 1997), 56.
[16] Betz and Stevens, *Cyberspace and the State*, location 2730.

long-term action with spontaneous street marches," and "the newly gained ability to mobilize may distract [leaders] from developing a more effective capacity to organize."[17] Alterman describes how the limitations of collective action tools, such as social media, become apparent in the post-protest period. While they help communicate grievances, they do very little to facilitate the necessary political bargaining required to successfully write a constitution. Also, they only play a limited role in helping form new political parties.[18] Revolutionaries accustomed to anonymity may have a hard time transitioning to non-repudiable activities, such as voting and paying taxes, potentially keeping the fever of the revolution from convalescing. Contrary to public perception, the Internet Age may actually erode rather than strengthen the ability to successfully participate in activism and form cohesive organizations.[19]

Research by Sherri Grasmuck, a sociologist at Temple University, reveals even more difficulties that may hinder the healing process. She found that many people who use social media groups to associate themselves with political movements or social causes do so for self-centered reasons. They join groups online not necessarily because they explicitly support a particular cause, but rather because they believe it is important to be seen by their online friends to care about such causes.[20] Their online presence represents their "hoped-for possible selves," not necessarily what they are actually like offline.[21] Malcolm Gladwell came to a similar conclusion after evaluating the how few people actually commit anything tangible to the causes they claim to support online. For example, in 2010, a Facebook page for Save Darfur Coalition had more than one million members, but the average per member donation was

[17] Morozov, *The Net Delusion*, 196.
[18] Alterman, "The Revolution Will Not Be Tweeted," 104.
[19] Morozov, *The Net Delusion*, 203.
[20] Morozov, *The Net Delusion*, 186.
[21] S. Zhao, S. Grasmuck, and J. Martin. "Identity construction on Facebook: Digital empowerment in anchored relationships," *Computer Human Behavior*, Vol. 24 (September 2008), 1816-1836.

only nine cents.[22] This phenomenon creates a significant barrier between displaying a propensity for behavior online and translating that desired behavior into real-world activity, especially when the activity is risky or costly.

Problem 2: Potentially Empowering Authoritarians

The second problem facing cyber-utopians is the potential for their efforts to backfire. Rather than achieving a liberal democracy, they may instead reinforce the power of incumbent authoritarian regimes. Some privacy advocates have expressed concern that promoting Internet freedoms may lead to an increased ability for authoritarian regimes to monitor and identify those who violate censorship laws. Morozov describes the dual nature of Internet technology when he writes, "The Internet is a much more capricious technology [than radio], producing side effects that can weaken the propaganda system but enhance the power of the surveillance apparatus or, alternatively, that can help to evade censorship but only at the expense of making the public more susceptible to propaganda."[23]

Rebecca MacKinnon, co-founder of the Global Network Initiative and advocate for protecting freedom of expression and privacy online, calls this phenomenon "networked authoritarianism." She highlights how authoritarian governments, prior to the Internet Age, were able to tightly control what their populations were hearing and saying. In the modern era, even when extensive filtering regimes are in place, citizens cannot be prevented from accessing and distributing content and participating in conversations, including exchanges related to politics and policy. Modern information technology environments have forced some traditional authoritarian governments to accept more dialogue

[22] Malcolm Gladwell, "Small Change: Why the revolution Will Not be Tweeted," *The New Yorker*, 4 October 2010, http://www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell (accessed 6 April 2012)
[23] Morozov, *The Net Delusion*, 83.

between themselves and their populations.[24] In theory, this is a positive step toward freedom of expression, but it has a darker side.

An increase in dialogue enhances the population's impression that it has a voice in its government and a stake in its political situation. Citizens may feel more engaged in their political circumstances as they participate in what they believe is a discourse between themselves and their government. This perception of having more freedom and influence comes at a price. As citizens increasingly migrate to the digital infrastructure to conduct those debates, the government increases its ability to manage information. As more conversations flow through cyberspace, the government improves its ability to monitor, curtail and prosecute behavior it deems unacceptable. The perception of freedom also serves to placate the populace by giving the people an outlet for their frustrations, which in turn suppresses dissident forces and helps legitimize the government. MacKinnon describes this situation as follows:

> Networked authoritarianism thus accepts and allows a lot more give and take between government and citizens than in a pre-Internet authoritarian state. The regime uses the Internet not only to extend its control but also to enhance its legitimacy. While one party remains in control, a wide range of conversations about the country's problems rage on Web sites and social-networking services. The government follows online chatter and sometimes people are able to use the Internet to call attention to social problems or injustices, and even manage to have an impact on government policies. As a result, the average person with Internet or mobile access has a much greater sense of freedom—and may even feel like he or she has the ability to speak and be heard—in ways that were not possible under classic authoritarianism. It also makes most people a lot less likely to join a movement calling for radical political change. Meanwhile, the government exercises targeted censorship focused on activities and conversations that pose the greatest threat to

[24] Rebecca MacKinnon, "Corporate Accountability in Networked Asia," 197-199.

> the regime's power, and also devotes considerable resources to proactively seeding and manipulating the nation's online discourse about domestic and international events.[25]

Networked authoritarianism is the embodiment of third-generation controls described in Chapter 1. Instead of focusing solely on the direct means of censorship, regimes may turn to "soft power" approaches for managing information to retain their authority. They recognize that too much blocking and filtering may encourage individuals to employ circumvention technologies. By allowing some dissent and encouraging at least the perception of freedom, authoritarian regimes keep their citizens on the networks they control. In this way, they can gather far more intelligence about the behavior of their citizens. They can also infuse the discussion with propaganda favorable to the regime. Third-generation controls, if used effectively, can pacify discontent, reinforce legitimacy and still manipulate behavior. Internet freedom campaigns that promote additional access to information technologies may reinforce this effect since they put even larger portions of the population online. Internet freedom could, under these circumstances, strengthen the position of the incumbent, rather than fostering political reform.

If the trend toward third-generation controls continues, then cyber-utopians will be faced with an obvious dilemma. Their attempts to incite a revolution by empowering the oppressed with freedom of expression may instead put more power in the hands of the incumbent authoritarian regime. It is still too early to tell how successful networked authoritarian regimes will be in this endeavor. Their activities will have to be carefully monitored to determine whether the net benefit of additional Internet freedoms favors the people or the regime. If the net effect is to empower the regime, then proponents of Internet freedom will have to refocus their strategy away from providing more access to the

[25] MacKinnon, "Corporate Accountability in Networked Asia," 198.

population toward countering third-generation controls. Morozov sums up the dilemma as follows:

> If, on careful examination, it turns out that certain types of authoritarian regimes can benefit from the Internet in disproportionally more ways than their opponents, the focus of Western democracy promotion work should shift from empowering the activists to topple their regimes to countering the governments' own exploitation of the Web lest they become even more authoritarian.[26]

Networked authoritarianism also raises significant issues associated with information sovereignty. Internet freedom campaigns challenge the ability for governments to control the flow of information within their territories. If information technology by itself threatens national sovereignty, then efforts to promote the spread of information technology may be considered aggressive behavior. For example, the official press agency of the People's Republic of China, the Xinhua News Agency, stated "information technology that has brought mankind all kinds of benefits has this time become a tool for interfering in the internal affairs of other countries."[27] They made this statement in response to the Green Revolution in Iran, which Chinese authorities saw as having been facilitated by America's purposeful use of information technology to undermine the Iranian government.[28]

If the aim, or even simply the perception of the aim, of such campaigns is regime change, then the regime will likely take action to defend its position. There is no reason for states promoting Internet freedom to assume that targeted regimes will only respond by enhancing their third-generation controls. If the regime feels sufficiently threatened by another nation's attempts to open up its society, then it may use

[26] Morozov, *The Net Delusion*, 28.
[27] Morozov, *The Net Delusion*, 12.
[28] Morozov, *The Net Delusion*, 12.

other forms of national power to retain control and maintain the status quo. Kristin Lord describes efforts to open up societies without the support of the incumbent government as "involuntary transparency." While cooperative and intentional acts of openness can lead to better relations among governments, she writes that "we should not expect involuntary transparency due to technological breakthroughs, investigative reporting by the global media or reports by NGOs to have the same effect."[29] Involuntary transparency will likely generate negative consequences ranging from deterioration in diplomatic relations to violence between nations.

If policy makers decide that regime change is in order, and that an Internet freedom campaign is an advantageous way to facilitate that objective, then they are not likely to consider the incumbent regime's claims to information sovereignty valid. Therefore, they may not have reservations about violating those claims. On the other hand, if the regime can successfully evolve toward networked authoritarianism, then campaigns for expanding access to information technology could end up strengthening the regime rather than bringing it down. As a result of the campaign, the regime will be in a better position to exert *de facto* sovereignty over the information within its borders than before the campaign began. If this occurred, the cyber-utopian approach would backfire and the regime may be able to manipulate the international political landscape to demonstrate how the Internet freedom programs violated their national sovereignty. In the worst case scenario, the result could be a blowback against the campaign originator, a less free target populace, and a more legitimate authoritarian state.

[29] Lord, *The Perils And Promise of Global Transparency*, 17.

Problem 3: Personal Use, Criminal Behavior and Violence

The third potential problem with Internet freedom concerns non-political use of the medium. Cyber-utopians hope that by expanding access to the Internet and eliminating controls, the forces of self-determination will take hold and the people will organize to form a freer government. This ideal, while laudable, must be balanced by the realization that political activity often comes with great risk. The users themselves may employ circumvention technology with noble aspirations of engaging in political debate, but quickly find themselves drawn to the less risky and more immediately satisfying goals. Morozov captured the essence of the problem when he proclaimed, "It seems highly naïve to assume that political ideals—let alone dissent—will somehow emerge from the great hodgepodge of consumerism, entertainment, and sex."[30]

Senior leaders who wish to facilitate the growth of the Internet should expect that the majority of users they enable will likely engage in purely personal pursuits. New users may not contribute to establishing a better, more democratic form of government, and may instead send e-mails, catch up with friends and family through social media, watch the latest episode of Lost or play Farmville. This kind of activity is not inherently bad, but it may be difficult for policy makers to justify the cost and political risk of Internet freedom programs when the usage statistics show how these connections contributed more to citizens' knowledge of Paris Hilton than Fidel Castro.

The following example highlights how these kinds of activities will be a portion of the consequences associated with enabling freedom online. In 2007, Forbes reported on how a concerned citizen named Steve Hunter decided to offer his personal computer as a proxy server to help oppressed individuals circumvent their oppressors. After installing

[30] Morozov, *The Net Delusion*, 70.

a software package known as "Psiphon" he posted instructions in a public forum on how to access the Internet through his computer and network connection. Shortly thereafter he was contacted by a prospective user who claimed to be in China. Unfortunately, the unexpected activity of his first customer turned him from an unfettered freedom advocate to a practitioner of censorship. Here is how the event unfolded:

> Mr. X first visited CNN.com and a few other media pages, but when Hunter checked his [proxy server] log again hours later, he discovered Mr. X had moved on to a search for nude pictures of Gwen Stefani and photos of a panty-less Britney Spears. Then he spent five hours on hard-core sex sites. "I was pretty pissed off," says Hunter. "I trusted that, as a person in certain vulnerable circumstances, he would act accordingly and behave himself. He didn't." Hunter blocked Mr. X from using his [proxy server], sent him an e-mail scolding him and posted a message to the Psiphon forum alerting other Psiphon hosts about the potential for porn surfers.[31]

The example shows how quickly idealism can change to realism in the face of experience. It also echoes Helmuth von Moltke's famous assertion that "No plan of operations survives the first collision with the main body of the enemy."[32] Cyber-utopians must be prepared to face many similar scenarios.

Non-political, personal use is far from the only problem. Those newly empowered with connectivity may also conduct illegal activity, such as identity theft, burglary, hacking, exploitation of minors or terrorism. The same anonymity that lowers the risk associated with political dissent also reduces the perceived risk of acting maliciously. The anonymity of the Internet may even encourage such behavior.

---

[31] Andy Greenberg, "Porn-Surfing By Proxy," *Forbes*, May 30, 2007. http://www.forbes.com/2007/05/30/psiphon-server-censorship-tech-intel-cx_ag_0530techpsiphon.html (accessed 6 April 2012).

[32] Daniel Hughes, ed., *Moltke On the Art of War: Selected Writings* (New York: Presidio Press, 1995), viii.

Individuals who believe there is little risk of adverse consequences may find themselves inclined to engage in behavior in the virtual world that they would not even consider in the physical world. Anyone who has ever read past the first few responses to a forum post or engaged in a debate in an open chat room understands that many people behave differently online. Secretary Clinton captured the positives and negatives of online anonymity in her Internet freedoms speech in 2010:

> [Anonymity] is one of the challenges we face. On the one hand, anonymity protects the exploitation of children. And on the other hand, anonymity protects the free expression of opposition to repressive governments. Anonymity allows the theft of intellectual property, but anonymity also permits people to come together in settings that give them some basis for free expression without identifying themselves.[33]

More opportunity to access the Internet means more opportunity for Internet-related crime. Some users will purposefully commit these crimes and others will be unwitting accomplices. The problem of cybercrime has become so widespread and so lucrative that experts estimated its economic impact to the US alone to be in excess of $1 trillion in 2008.[34] It is also an enticing alternative to poverty and oppression. Having freedom of expression does not, by itself, put food on the table or clothe one's family. When there are few alternatives for generating income, impoverished individuals may, for example, turn to identity theft or credit card fraud to alleviate their financial burdens. Others may not intentionally engage in criminal activity, but may facilitate it nonetheless. Criminals may gain access to an individual's accounts, infect their machines with malware or hijack their Internet connections. Each of these security breaches cover the actual criminal's

[33] Hillary Clinton, "Remarks on Internet Freedom."
[34] White House, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," May 2009, 2. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (accessed 17 April 2012).

tracks and may lead law enforcement to the innocent patsy rather than the perpetrator. It is unlikely that new Internet users empowered with access to information technology will understand the complexities of digital security. Internet freedom initiatives may open up their access to information, but may also put them at risk.

In addition to economic crime, Internet freedom initiatives may also empower users to attack the United States. Simply because oppressed individuals may be unhappy with their own government does not imply that they have a favorable view of America. After gaining access to the Internet, rather than taking to the blogosphere they may download the latest copy of Metasploit and begin hacking campaigns against US interests. Even those individuals that do proceed to political activism within their own nations may be equally inclined to challenge the US government. Some may volunteer their connections and machines to activist groups. For example, the hacker group Anonymous encourages volunteers to download software called the Low Orbit Ion Cannon to support distributed denial of service attacks.[35] Others may look to low-cost cloud computing service providers to gain access to tremendous amounts of computational resources. For example, for as little as $0.08 per hour per machine, users can gain access to infrastructure hosted in Amazon's Elastic Compute Cloud.[36] By tying many of these virtual machines together, malevolent users can attempt to crack passwords or launch denial of service attacks on demand.

Finally, digitally enabled terrorism represents one of the biggest threats to the cyber-utopian agenda. It is one of the most serious and politically charged aspects of the free speech debate. Many terrorist organizations, such as Al Qaeda, are masters of online propaganda. The

[35] Tom Nardi, "Low Orbit Ion Cannon: Exposed," *The Power Base*, 4 March 2012, http://www.thepowerbase.com/2012/03/low-orbit-ion-cannon-exposed/. (accessed 30 March 2012).
[36] Amazon, "Amazon EC2 Pricing," http://aws.amazon.com/ec2/pricing/ (accessed 30 March 2012).

distributed nature of the medium fits their organizational model perfectly. Terrorist groups leverage social networking services, blogging sites and discussion forums to promulgate their message, indoctrinate recruits and display their violent acts to the world. Connectivity to cyberspace also supports fundraising, financial transfers between operating cells and money laundering.[37]

The Internet is an especially useful tool for tying together likeminded individuals separated by vast geographic distances. The global nature of cyberspace facilitates the dissemination of terrorist ideology and increases the pool of potential recruits. Many counterterrorism professionals, especially those in Western European nations, are finding it difficult to keep the ideology from radicalizing an increasingly alienated and vulnerable immigrant population inside their own borders.[38] Promoting additional connectivity to the Internet may exacerbate this growing trend among the diaspora of culturally similar, but geographically separated, individuals. Advocates of Internet freedom initiatives need to approach this situation with caution. It will likely be extremely difficult, from a political perspective, to adhere to the Internet freedom agenda after the first American-supplied circumvention tool is used in an attack against America.

Conclusion

Each of the examples in this section helps express the dual-nature of information technologies. On one hand, they can help promote universal human rights, but on the other they can be used to undermine those same values. Because negative consequences exist, there will be limits to how far nations are willing to go in promoting freedom of expression through the expansion of access to information technology. It

[37] Audrey Kurth Cronin, *How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns* (New York: Princeton University Press, 2011), 175.
[38] John Mackinlay, *The Insurgent Archipelago: from Mao to Bin Laden* (New York: Columbia University Press, 2010), 99-121.

is unrealistic to expect that everyone empowered with the responsibility that comes with free speech will uphold that responsibility in a worthy manner. Despite the challenges, nations that value freedom must find ways to appropriately mitigate the negatives without compromising their core principles. They must maintain a proper perspective and not lose sight of the benefits. Lawrence Lessig captured this succinctly when he declared, "I care less about enabling the war on drugs than I do about enabling democracies to flourish." Secretary Clinton summarized the issue in a more diplomatic tone as follows:

> Now, all societies recognize that free expression has its limits. We do not tolerate those who incite others to violence, such as the agents of Al Qaida who are, at this moment, using the Internet to promote the mass murder of innocent people across the world. And hate speech that targets individuals on the basis of their race, religion, ethnicity, gender, or sexual orientation is reprehensible. It is an unfortunate fact that these issues are both growing challenges that the international community must confront together. And we must also grapple with the issue of anonymous speech. Those who use the Internet to recruit terrorists or distribute stolen intellectual property cannot divorce their online actions from their real world identities. But these challenges must not become an excuse for governments to systematically violate the rights and privacy of those who use the Internet for peaceful political purposes.[39]

The scope and scale of modern information technology make it tempting for some to believe that the fundamental nature of freedom has changed. For those who do, the Internet is a scary place. They believe the risks associated with cyberspace vulnerabilities and security threats outweigh the benefits cyberspace provides. They also contend that while the First Amendment of the Bill of Rights and the universal values of freedom of expression promoted by the UDHR were appropriate historically, those ideals cannot endure in the modern communications

[39] Hillary Clinton, "Remarks on Internet Freedom."

environment. As a result, those who see the Internet Age as having fundamentally shifted the nature of freedom may be willing to trade significant portions of their digital liberty for security.

A more likely reflection of the Internet Age is that only the character of freedom has changed and traditional notions of protecting liberty are still applicable today. As Benjamin Franklin famously said, "Those who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety."[40] Those fearful of information technology who are willing to undermine American principles in the name of security would do well to ruminate over his words. This is not to say that the challenges outlined in this chapter are not significant, only to reinforce that they are not fundamentally different from the challenges associated with freedom since the dawn of history. In every free society there will be a healthy and vigorous exchange of ideas, and there will be liars and frauds. In every free economy there will be cooperative and mutually beneficial trade, and there will be theft and counterfeit.

Democracies do not throw out their core principles to overcome these challenges. Rather, they mitigate them to the best of their ability without violating their fundamental values. They see freedom as more beneficial to society in the aggregate and they are willing to accept the inevitable bad actors out of a belief that there is a larger and more powerful pool of good ones.

[40] William Temple Franklin, *Memoirs of the Life and Writings of Benjamin Franklin* (London: H. Colburn, 1818), 270.

Chapter 4

Recommendations

On their own, new technologies do not take sides in the struggle for freedom and progress, but the United States does.
– Hillary Clinton

To subdue the enemy without fighting is the acme of skill.
– Sun Tzu

If the United States believes that protecting freedom of expression around the world is not only in its national interest, but is also a fundamental human right, then it must take practical steps toward promoting that objective. This chapter provides a series of recommendations for engaging in Internet freedom initiatives. It is largely focused on the DOD, but many of the recommendations will require participation from a broad range of government and non-government actors. In focusing on the Department of Defense, the aim is not to undermine the current important efforts ongoing in cyberspace offense, defense and exploitation, but rather to encourage the DOD to expand its range of capabilities. In addition to denying, degrading, disrupting and destroying to eliminate security threats, the DOD should also promote and provide access to information technology to champion American values.

Five categories of recommendations are presented. The first deals with "walking the walk" as they say. First and foremost, the US must lead by example and demonstrate its commitment to digital freedom at home to enhance American credibility abroad. Second, the DOD needs to expand the lexicon of cyberspace operations to promote a more broad consideration of opportunities in the new domain, to include Internet freedom initiatives. In line with expanding the range of thought on cyberspace operations, this chapter gives particular attention to the term

Strategic Information Warfare. The third recommendation includes expanding the historical definition of this term to include combating information controls for enhancing freedom of expression. The fourth recommendation recognizes that the DOD will not be able to accomplish these tasks in isolation from other government agencies or even private organizations. The ubiquitous nature of information technology and the diverse skills required to promote Internet freedom will require careful coordination among many stakeholders. The final recommendation offers a series of practical methods for helping the DOD incorporate Internet freedom initiatives into its suite of capabilities. This last recommendation covers both technical and personnel issues.

Lead by Example

The first and most fundamental recommendation for America is to lead by example. The most legitimate means of securing American values and promoting them abroad is to safeguard them domestically. This is a less direct form of influence than discussed in Chapter 2. Leadership through example is based on the recognition that not all forms of influence are transactional and the US should not assume that it can directly manipulate the cost equation associated with all actors in cyberspace. There are simply too many actors, too many interactions and insufficient resources to shape all cyberspace behavior. This form of influence works by allowing others to see the positive results that freedom can bring and, if they value those outcomes, they may be more inclined to adopt similar strategies on their own.

This is easier said than done. As Hal Roberts and John Palfrey acknowledged, "The Internet is a 'surveillance-ready' technology."[1] Modern information technology enables governments to monitor

[1] Hal Roberts and John Palfrey, "The EU Data Retention Directive in an Era of Internet Surveillance," *Access Contested: Security, Identity, and Resistance in Asian Cyberspace Information Revolution and Global Politics*, Ronald Deibert et al., eds. (Cambridge, MA: The MIT Press, 2012), 36.

behavior, retain records of behavior and search for patterns of behavior in radically more expansive and more efficient ways. Traditional forms of surveillance and censorship were mitigated by the difficulties associated with accomplishing the task. The natural friction between surveillance and censorship laws, and the ability to enforce them, formed a protective barrier around individual privacy. Digital technologies alter the balance in favor of surveillance.[2] By removing the friction, information technologies make it easier for governments, even liberal democratic ones, to enact laws based on expediency rather than to legislate in ways that reinforce fundamental values.

Despite the intense political pressure to be seen as "doing something," US lawmakers and senior leaders must rise above expediency. They must recommit to the principles of freedom of expression and recognize that these values are enduring. Their nature has not changed even as the character of information technology has changed rapidly. The 2010 *National Security Strategy* reinforces America's commitment to overcoming this challenge. It states:

> Our values have allowed us to draw the best and brightest to our shores, to inspire those who share our cause abroad, and to give us the credibility to stand up to tyranny. America must demonstrate through words and deeds the resilience of our values and Constitution. For if we compromise our values in pursuit of security, we will undermine both; if we fortify them, we will sustain a key source of our strength and leadership in the world—one that sets us apart from our enemies and our potential competitors.[3]

Finding the appropriate balance will be difficult, but failing to abide by these words may have many unintended consequences, both domestically and internationally. Domestic surveillance and censorship

[2] Lessig, *Code: Version 2.0*, 201-203.
[3] White House. "National Security Strategy of the United States of America," 10.

laws that are too expansive will push users to networks outside of the purview of these laws and expand the demand for circumvention technology. As a result, law enforcement will have less access to useful data. A second order effect could be the further erosion of network security. As more users employ circumvention tools they become increasingly more vulnerable to the developers and deployers of those tools and the networks on which they reside. For example, when the music industry cracked down on file sharing, many users moved to the digital underground to obtain the files. Malware developers capitalized on the transition and unwitting audiophiles became significant targets.[4] As they moved between the more trusted parts of the Internet and the unregulated file transfer sites, they spread the malware between these domains and opened up new security vulnerabilities to the larger population of Internet users. Finally, efforts to enforce overly restrictive surveillance and censorship laws could create the equivalent of an arms race in cyberspace where each side develops measures and countermeasures in an increasingly costly and self-defeating spiral.[5]

The effects of such domestic regulation will also have international effects. If the United States is serious about enhancing freedom of expression by promoting information technology abroad, then it cannot unjustly restrict those freedoms at home. Efforts to undermine the information controls of authoritarian nations would be delegitimized by American domestic policy. It would be a classic case of "do as I say, not as I do." Too many domestic restrictions may even help reinforce censorship abroad as authoritarian nations point to the precedent set by the US to justify their own controls. Morozov captured this challenge when he wrote, "As long as Western governments regulate the Internet out of concerns for terrorism or crime, as they currently aspire to, they

[4] Roberts and Palfrey, "The EU Data Retention Directive in an Era of Internet Surveillance," 41.
[5] Roberts and Palfrey, "The EU Data Retention Directive in an Era of Internet Surveillance," 41.

also legitimize similar efforts—but this time done primarily for political reasons—undertaken by authoritarian governments."[6]

Expand the Cyberspace Mindset

There is little, if any, discussion of *reinforcement* strategies in current cyberspace doctrine or training. Senior leaders should fix this skewed emphasis on *punishment* by taking steps to change the military's current threat-focused culture and enhance awareness of opportunities in the domain. While it is extremely important to remain vigilant in protecting the .mil networks and to deter international aggression, this one-sided perspective fails to cover the full spectrum of ways to influence cyberspace actors. By emphasizing a more comprehensive approach to cyberspace influence in public forums, doctrine and training, leadership can expand the option space for its cadre of cyberspace professionals.

Without emphasizing reinforcement strategies in cyberspace, the DOD will not be able to move beyond the Four D's— disrupt, deny, degrade, or destroy—to incorporate the Two P's—promote and provide. This is nothing new for other aspects of the military. The DOD has been participating in reinforcement campaigns in other domains for decades. From the Berlin Airlift after World War II to the recent earthquake relief in Haiti, the DOD has been instrumental in alleviating physical suffering by providing humanitarian assistance and protecting civilians from violence. Cyberspace professionals should be equally prepared to alleviate threats to freedom of expression. They should be trained and equipped in circumvention technologies and methods so they are capable of recognizing, and are prepared to combat, information oppression.

Contributing to the problem is an imprecise understanding of the many facets of "cyberspace operations." Adequately preparing cyberspace professionals for Internet freedom initiatives will require a more nuanced

[6] Morozov, *The Net Delusion*, 224.

treatment of the term. There are many layers of cyberspace operations and the term's current usage fails to account for the significant differences associated with operations at each layer. Military doctrine captures how operations can occur both "in, through and from"[7] cyberspace, but more emphasis needs to be placed on operations that occur *on* the domain itself. The former description, while valid, creates the impression that cyberspace is a static domain. By adding more emphasis to operations conducted to modify the domain itself, cyberspace professionals will be better equipped to understand key components of censorship and circumvention.

Operations "through and from" cyberspace contribute to effects in other domains. For example, by employing digital communications, leaders can exert command and control over physical forces. Offensive cyberspace operations may even contribute to disruptive or destructive effects in the real world. Operations "in" cyberspace contribute mostly to effects against the semantic layer of cyberspace by adding, exchanging, modifying, destroying or disrupting information. In contrast, operations "on" cyberspace shape the domain itself by modifying the physical or syntactic layers to create military advantages. Combat engineering provides a good analogy. If a land army wishes to cross a river or march through a forest, it can modify the terrain by building a bridge or cutting a road. The combat engineer operates *on* the land domain to facilitate operations *in* and *through* it.

To understand censorship and circumvention, especially first- and second-generation techniques, one must grasp operations *on* cyberspace. Creating and combating these effects requires an intimate knowledge of the protocols, software, engineering and standards that make up the domain. Third-generation censorship and circumvention largely operates

[7] United States Air Force, "Air Force Doctrine Document 3-12: Cyberspace Operations," 2.

in the cyber domain and practitioners who wish to combat censorship at this level require a different skill set. Rather than detailed technical knowledge, third-generation circumvention techniques require strategic communication skills, the ability to engage on the battle ground of ideas and the ability to counter propaganda.

By expanding the mindset of cyberspace operations and incorporating a more comprehensive approach to influence, senior leaders can enrich the culture of cyberspace professionals. It requires public acknowledgements of the need for *reinforcement* strategies, doctrinal revisions and enhanced training. It also requires a more nuanced description of cyberspace operations. By emphasizing the ability to modify the medium of cyberspace, in addition to communicating in it and operating through it, the DOD will expand its range of capabilities for creating cyberspace effects. Internet freedom initiatives require this level of detail to effectively develop the breadth of tools and skill sets required to combat censorship across all generations of controls. Finally, cyberspace doctrine should be updated to include practical provisions for promoting and enhancing Internet freedoms tailored to match the needs of each phase of military operations.

Rethink Strategic Information Warfare

Clausewitz established that all activity in war was conducted "to compel our enemy to do our will."[8] He stressed influence, albeit violent influence, as opposed to compulsion through annihilation. Early air power theorists, such as Giulio Douhet and Billy Mitchel, seized upon the airplane as a radically new means of attacking the enemy's most cherished assets. The strategic bombing campaigns of World War II formulated by the Air Corps Tactical School (ACTS) leaned heavily on these theories. As a result, ACTS produced air campaign plans aimed at

[8] Clausewitz, *On War*, 75.

maximizing Allied influence over the enemy's will through targeted bombing. Despite being tempered by the practical outcomes of World War II and subsequent efforts in Korea and Vietnam, modern air power theory retains much from its foundational texts. For example, Colonel John Warden saw the Iraqi army as composed of five concentric rings each holding progressively more value to enemy.[9] His team at Checkmate devised an air campaign for the first Gulf War to target the central, most valuable rings to achieve the most influential effect on the enemy's will.

Yet these theories of influence through air power are still essentially indirect means of shaping an adversary's desire to continue hostilities. They operate by threating or carrying out violence. The enemy may still be hostile even after these campaigns; only they may no longer have the capacity to act on their desires. Cyberspace may offer a more direct method of changing the adversary's will to act.

Reflecting the influence air power theory has had on other domains, in 1996, the RAND Corporation released a report that added the term *Strategic Information Warfare* (SIW) to the military lexicon. The authors defined SIW as "utilizing cyberspace to affect strategic military operations and inflict damage on national information infrastructures."[10] The report centered on the growing threat posed by America's reliance on the rapidly expanding communications infrastructure of cyberspace. It highlighted how information-dependent critical infrastructure, such as electric power distribution, monetary exchange, air traffic control and oil and gas management, could potentially be "attacked" from anywhere around the globe. In the Internet Age, America's posture of projecting power abroad to ensure domestic security may no longer be entirely valid

[9] John Andreas Olsen, *John Warden and the Renaissance of American Air Power* (Washington, D.C: Potomac Books Inc., 2007), 108-112.
[10] Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, *Strategic Information Warfare: a New Face of War* (Santa Monica, CA: RAND Publishing, 1996), 1.

because there is no "front line" in cyberspace for vulnerable infrastructure to hide behind.[11]

David Lonsdale reinvigorated the concept of SIW in his 2004 book, *The Nature of War in the Information Age: Clausewitzian Future*. Rather than simply focusing on the threat posed by the adversary's use of SIW, Lonsdale envisioned the opportunity for the US to gain advantage by conducting its own SIW campaigns. He defined SIW as "the ability to conclude wars by attacking the National Information Infrastructure (NII) of an enemy through cyberspace."[12] He also highlighted its relationship to strategic bombing, since it seeks to bypass enemy surface forces and strike directly at an enemy's centers of gravity.

There is no doubt that the ability to use cyberspace for creating destructive effects in the physical domain is extremely important. The problem, though, is that the term SIW is limited to a focus on only these effects. It does not account for the far more prevalent war over the control of information going on inside cyberspace. While the consequences of a cyber attack on critical, physical infrastructure could be significant, to date, none of the doomsday predictions have materialized. This is not to say that the US should diminish its efforts to protect itself against major cyber attacks. Rather, the intention is to emphasize that a far more widespread and continuous information war is going on every day. In this conflict individual battles result in far lesser consequences than a major cyber attack against critical infrastructure, but their aggregate effect may be just as significant to overall US interests.

Modern SIW is just as much about the battle over influence and information as it is about disrupting or destroying physical systems. The

---

[11] Molander et al., *Strategic Information Warfare*, xiii.
[12] David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future (Strategy and History)* (London: Routledge, 2004), 135.

stifling effect of information control suppresses a people's ability to determine their own form of government. This helps keep authoritarian regimes in power and creates tension between authoritarian states and democratic ones. A more powerful form of SIW may be engaging in Internet freedom initiatives to undermine the ability for authoritarian regimes to assert their controls. This expanded view of SIW may be more politically advantageous than the traditional form, since the international community has already professed a commitment to the universal value of freedom of expression. Many in the international community are therefore more likely to support Internet freedom initiatives than destructive cyber campaigns targeting critical infrastructure.

Incorporate Whole of Nation Approaches

Stovepiped decision making hinders the America's ability to respond effectively to international issues. As Chapter 2 highlighted, agencies within the US do not speak with a singular voice. From a cyberspace perspective, the DHS and DOD focus on threats and influence through *punishment*, while the State Department sees more opportunities and pursues influence with an emphasis on *reinforcement.* Their inherent responsibilities, their internal culture and their organizational histories helped shape each agency's perspectives on dealing with cyberspace. It is not surprising that each arrived at different conclusions, although those differences should not become excuses for working in isolation. Rather these agencies should integrate their respective capabilities and strengths to achieve US national security objectives and to reinforce American values abroad.

The DOD already has a significant history of working with other agencies to tackle international problems. Joint Publication 1: *Doctrine for the Armed Forces of the United States,* commits the DOD to unity of effort through "close, continuous interagency and interdepartmental coordination and cooperation, which are necessary to overcome discord,

inadequate structure and procedures, incompatible communications, cultural differences, and bureaucratic and personnel limitations."[13] It also provides a mechanism for organizing the interactions of multiple agencies. The construct is called the Joint Interagency Coordination Group (JIACG). It is a tool for Geographic Combatant Commanders (GCC) to collaborate with other US government agencies and departments. Through the JIACG, the GCC can facilitate tailored solutions in partnership with US ambassadors and country teams to customize Internet freedom efforts in the region.

The regional focus of the JIACG is important because the requirements for combating digital oppression will vary by country. Intimate knowledge of the political, social, legal and economic factors in each region will be critical for understanding how receptive the local populace will be to Internet freedom initiatives. Only those familiar with the local details will be capable of mitigating the potential problems described in Chapter 3 while still promoting information freedom to support political reform. In particular, regional leaders will be in the best position to sense whether the conditions for reform are present. They will also be instrumental in monitoring whether the Internet freedom initiatives are leading to a broader engagement between the people and their government or if the government is turning the effort into effective networked authoritarianism. Depending on the direction, regional leaders will have to adapt their strategies accordingly either by continuing to expand access for the people or by targeting the controls of the regime. Finally, since resources are finite, the regional leaders will also be in the best position to efficiently and effectively allocate money, people and infrastructure to the problem.

[13] Department of Defense, "Joint Publication 1: Doctrine for the Armed Forces of the United States," Change 1, 20 March 2009, xxi.

Interacting with other government agencies is only part of the solution. Much of the technological expertise for information technology resides outside of the government. Effectively implementing Internet freedom initiatives requires additional coordination and partnership with industry and nongovernment organizations. This interaction has to occur both in the region where the efforts are focused and at home where important coordination forums already exist. In theater, the primary mechanism for nongovernmental organization coordination is the Civil-Military Operations Center (CMOC). It is composed of representatives from military, civilian, US and even multinational agency stakeholders.[14] The CMOC is only a coordination cell; it does not translate into authority over the participants. Many of the participants will have dramatically different organizational structures, operating methods and philosophies. They are not likely to put themselves in a supporting role to the DOD, but they may be incentivized to participate with the DOD so long as that interaction contributes to a common objective.[15] The DOD should facilitate discussion, coordination and operations concerning Internet freedoms through both the JIACG and CMOC to ensure unity of objective and maximize efficiency.

Domestically, there are already forums where nongovernment organizations are engaged in Internet freedom initiatives. For example, in 2009, companies such as Facebook, Google, MTV and AT&T came together for a summit called the Alliance of Youth Movements. The event demonstrated that private companies and citizens were concerned about the future of freedom of expression and that they were committed to using their skills and resources to combat censorship.[16] Secretary

[14] Department of Defense, "Joint Publication 1: Doctrine for the Armed Forces of the United States," VII-7.
[15] Department of Defense, "Joint Publication 3-08: Interorganizational Coordination During Joint Operations," 24 June 2011, IV-27.
[16] Morozov, *The Net Delusion*, 182.

Clinton even endorsed the meeting in an official address.[17] Movements.org arose from the collaboration of the summit. Its mission is to help digital activists build their capacity and make a greater impact on the world. They help identify, connect and support the endeavors of grassroots activists around the globe for promoting social change.[18]

Another important forum is the Global Network Initiative (GNI). Google, Microsoft, and Yahoo! have joined together with human rights groups, press freedom groups, private investors and academia to deal with "increasing government pressure to comply with domestic laws and policies in ways that may conflict with the internationally recognized human rights of freedom of expression and privacy."[19] The GNI works with information technology companies to help them meet their business objectives without compromising on their principles. It offers guidance, knowledge and even policy engagement to help protect the accountability and transparency of citizens around the world.[20]

Forums like these are shaping international relations. As multinational corporations recognize the power that they wield as a result of their dominant positions in the global economy, they are increasingly using that power to engage in a form of foreign policy that was once reserved for nations alone. They have no means for engaging in violence, and no desire to, but they do have tremendous influence over the ways that nations and their citizens communicate. Promoting values abroad is no longer reserved solely for diplomats and militaries. Therefore, the DOD, in partnership with other government agencies,

---

[17] Hillary Clinton, "Message for Youth Movement Summit," 16 October 2009, http://video.state.gov/en/video/45067767001/message-for-youth-movement-summit/s~creationDate/p~1/?s=YWxsaWFuY2Ugb2YgeW91dGg= (accessed 30 March 2012).
[18] Movements.org, "Mission," http://www.movements.org/pages/mission (accessed 30 March 2012).
[19] Global Network Initiative. "Global Network Initiative," https://www.globalnetworkinitiative.org/index.php (accessed 30 March 2012).
[20] Global Network Initiative. "Who We Are. What We Do. Why It Matters," https://www.globalnetworkinitiative.org/cms/uploads/1/GNI_WhoWhatWhere_1.pdf. 2. (accessed 30 March 2012).

especially the State Department, must participate in and integrate with these powerful private initiatives to help promote American values. In this way, the US will become more effective at organizing all of the tools at its disposal toward a common purpose.

Develop Capabilities that Promote Internet Freedom

Finally, the DOD must put the previous recommendations into practical application. This starts by organizing, training and equipping people with skill sets that span all aspects of cyberspace. To be truly successful in this domain, the military will have to differentiate the cyberspace professional workforce with more precision. Each layer of the Internet protocol stack from Figure 1 requires its own unique blend of education, skill, and experience. The required technical specialties span computer and electrical engineering, computer science, information theory, network management, information security and application design. Aside from technical expertise, comprehensive cyberspace operations also require specialists in psychology, anthropology, international relations and political science. No one training or accession program will be capable of producing individuals with all of those skills. Rather, effective cyberspace operations will come from teams of specialized members capable of working together "on, in, through and from" cyberspace to achieve national security objectives.

The DOD should also expand cyberspace doctrine to incorporate more options across all phases of operations. Joint Publication 3-0: *Joint Operations* presents the "Phasing Model," which describes six phases of possible operations based on existing geo-political conditions: *Shape, Deter, Seize Initiative, Dominate, Stabilize,* and *Enable Civil Authority*.[21] Traditional military operations and capabilities largely focus on applying overwhelming force in the *Seize Initiative* and *Dominate* phases. The joint

[21] Department of Defense, "Joint Publication 3-0: Joint Operations," 11 August 2011, V-7 through V-9.

publication calls for the military to place a commensurate amount of emphasis on shaping the battlefield prior to hostilities and to support a peaceful transition to civil control after hostilities complete.

Joint and service-level doctrine governing cyberspace operations should be aligned with the Phasing Model. Joint Publication 3-13: *Information Operations* and Air Force Doctrine Document 3-12: *Cyberspace Operations* still focus primarily on cyberspace offensive, defensive and exploitation operations. These activities form an incomplete picture of what needs to occur to achieve a more comprehensive range of mission objectives. They lack sufficient detail describing how to apply cyberspace influence in the *Shape*, *Deter*, *Stabilize*, and *Enable Civil Authority* phases where Internet freedom initiatives play the greatest role.

Specifically, cyberspace doctrine should acknowledge the importance of providing communications capabilities as well as circumvention tools during the *Shape* and *Deter* phases. At the physical layer, the military can expand access to the Internet by providing the basic information infrastructure and the ways for individuals to connect to that communications backbone. In the early phases of a campaign, the military could leverage existing terrestrial, airborne and satellite communications assets and make them available to oppressed peoples. This strategy may require the DOD to invest in end-user connection devices, such as laptops, handsets, radios, satellite dishes or cell phones to enable the target populace to gain access to the communication channel. Planners would have to apportion these assets to the task and logisticians would be required ensure that the necessary connection devices could be distributed to those in need. Additional security measures may also be required to protect the identity and safety of those who access the network this way, since in doing so they may be violating their host government's regulations.

In addition to physical infrastructure, the DOD needs software tools and applications for combating information oppression and censorship. When new physical connections are not practical or possible, then the military must employ ways to help the oppressed circumvent the controls inherent in their own networks. Encryption technology, software and content alternatives, proxy servers and education programs are some of the most basic requirements. The reader is encouraged to review the detailed description of the range of possible approaches to circumvention provided in Chapter 1.

Careful planning and acquisition during these early phases of operations may also help in the latter phases. Hopefully, most campaigns will not escalate to hostility; but if they do, the military should prepare in advance for the necessary social and governmental capabilities that will be required after the *Dominate* phase. If it is advantageous for preserving a more lasting peace, military communications infrastructures can be left in place to support the transition back to normalcy. Especially in underdeveloped nations, leaving a robust communications infrastructure behind after hostilities conclude, such as communications networks, data centers and power generation equipment, can help promote stability, governance and economic growth in the post-conflict environment. The military may even support the host nation with technical and managerial expertise until the government can provide those services indigenously.

The DOD will also require professionals skilled in strategic communications and countering propaganda. As has been covered throughout, the character of censorship is evolving away from simply blocking and filtering at the syntactic layer of the Internet. Authoritarian governments are increasingly turning to third-generation controls that work by combating the message itself through targeted propaganda, counter-information campaigns and the flooding of the medium with pro-

regime content. The DOD must be prepared to not only engage oppression with force and technical skill, but also with information and agile communication.

Conclusion

By implementing these objectives, the nation and, in particular, the DOD will be better equipped to promote universal freedom of expression. While the US must still remain vigilant with respect to cyberspace threats it must not become so focused on the threats that it loses site of its values. Promoting American values through cyberspace requires a comprehensive influence strategy. Through expanded awareness, careful coordination and purposeful planning, the DOD, in conjunction with other government agencies and private interest groups, can promote this ideal throughout the world.

Conclusion

You and I, my dear friend, have been sent into life at a time when the greatest lawgivers of antiquity would have wished to live. How few of the human race have ever enjoyed an opportunity of making an election of government… for themselves or their children!

– John Adams

It may not turn out to be a revolution in the end, but whatever it is, it altered the status quo faster than anyone could have imagined previously.

– Jon Alterman

Democracies do not fear freedom, they embrace it. They embrace it not just for themselves, but for all of humanity because freedom and peace tend to reinforce each other. This is an inherent aspect of American foreign policy. As the 2010 *National Security Strategy* proclaims, "Political systems that protect universal rights are ultimately more stable, successful and secure."[1] Basic human rights must be protected at home and abroad to ensure a more peaceful global order.

The Internet is a technological and social marvel for facilitating communication and promoting one of the most basic human rights, freedom of expression. In its purest form, its low barriers to access and globally distributed infrastructure have leveled the playing field between individuals, organizations, societies and states. All can have a voice and all can participate in the exchange of ideas. Yet, the purity of freedom for the many can be corrupted by the avarice of the few. Authoritarian political systems often suppress truth to consolidate power. They attempt to stifle the exchange of information to keep dissention in check and to maintain control.

Many modern authoritarian regimes are trying to exert the same forms of influence in cyberspace, but the scope and scale of this medium may be too great for them to employ their traditional tactics of repressive

[1] White House. "National Security Strategy of the United States of America," 37.

governance. What was once a strategic strength of dictators is being undermined by the new character of information exchange. Their attempts to control information have become their biggest strategic vulnerability. This strategic vulnerability creates a tremendous opportunity for those who wish to promote freedom and democracy. Enhancing access to information technologies and facilitating freedom of expression for those living under oppression will help them participate in their own political self-determination. While early predictions about the role of information technology in upsetting authoritarianism may have been premature, perhaps the modern communications environment has reached the tipping point where the values enshrined in America's First Amendment can finally flourish around the world. Lawrence Lessig sees this as the case:

> This debate has gone on at the political level for a long time. And yet, as if under cover of night, we have now wired these nations with an architecture of communication that builds within their borders a far stronger First Amendment than our ideology ever advanced. Nations wake up to find that their telephone lines are tools of free expression, that e-mail carries news of their repression far beyond their borders, that images are no longer the monopoly of state-run television stations but can be transmitted from a simple modem. We have exported to the world, through the architecture of the Internet, a First Amendment more extreme in code than our own First Amendment in law.[2]

If Lessig is correct, then the Internet may be the ideal pathway for democratic nations to exert pressure on authoritarian regimes to either reform or risk the consequences of a popular uprising. Some have called this the "Dictator's Dilemma."[3] Taylor Boas, writing in *The Washington Quarterly*, summed up the quandary of authoritarian regimes as follows:

---

[2] Lessig, *Code: Version 2.0*, 236.
[3] Morozov, *The Net Delusion*, 93.

> Authoritarian leaders in the Information Age are confronted with an unmistakable dilemma. On the one hand, the Internet and associated information and communication technologies offer enormous economic potential for developing countries, and the increasingly interconnected global economy thrives on openness of information. On the other hand, the information revolution poses new challenges for regimes that rely on centralized political control.[4]

Unfortunately, the last few years have produced ample evidence of authoritarian regimes coming down on the side of oppression rather than reform. Many authoritarians have demonstrated their fear of losing control by the extreme measures they employ to suppress or negate the flow of information to their own people. In some cases, this strategic error ushered in their downfall. In others, the regime retained its power, but only time will tell how long repression will remain a viable option in the face of mounting popular pressure for reform.

This is not to imply that there is a direct causality between Internet freedom and overcoming oppression. In most cases, freedom of expression is a necessary, but not sufficient, condition for self-determination. Rather, recent events demonstrate how authoritarian regimes recognize that freedom of expression is a necessary condition of self-determination; therefore, they believe that they can retain power by denying freedom of expression to their people. The actions of authoritarian regimes show how vital information control to their strategy. The actions of people living under authoritarian control demonstrate how much they value freedom of expression. Democratic nations wishing to promote universal freedom of expression can exploit the state of modern information technology and capitalize on this strategic vulnerability of authoritarians. The Internet Age seems balanced in favor of the people over their oppressors.

---

[4] Taylor C. Boas, 2000. "The dictator's dilemma? The Internet and US policy toward Cuba," *Washington Quarterly*, volume 23, number 3(Summer), pp. 57-67.

For example, by 2011, the population of Egypt was determined to change its dreadful economic situation. The youth unemployment rate had reached 25 percent and annual inflation had soared to 10 percent.[5] Adding to the unrest, then President Hosni Mubarak steered the election in his own favor despite the growing opposition to his government's direction. Many, such as Google executive Wael Ghoneim, used social media to help organize protest movements. Ghoneim created a Facebook group dedicated to the memory of an Internet activist beaten to death by Egyptian police. When the protests began on 25 January, the group had nearly a half-million members.[6] This and other movements organized through social media have helped spurn activism in conjunction with support from traditional broadcast media sources. Fearing the conditions were growing out of his control, Mubarak shut down Internet access inside his borders, shuttered texting services and turned off Al-Jazeera's operations in the country.[7] He attempted to draw from the traditional playbook of authoritarians by suppressing information, but information technology proved too capable to be bottled up. Through "peer-to-peer networking and grassroots innovation,"[8] the Egyptian people used social media and user-generated content to become activists and to exercise self-determination. As a result of their efforts, Mubarak was forced to step down after a 30-year reign.

Another example is the recent revolt in Libya. Almost immediately after the Egyptian people were successful in ousting their long-standing president, Libyans with the same goal began a similar undertaking. Peaceful protests started in February 2011, but Libyan dictator Muammar Gaddafi quickly took measures to suppress the dissidents. His government responded with aggressive military force, censorship and

[5] Alterman, "The Revolution Will Not Be Tweeted," 108.
[6] Alterman, "The Revolution Will Not Be Tweeted," 110.
[7] Alterman, "The Revolution Will Not Be Tweeted," 112.
[8] Alterman, "The Revolution Will Not Be Tweeted," 113.

communications blocking to limit anti-government protests. The first blackout of the Libyan Internet occurred on 18 February, but lasted only 7 hours.[9] Then, the regime initiated a more complete and lasting blackout on 2 March. Libyan access to the Web went dark and stayed that way until mid-July as rebel forces slowly took control of key cities in the country.[10] After six months of conflict, on 22 August, Tripoli fell from the grip of the Gaddafi regime. In a testament to the importance of digital communication to the Libyan people, the Internet and mobile messaging services in the country were restored almost immediately after the rebels reclaimed the capital city. The nation's ISP, Libyan Telecom and Technology, posted this message on its webpage: "Congratulations, Libya, on emancipation from the rule of the tyrant."[11]

Figure 3 provides a visible depiction of Libyan censorship over the period.[12] It comes from data captured by Google and it shows the pattern of Internet activity coming from and going to addresses in Libya. It displays the regime's initial response to the uprisings in mid-February followed by the complete crackdown on digital communication in early March. It also shows how rapidly the Internet came back to life after the Gaddafi regime fell. The dictator's era ended after 40 years of oppression. He erred on the side of control rather than freedom, and it eventually cost him his life.

---

[9] Amanda Cosco, "Libyan Internet Blackouts Feel Like A 'Post-Apocalyptic Scenario'," *Social Times*. 9 March 2011, http://socialtimes.com/libyan-internet-blackouts-feel-like-a-post-apocalyptic-scenario_b41300 (accessed 30 March 2012).
[10] Google. "Transparency Report: Libya," http://www.google.com/transparencyreport/traffic/?r=LY&l=EVERYTHING&csd=1297962000000&ced=1300381200000 (accessed 6 April 2012).
[11] James Cowie, "The Battle for Tripoli's Internet," *Renesys*, 21 August 2011, http://www.renesys.com/blog/2011/08/the-battle-for-tripolis-intern.shtml (accessed 6 April 2012).
[12] Google. "Transparency Report: Libya."

Figure 3. Google Transparency Report on Libyan Internet Traffic

Source: Google. "Transparency Report: Libya," http://www.google.com/transparencyreport/traffic/?r=LY&l=EVERYTHING&csd=1297962000000&ced=1300381200000 *(accessed 6 April 2012).*

Finally, China's current situation is the embodiment of the Dictator's Dilemma. On the economic side, the Chinese government wants to maintain its pace of growth by continuing to adopt Western technology and capitalism. While its economy is becoming more open, its politics are not. It still holds to Leninist-style communism under single-party rule.[13] Freedom House has consistently given China its lowest ranking in the Political Rights category and labeled the country as "Not Free" in its survey of freedom around the world.[14] Despite China's tremendous potential, the Chinese government finds itself in a struggle between progress and control, and it often comes down on the side of the latter.

The potential ramifications of the popular uprisings in Egypt and Libya were not lost on the Chinese government. Fearing similar movements within China, Chinese authorities responded with "a near-hysterical campaign of arrests, incommunicado detentions, press

[13] Milton L. Mueller, "China and Global Internet Governance," *Access Contested: Security, Identity, and Resistance in Asian Cyberspace Information Revolution and Global Politics*, Ronald Deibert et al., eds. (Cambridge, MA: The MIT Press, 2012), 190.
[14] Freedom House. "Freedom in the World 2012: The Arab Uprisings And Their Global Repercussions," http://www.freedomhouse.org/sites/default/files/inline_images/FIW%202012%20Booklet--Final.pdf. 14. (accessed 3 April 2012).

censorship, and stepped-up control over the Internet."[15] Rather than engage with their population in the political process, the Chinese government ramped up Internet censorship, suppressed minorities and sought to eliminate political dissent. In particular, they repressed all public discussion of Arab movements regarding democracy and prosecuted many social media commentators and human rights activists who violated their policies.[16]

This most recent occurrence of political oppression is only the latest example in a history of similar activities by the Chinese government. In 2008, on the anniversary of the 1959 Tibetan Uprising, the Chinese government clamped down on foreign and domestic media sources and escalated its targeted Internet censorship campaign in the wake of Tibetan protests for human rights, religious freedom and political independence.[17] In 2009, the government completely shut down the Internet and telephone access in the province of Xinjiang and blocked Facebook, Twitter and other social media sites nationwide in the wake of civil unrest in the region.[18] In an attempt to craft a favorable narrative, Chinese authorities allowed foreign media to cover the riots, but confined journalists to the urban areas and only permitted them to report on violence instigated by the citizens. China retained its lockdown on Internet access in Xinjiang for ten months.[19] As these examples highlight, Chinese government officials are fearful of the free flow of information. Hopefully, as they continue to see the benefits of a more open economy, they will also recognize the benefits of a freer society.

---

[15] Freedom House, "Freedom in the World 2012," 1.
[16] Freedom House, "Freedom in the World 2012," 6.
[17] OpenNet Initiative, "ONI Country Profile: China," *Access Contested: Security, Identity, and Resistance in Asian Cyberspace Information Revolution and Global Politics*, Ronald Deibert et al., eds. (Cambridge, MA: The MIT Press, 2012), 273.
[18] Rebekah Heacock, "China Shuts Down Internet in Xinjiang Region After Riots," 6 July 2009 http://opennet.net/blog/2009/07/china-shuts-down-internet-xinjiang-region-after-riots (accessed 6 April 2012).
[19] OpenNet Initiative, "ONI Country Profile: China," 273.

At a fundamental level, most have embraced the recent surge of citizens demanding more political freedom as a positive demonstration of basic human rights. Yet, there is still apprehension over the potential outcomes of these uprisings at the practical level. The Arab Spring has given many people hope for a better future, but hope is not a guarantee. It is still unclear whether the future governments of Tunisia, Egypt, Libya or Syria will serve their populations better than they have in the past. Therefore, the debate over the benefits of promoting Internet freedom will continue for the foreseeable future.

Where one comes down in the debate over the benefits versus risk of Internet freedom initiatives depends on whether one sees technology as having fundamentally changed the nature of freedom. As this thesis has covered, it is more likely that only the character of freedom has changed with the advent of modern information technologies. While nations must balance freedom and security as they always have, the essential nature of freedom is the same. Freedom can be messy. Freedom will come with challenges. There will be highs and lows, but the balance will always tip in favor of freedom's benefits. In the aggregate, freedom reigns. Nations must have a resolute faith in these qualities of freedom. At the foundational level, it will be less about a calculated, quantitative decision over whether or not to advance the cause of human rights, and more about a qualitative belief in their universal applicability and benefit. The complexity of the modern information technology environment requires a bit of faith in addition to pragmatism. Zittrain and Palfrey recognized this when they wrote:

> [It] boils down to a belief in the value of a relatively open information environment because of the likelihood that it can lead to a beneficial combination of greater access to information, more transparency, better governance, and faster economic growth. The Internet, in this sense, is a generative network in human terms. In the hands of the

> populace at large, the Internet can give rise to a more empowered, productive citizenry.[20]

Modern information technology presents free nations with a strategic opportunity. It can give a voice to the voiceless and empower the weak. Free nations should not lose sight of this opportunity even as they struggle with the challenges of a massively connected global society. They should purposefully embrace modern technology as a way to promote freedom of expression and self-determination around the world. They should do so because democracies thrive on the benefits of freedom. Authoritarian states do not. Democracies are resilient to the challenges associated with freedom. Authoritarian states are not. Walter Wriston was correct when he wrote:

> No government, no matter how repressive or authoritarian, can over time stand in opposition to what Jefferson called "a decent respect to the opinions of mankind." No one should be naïve enough to believe that the totalitarian powers of the world will give up easily… But information is the virus that is carrying the powerful idea of freedom to the four corners of the world, and modern technology assures that sooner rather than later everyone on the planet will have heard the message.[21]

[20] Zittrain and Palfrey, "Internet Filtering," 51.
[21] Wriston, *The Twilight of Sovereignty*, 173-174.

Bibliography

Articles

Allnutt, Luke. "Twitter Doesn't Start A Revolution, People Do." Christian Science Monitor. February 8, 2010. http://www.csmonitor.com/Commentary/Opinion/2010/0208/Twitter-doesn-t-start-a-revolution-people-do (accessed 17 April 2012).

Alterman, Jon B. "The Revolution Will Not Be Tweeted." The Washington Quarterly, 34.4 (2011).

Amazon, "Amazon EC2 Pricing," http://aws.amazon.com/ec2/pricing/ (accessed 30 March 2012).

Atran, Scott. *Talking to the Enemy: Faith, Brotherhood, and the (un)making of Terrorists*. New York: Ecco, 2010. p. 233.

Barlow, John P. "A Declaration of the Independence of Cyberspace," 8 February 1996, https://projects.eff.org/~barlow/Declaration-Final.html (accessed 22 February 2012).

Betz, David J. and Tim Stevens, *Cyberspace and the State: Toward a Strategy For Cyber-Power*. Kindle Ed. New York: Routledge, 2012.

Boas, Taylor C. "The dictator's dilemma? The Internet and US policy toward Cuba," Washington Quarterly, volume 23, number 3 (Summer) (2000).

Brinton, Crane. *The Anatomy of Revolution*. Revised ed. New York: Vintage, 1965

Broadcasting Board of Governors. BBG 2009 Annual Report. http://media.voanews.com/documents/09anrprt.pdf (accessed 26 March 2012).

Broadcasting Board of Governors. "BBG Strategic Plan 2012-2016," February 2012, http://www.bbg.gov/wp-content/media/2012/02/BBGStrategicPlan_2012-2016_OMB_Final.pdf (accessed 26 March 2012).

Broadcasting Board of Governors, "Frequently Asked Questions," http://www.bbg.gov/about-the-agency/history/faqs/ (accessed 26 March 2012).

Broadcasting Board of Governors. "Program Delivery Overview," July 2010. http://media.voanews.com/documents/Engineering_FactSheet_7_101.pdf (accessed 26 March 2012).

Bush, George W. "Remarks by the President from the USS Abraham Lincoln." Delivered May 1, 2003. http://georgewbush-whitehouse.archives.gov/news/releases/2003/05/20030501-15.html (accessed 7 April 2012).

Chance, Paul. *Learning and Behavior: Active Learning Edition*. 6th ed. Belmont, CA: Wadsworth Publishing, 2009.

Clausewitz, Carl Von. *On War*. ed. and trans. Michael Howard and Peter Paret. Princeton: N.J.: Princeton University Press, 1976.
Clinton, Hillary. "Remarks on Internet Freedom," 21 January 2010, http://www.state.gov/secretary/rm/2010/01/135519.htm (accessed 20 March 2012).
Clinton, Hillary. "Message for Youth Movement Summit," 16 October 2009, http://video.state.gov/en/video/45067767001/message-for-youth-movement-summit/s~creationDate/p~1/?s=YWxsaWFuY2Ugb2YgeW91dGg (accessed 30 March 2012).
Cosco, Amanda. "Libyan Internet Blackouts Feel Like A 'Post-Apocalyptic Scenario'" *Social Times*. 9 March 2011, http://socialtimes.com/libyan-internet-blackouts-feel-like-a-post-apocalyptic-scenario_b41300 (accessed 30 March 2012).
Cowie, James. "The Battle for Tripoli's Internet," *Renesys*, 21 August 2011, http://www.renesys.com/blog/2011/08/the-battle-for-tripolis-intern.shtml (accessed 6 April 2012).
Cronin, Audrey K. *How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns*. New York: Princeton University Press, 2011
Deibert, Ronald, John Palfrey, Rafal Rohozinski and Jonathan Zittrain, "Access Contested: Toward the Fourth Phase of Cyberspace Controls," *Access Contested: Security, Identity, and Resistance in Asian Cyberspace Information Revolution and Global Politics*, Ronald Deibert et al., eds., Cambridge, MA.: The MIT Press, 2012
Deibert, Ronald and Rafal Rohozinski, "Control and Subversion in Russian Cyberspace," *Access Controlled: the Shaping of Power, Rights, and Rule in Cyberspace*, Ronald Deibert et al. eds., Cambridge, Mass.: The MIT Press, 2010
Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," July 2011.
Department of Defense, "Joint Publication 1: Doctrine for the Armed Forces of the United States," Change 1, 20 March 2009.
Department of Defense, "Joint Publication 3-0: Joint Operations," 11 August 2011.
Department of Defense, "Joint Publication 3-08: Interorganizational Coordination During Joint Operations," 24 June 2011.
Department of Defense, "Joint Publication 3-13: Information Operations," 13 February 2006.
Department of Defense, "The National Military Strategy of the United States of America," 2011.
Department of Homeland Security, "National Infrastructure Protection Plan," 2009.
Department of Homeland Security, "Quadrennial Homeland Security Review," February 2010.

Department of State, "Factsheet: State Department Internet Freedom Programs," 8 December 2012, http://www.humanrights.gov/wp-content/uploads/2011/12/20111208-FactSheet-InternetFreedomPrograms.pdf (accessed 26 March 2012).
Department of State, "Internet Freedom," 15 February 2012, http://www.state.gov/r/pa/prs/ps/2011/02/156623.htm (accessed 26 March 2012).
Dolman, Everett. *Pure Strategy: Power and Policy in the Space and Information Age (Strategy and History)*, New ed. New York: Routledge, 2005.
Doyle, Michael W. *Ways of War and Peace: Realism, Liberalism, and Socialism*. New York: W. W. Norton & Company, 1997.
Encyclopedia Britannica, *Great Books #23 - Machiavelli – Hobbes*. University of Chicago, 1952.
Faris, Robert and Nart Villeneuve, "Measuring Global Internet Filtering," *Access Denied: the Practice and Policy of Global Internet Filtering*, Ronald Deibert et al., eds., Cambridge, MA.: The MIT Press, 2008.
Franklin, William Temple. *Memoirs of the Life and Writings of Benjamin Franklin*. London: H. Colburn, 1818.
Freedom House. "Freedom in the World 2012: The Arab Uprisings And Their Global Repercussions," http://www.freedomhouse.org/sites/default/files/inline_images/FIW%202012%20Booklet--Final.pdf (accessed 3 April 2012)
Gladwell, Malcolm. "Small Change: Why the revolution Will Not be Tweeted," *The New Yorker*, 4 October 2010, http://www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell (accessed 8 April 2012).
Gleick, James. *The Information: a History, a Theory, a Flood*. New York: Pantheon, 2011.
Global Network Initiative, "Frequently Asked Questions," https://www.globalnetworkinitiative.org/faq/index.php (accessed 26 March 2012).
Global Network Initiative. "Global Network Initiative," https://www.globalnetworkinitiative.org/index.php (accessed 30 March 2012).
Global Network Initiative. "Who We Are. What We Do. Why It Matters." https://www.globalnetworkinitiative.org/cms/uploads/1/GNI_WhoWhatWhere_1.pdf (accessed 30 March 2012).
Google. "Transparency Report: Libya" http://www.google.com/transparencyreport/traffic/?r=LY&l=EVERYTHING&csd=1297962000000&ced=1300381200000 (accessed 6 April 2012).
Greenberg, Andy. "Porn-Surfing By Proxy." *Forbes*, May 30, 2007. http://www.forbes.com/2007/05/30/psiphon-server-censorship-tech-intel-cx_ag_0530techpsiphon.html (accessed 6 April 2012).

Heacock, Rebekah. “China Shuts Down Internet in Xinjiang Region After Riots,” 6 July 2009 http://opennet.net/blog/2009/07/china-shuts-down-internet-xinjiang-region-after-riots (accessed 6 April 2012).
Helmuth von Moltke, *Moltke On the Art of War: Selected Writings*. ed. Daniel Hughes. New York: Presidio Press, 1995.
Internet World Stats. “Internet Growth Statistics,” http://www.internetworldstats.com/emarketing.htm (accessed 15 Feb 2012).
Kidder, Rushworth M. *How Good People Make Tough Choices Rev Ed: Resolving the Dilemmas of Ethical Living*. Rev Upd ed. Harper Perennial, 2009.
Knafo, Saki. “Anonymous And The War Over The Internet,” *The Huffington Post*, 30 January 2012, http://www.huffingtonpost.com/2012/01/30/anonymous-internet-war_n_1233977.html (accessed 8 April 2012).
Kurose, James F. and Keith W. Ross. *Computer Networking: a Top-Down Approach*. 5th ed. Boston: Addison Wesley, 2010.
Lessig, Lawrence. *Code: Version 2.0*. 2nd ed. New York, USA.: Basic Books, 2006.
Levine, Rick et al., *The Cluetrain Manifesto: The End of Business as Usual*. Da Capo Press, 2001.
Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. New York, NY: Cambridge University Press, 2007.
Lonsdale, David J. *The Nature of War in the Information Age: Clausewitzian Future (Strategy and History)*. London: Routledge, 2004.
Lord, Kristin M. *The Perils And Promise of Global Transparency: Why the Information Revolution May Not Lead to Security, Democracy, or Peace*. Suny Series in Global Peace. annotated edition ed. Albany, NY: State University of New York Press, 2007.
Mackinlay, John. *The Insurgent Archipelago: from Mao to Bin Laden*. New York: Columbia University Press, 2010.
MacKinnon, Rebecca. “Corporate Accountability in Networked Asia,” *Access Contested: Security, Identity, and Resistance in Asian Cyberspace Information Revolution and Global Politics*, Ronald Deibert et al., eds., Cambridge, MA.: The MIT Press, 2012.
McDougall, Walter A. *… The Heavens and the Earth: A Political History of the Space Age*. Baltimore and London: Johns Hopkins University Press, 1997.
Molander, Roger C., Andrew S. Riddile, and Peter A. Wilson, *Strategic Information Warfare: a New Face of War*. Santa Monica, CA.: Rand Publishing, 1996.

Morozov, Evgeny. *The Net Delusion: the Dark Side of Internet Freedom*. New York: PublicAffairs, 2011.
Movements.org, "Mission," http://www.movements.org/pages/mission (accessed 30 March 2012)
Mueller, Milton L. "China and Global Internet Governance," *Access Contested: Security, Identity, and Resistance in Asian Cyberspace Information Revolution and Global Politics*, Ronald Deibert et al., eds., (Cambridge, MA.: The MIT Press, 2012)
Murdoch, Steven J. and Ross Anderson, "Tools and Technology of Internet Filtering," *Access Denied: the Practice and Policy of Global Internet Filtering*, Ronald Deibert et al., eds., Cambridge, MA.: The MIT Press, 2008.
Nardi, Tom. "Low Orbit Ion Cannon: Exposed," *The Power Base*, 4 March 2012, http://www.thepowerbase.com/2012/03/low-orbit-ion-cannon-exposed/. (accessed 30 March 2012).
Office of the United Nations High Commissioner For Human Rights, "International Covenant on Civil and Political Rights," http://www2.ohchr.org/english/law/ccpr.htm#art19 (accessed 19 March 2012).
Olsen, John A. *John Warden and the Renaissance of American Air Power*. Washington, D.C.: Potomac Books Inc., 2007.
OpenNet Initiative, "ONI Country Profile: China," *Access Contested: Security, Identity, and Resistance in Asian Cyberspace Information Revolution and Global Politics*, Ronald Deibert et al., eds., Cambridge, MA.: The MIT Press, 2012
Orwell, George. "You and the Atom Bomb," *Tribune*, 19 October 1945.
Radio Free Asia, "Getting Around Internet Blockage" http://www.rfa.org/english/about/help/web_access.html (accessed 13 March 2012).
Ramasoota, Pirongrong. "Internet Politics in Thailand after the 2006 Coup," *Access Contested: Security, Identity, and Resistance in Asian Cyberspace Information Revolution and Global Politics*, Ronald Deibert et al., eds., Cambridge, MA.: The MIT Press, 2012.
Reagan, Ronald. "Reagan Urges 'Risk' on Gorbachev: Soviet Leader May Be Only Hope for Change, He Says." Los Angeles Times, June 13, 1989, http://articles.latimes.com/1989-06-13/news/mn-2300_1_soviets-arms-control-iron-curtain (accessed 8 April 2012).
Roberts, Hal and John Palfrey, "The EU Data Retention Directive in an Era of Internet Surveillance," *Access Contested: Security, Identity, and Resistance in Asian Cyberspace Information Revolution and Global Politics*, Ronald Deibert et al., eds., Cambridge, MA.: The MIT Press, 2012
Roberts, Hal, Ethan Zuckerman, and John Palfrey, "Interconnected Contests," *Access Contested: Security, Identity, and Resistance in*

Asian Cyberspace Information Revolution and Global Politics, Ronald Deibert et al., eds., Cambridge, MA.: The MIT Press, 2012

Roosevelt, Franklin. "Transcript of President Franklin Roosevelt's Annual Message (Four Freedoms) to Congress (1941)," 6 January 1941, http://www.ourdocuments.gov/doc.php?flash=true&doc=70&page=transcript (accessed 20 March 2012).

Rundle, Mary and Malcolm Birdling, "Filtering and the International System," *Access Denied: the Practice and Policy of Global Internet Filtering*, Jonathan L. Zittrain et al., eds., Cambridge, MA.: The MIT Press, 2008.

Schmitt, Eric and Thom Shanker. *Counterstrike: the Untold Story of America's Secret Campaign Against Al Qaeda*. (New York: Times Books, 2011)

Seidensticker, Bob. *Future Hype: the Myths of Technology Change*. Berkeley, CA: Berrett-Koehler Publishers, 2006.

Shapiro, Carl and Hal R. Varian. *Information Rules: a Strategic Guide to the Network Economy*. Boston, Mass.: Harvard Business Review Press, 1999.

Skinner, B. F. *Science And Human Behavior*. Free Press, 1965.

Skoudis, Ed and Tom Liston. *Counter Hack Reloaded: a Step-by-step Guide to Computer Attacks and Effective Defenses*. 2nd ed. Upper Saddle River, NJ: Prentice Hall, 2006.

Stableford, Dylan. "As Wikipedia Goes Dark to Protest SOPA, Media Offer Support," *Yahoo! News*, 18 Jan 2012. http://news.yahoo.com/blogs/cutline/wikipedia-goes-dark-protest-sopa-media-offer-support-154353847.html (accessed 8 April 2012).

Tor, "Anonymity Online," https://www.torproject.org/ (accessed 23 February 2012).

United Nations, "The Drafters Of The Universal Declaration Of Human Rights," http://www.un.org/en/documents/udhr/drafters.shtml (accessed 19 March 2012).

United Nations, "The Foundation Of International Human Rights Law," http://www.un.org/en/documents/udhr/hr_law.shtml (accessed 19 March 2012).

United Nations, "History of the Document," http://www.un.org/en/documents/udhr/history.shtml (accessed 19 March 2012).

United Nations, "Treaty Collection," http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en (accessed 19 March 2012).

United Nations, "The Universal Declaration of Human Rights," http://www.un.org/en/documents/udhr/index.shtml (accessed 19 March 2012).

United States, "Declaration of Independence," 4 July 1776. http://www.archives.gov/exhibits/charters/declaration_transcript.html (accessed 8 April 2012).
United States, "The Constitution of the United States of America," 17 September 1778. http://www.archives.gov/exhibits/charters/constitution_transcript.html (accessed 8 April 2012).
United States Air Force, "Air Force Doctrine Document 3-12: Cyberspace Operations," Change 1, 30 November 2011.
White House, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," May 2009.
White House, "International Strategy for Cyberspace," May 2011.
White House. "National Security Strategy of the United States of America." May 2010.
Worldwidewebsize.com. "Daily Estimated Size of the World Wide Web," http://www.worldwidewebsize.com/ (accessed 23 February 2012).
Wriston, Walter B. *The Twilight of Sovereignty: How the Information Revolution Is Transforming Our World*. New York: Scribner, 1992.
Yarger, Harry R. *Strategy and the National Security Professional: Strategic Thinking and Strategy Formulation in the 21st Century*. Westport, CT.: Praeger, 2008.
Zhao, Shanyang, Sherri Grasmuck and Jason Martin, "Identity construction on Facebook: Digital empowerment in anchored relationships," *Computer Human Behavior,* Vol. 24 (September 2008), pp. 1816-1836.
Zittrain, Jonathan, and John Palfrey, "Internet Filtering: The Politics and Mechanisms of Control," *Access Denied: the Practice and Policy of Global Internet Filtering*, Jonathan L. Zittrain et al., eds., Cambridge, MA.: The MIT Press, 2008.
Zuckerman, Ethan. "Internet Freedom: Beyond Circumvention." February 22, 2010. http://www.ethanzuckerman.com/blog/2010/02/22/internet-freedom-beyond-circumvention/ (accessed 6 April 2012).