Information sovereignty

Benjamin Peter Hagen
Iowa State University

Follow this and additional works at: https://lib.dr.iastate.edu/rtd

Recommended Citation
Hagen, Benjamin Peter, "Information sovereignty" (2004). Retrospective Theses and Dissertations. 20565. https://lib.dr.iastate.edu/rtd/20565

This Thesis is brought to you for free and open access by the Iowa State University Capstones, Theses and Dissertations at Iowa State University Digital Repository. It has been accepted for inclusion in Retrospective Theses and Dissertations by an authorized administrator of Iowa State University Digital Repository. For more information, please contact digirep@iastate.edu.
Information sovereignty

by

Benjamin Peter Hagen

A thesis submitted to the graduate faculty
in partial fulfillment of the requirements for the degree of
MASTER OF SCIENCE

Major: Information Assurance

Program of Study Committee:
Steffen Schmidt, Major Professor
James McCormick
Thomas Daniels

Iowa State University
Ames, Iowa
2004

Copyright © Benjamin Peter Hagen, 2004. All rights reserved.
Graduate College
Iowa State University

This is to certify that the master's thesis of

Benjamin Peter Hagen

has met the thesis requirements of Iowa State University

Signatures have been redacted for privacy
TABLE OF CONTENTS

CHAPTER 1. INTRODUCTION
   Introduction 1
   Information Control 1
   A “Paradigm” Shift 2
   Information Control and the Internet 6
   Political Models 8
      The Realist Model 8
      The Liberal Model 9
      A Convergence 10
   A Question of Sovereignty? 11
   CIA 13
   Current Situation 16
      Statistics 16
      Internet Restriction (Chart: Countries & Internet Restriction) 17

CHAPTER 2. A TECHNOLOGY REGIME 19
   Introduction 19
      A Brief History of the Internet 19
   International Standards Regime 21
   Packets & Switches 24
   A Network of Neighbors 26
   Unobvious Content 28
      Levels of Connection 28

CHAPTER 3. REGIME ACCEPTANCE 31
   Pressure from Market Forces 31
   Security 31
   Transparency 32
Stability 33
Sovereignty 33

CHAPTER 4. CASE STUDIES 34
China 34
   Government Restrictions 34
   The Firewall 35
Saudi Arabia 37
USA 40

CHAPTER 5. CONCLUSION 42
Regime 42
Contributing Factors 44
   Population 44
   Economy 45
   Government Regime Type 47
   A General Relationship 48
The Impact of Information Sovereignty 49
Future Considerations 49
   Bypassing Software 49
   Arms Race 51
   "Laws of Censorship" 51
   A New Taxonomy 53
Conclusion 53

REFERENCES 55
CHAPTER 1. INTRODUCTION

Introduction

This thesis seeks to explore the relationship between information technologies, specifically the Internet, and the nation-state system and answer several important questions which impact the sovereignty of information: How does the Internet differ from previous forms of communication and media? How do these differences impact the sovereignty of information within the nation-state system? What has been the reaction of the nation-state to the Internet? What factors affect the nation-state’s decision to place controls on Internet access?

Chapter one of this thesis examines the Internet as a fundamental shift in the communications capability of humankind and argues that the Internet can be considered as a technology and standards regime which ensures the interoperability and technical standards of domestic computer networks that connect to the global Internet. An examination of the technological background of the Internet is presented in chapter two. This examination suggests that this new form of communication impacts the sovereign ability of the nation-state to control the flows of information both within and across its borders. Chapter three examines the role which international markets play in promoting the Internet regime. Markets desire compliance with the international regime in order to ensure transparency, security, and stability. Nation-states make a rational cost/benefits decision on the form which networking takes within their domestic boundaries and on what controls are placed upon access to the network. There have been varied and diverse responses to the question of network access; from national firewalls and strictly controlled access privileges, to legislative barriers and freedom of information movements. Chapter four introduces case studies of internet controls in China, Saudi Arabia, and the US as examples of three different levels of control. Finally chapter five presents aggregate data which indicates a relationship between nation-state controlled access to the Internet and several different economic and social factors including: user populations, per-capita income, and high-technology imports.
Information Control

Nation states want to have control over the flows of information. The fundamental operations of the modern nation state rely upon its ability to control information. Voting, trade, taxes, education, transportation, and security all depend at some level upon the movement of information. With the proliferation of Internet access across the world the nation’s traditional ability to control information has come into question. In many parts of the world state control of the Internet is a modern reality. China, North Korea, Cuba, and Saudi Arabia are just a few of the states with established methods of controlling what information their citizens are able to access on the Internet. Yet some states choose not to limit access at all; the reactions of states are varied and diverse. Despite a strong desire to maintain an ability to control information, nation states have ceded much of their control to modern forms of information technology; in particular the Internet. Why do some states choose to control access while others do not?

A “Paradigm” Shift

Within recent years the Internet has become one of humankind’s most powerful tools for information gathering and communication. It allows users connected at any point on the network to access a wealth of information on a truly diverse set of topics. Moreover this new medium is not limited to a one way flow of information. Once connected to the network, most users have the ability to not only receive information, but also transmit it. This bidirectional capability to both receive and transmit information creates a wealth of possibilities not yet realized by more traditional forms of media and communication.

Ancient movements of information occurred simultaneously with the movement of the human body. As peoples crossed the great spaces of Earth so did their knowledge, histories, and understanding. Before the development of sophisticated and versatile forms of verbal communication humans were relegated to simplistic forms of information transfer. Those with knowledge could only spread it to those with the time and desire to learn through local and locally understood language. The movement of information was dependent upon the movements of people.

With the widespread adoption of consistent languages across large populations humans could transfer ideas away from their source with increased speed and distance. A
new technique for farming could be passed from farmer to farmer until its spread met a limit of practicality or physicality. A mountain could stop information if there was no one willing to cross it — or if there was no one on the other side who could understand the message once it arrived. Language allowed information to be passed away from the source.

With the development of written forms of communication ideas could be passed more precisely than through verbal forms. As verbal messages cross human minds their messages invariably shift away from their original meaning. Written forms of communication are more permanent and persistent. Moreover copies can be made which are almost identical to the original. Written language allowed information to become archived and duplicated with great accuracy.

The mechanical printing press brought written communication to a mass audience. This technology demoted human labor to a minimum role in the duplication of information; machines did most of the physical work. The printing press allowed ideas to flow to large numbers of people and significantly reduced the cost associated with producing mass quantities of written material.

Early forms of electronic communication such as the telegraph greatly increased the speed and distance at which human communication could occur. The only limit to a message’s final destination was the existence of infrastructure capable of relaying the message and trained operators with the ability to understand it. The telephone brought the capability for easy, near instantaneous, two way communication to much of the Earth.

The Internet eliminates much of the expense once associated with traditional forms of publishing. It is now somewhat trivial to create a resource which can be accessed by millions of individuals. Previous forms of communication such as the telephone, radio, and television have all realized their own incarnations through Internet enabled technologies. New-world equivalents of old world communication systems are available.

The Internet is significantly different from previous forms of communication in a number of ways:

♦ Extraterritoriality\(^1\) — On the Internet the source of information exists in a somewhat ethereal place. The computer which houses the information resides

---

\(^1\) Thierer (2003), p. 61
in a physical location; however this location is often not plainly obvious or detectable. Thus the physicality of information is difficult or impossible to determine.

♦ Notice² – The transmission of information occurs with little regard to the physical borders it crosses and thus jurisdiction over the flows of information is often difficult and wholly unrealized. Data transmitted over the Internet has the potential to travel across the globe and through an immense number of jurisdictions before it finally reaches its final destination. This data normally travels with little regard or hindrance from local jurisdictional infrastructures. For example data traveling from the US to Germany through a connection in Great Britain is not expected to differ in any way based upon its path through tertiary or connecting countries.

♦ Spillover³ – In relation to “notice” any sort of control placed upon information in one jurisdiction could potentially “leak” into the borders of another. This is increasingly possible as access providers become multi-national in scope. Controls placed upon infrastructure within one country could potentially affect the data traveling across it regardless of origin and destination.

♦ Instantaneous Communication⁵ - The Internet provides near instantaneous communication. Although this does not differ greatly from other forms of electronic information, it does differ from normal forms of market or commerce. The Internet creates the potential for goods and services to be sold, delivered, and consumed at near instantaneous speeds.

♦ Low Marginal Cost⁶ - Publishing information on the Internet is significantly cheaper than most forms of publishing. For print, radio, and television the start-up cost to produce published materials is enormous (usually involving

---

² Thierer (2003), p. 61
³ Thierer (2003), p. 62
⁴ Thierer (2003), p. 62
⁵ Thierer (2003), p. 78
⁶ Thierer (2003), p. 78
the purchase of a printing press, or radio/TV transmitter). If only considered in terms of publishing cost (not considering the cost of authorship, etc.) the Internet represents a significant change from previous forms of publication.

- Little to no Error in Duplication\textsuperscript{7} - As a digital medium the Internet provides very little chance of error in duplication. The digital medium makes error checking and correction very easy and is often built into the specific protocol used for communication.

- Translation\textsuperscript{8} - The automatic translation of digital documents is becoming increasingly accurate and cost effective. The Internet makes the potential for automatic translation of an enormous amount of information a real possibility. Normal forms of media such as print, radio, or television all require an enormous amount of time and money to produce a quality translated copy of the original.

- Audience - The Internet creates the potential for a huge audience for any given piece of information. The most active websites receive millions of hits every day. Although in most forms of Internet communication the popularity of a resource is dependant upon the active request of the consumer, the potential exists for any percentage of the total user base to access any single bit of information.

- Scope - The Internet encompasses not only an immense amount of information and a diverse set of topics; the user base of the Internet is perhaps the most diverse collection of world populations ever collected. Previous forms of mass media have attracted huge audiences; however they have never had the potential to reach so many, so quickly, with so little cost in duplication and publication.

All of these factors contribute to making the Internet a significant shift in the communications potential and practice humankind.

\textsuperscript{7} Thierer (2003), p. 78

\textsuperscript{8} Thierer (2003), p. 78
Information Control and the Internet

Nation-states, in large part, retain some sort of control over the manner in which the Internet is allowed to exist in each country. Government regulatory agencies control infrastructure and access concerns. Timothy Wu notes that “at the most basic level, a state can simply choose not have any connection to the Internet.” This choice however is not a simple binary decision. To limit or deny connectivity to the Internet inherently limits the benefits gained from the “information revolution.”

Aside from issues of access and availability, countries further have the ability to limit the use of the Internet via software and hardware limitations. Sophisticated software filters enable a country to block only the portions of the Internet it deems off limits to its citizens. These can occur at several technological levels. The simplest forms enable the government to block access to a specific list of Internet sites. This site or IP based filter is akin to black listing certain telephone numbers or international addresses. More sophisticated filters are able to analyze the content of what is being done on the Internet. For example a protocol based filter could prevent peer-to-peer based file sharing or email, whereas a content filter could prevent users from accessing sites with blacklist words, ideas, or pictures.

Despite the sophistication of access limiters, they can never be 100% accurate when the content of, or access to the Internet is not directly controlled by the nation-state. Just as sophisticated software access controls exist, so also exist sophisticated programs designed to bypass those access controls. Through encryption, anonymous proxies, and other methods there will likely always remain ways for software barriers to be breached. These are not, however, likely to reach mainstream acceptance. Individuals motivated enough to search out and use anti-regulatory technology may be able to do so, however mass populations will not.

A government’s decision to limit access to the Internet is a cost-benefits calculation. There are several different forms of access control available to nation states. These can be generally classified into three different areas: legislative controls, access controls, and technological controls.

Legislative controls involve legal restrictions on what information may be transmitted over the Internet. These often take the form of legislation which specifically disallows the transmission of certain content: pornography, gambling related websites, etc. For example
the US, as well as many other nations, prohibits the possession and transmission of child pornography. Legislation provides the restriction.

Access controls deal with how the state delegates permission to access information systems. In the broadest sense the state can regulate the Internet providers and require them to meet certain standards or restrictions. In the strictest sense the state may require a license in order for users to have access to the Internet and control a government owned monopoly on access to the Internet. Within North Korea only authorized individuals are allowed to have access to the Internet. The government controls any potential “mis-use” of the Internet by preventing the general population from having access.

Technological controls attempt to control the actual information as it is transmitted over the Internet. Technological controls take one of three forms; client side controls, server side controls, and infrastructure controls. Client side controls exist on the user’s machine and prevent the user from accessing certain forms of information based upon the user’s computer’s knowledge of what is permissible and what isn’t. Client side controls often take the form of watchdog programs which prevent computer users from accessing material deemed inappropriate (programs which prevent children from viewing adult material is one example). Many US libraries install client side controls which prevent library users from accessing “inappropriate” sites while in the library. Server side controls exist at the source of information and control who has access to it based upon a knowledge of who is attempting to access what information. This type of control often exists as a barrier limiting access to a certain set of users; for example students at a specific university, or customers who have paid a subscription fee. Infrastructure controls have the most wide reaching potential for control. They exist within the Internet’s infrastructure itself and monitor the traffic which passes through it. These controls can analyze Internet traffic on a number of levels but often only block a certain set of blacklisted websites or sources of information. These forms of frequently take the form of firewall which block certain content from being accessed by a certain population. For example Saudi Arabia operates a nation wide firewall which prevents access to a list of sites that violate government regulations or the Islamic faith.
Political Models

The international system is diverse in actors and reaction. As with any social system, the international nation state system is difficult to predict. Political science provides a variety of theories as to how the system functions and makes decisions. No one theory can produce an analysis which provides comprehensive predictive ability. However when used in appropriate circumstances with appropriate assumptions, they do provide deeper insights as to the reasoning and rational behind state action. The two most popular and general theories of nation state behavior are the realist and liberal models.

The Realist Model

The realist believes that the nation state is the key actor within the international system. Nation states, through either direct or indirect means, have more or less absolute control over their sovereign regions and are the primary voices within global politics. There are several key assumptions which the realist view makes about the international system. First, the international system is anarchic. The state is the highest level of organization within the system; hence there is no controlling factor above the nation state. Second, states act rationally to maximize their benefit. When faced with a decision they determine which actions will produce the most gain for themselves. This is a logical process and is calculated based upon their access to information and their understanding of the probably reactions of other actor within the international system. Finally, states act as a singular actor within the international system. Regardless of the internal makeup of each state, their actions within the international system are made with a singular voice.

The realist view of international politics holds the nation state as the regulator of both its own internal structure and its interaction within the international system. The state has sovereign control over its various components: population, economy, military, etc. The realist views information as another area of sovereign state control. The state’s role is clear; the state has the right and responsibility to regulate and control the information which flows both within and across its borders. Given the rational nature of the realist nation state, the decision to implement controls will be a cost/benefits calculation.
The Liberal Model

Liberal theory believes that the international system benefits from the existence of so-called "liberal" states which place a strong emphasis on things such as personal freedoms, public participation in the political process, and government support and regulation of the market. Moravcsik proposed the following three main assumptions as the basis of liberal theory:

1. The fundamental actors in international politics are individuals and private groups, who are on the average rational and risk-averse and who organize exchange and collective action to promote differentiated interests under constraints imposed by material scarcity, conflicting values, and variations in societal influence.

2. States (or other political institutions) represent some subset of domestic society on the basis of whose interests state officials define state preferences and act purposively in world politics.

3. The configuration of interdependent state preferences determines state behavior.

Within the general liberal context Moravcsik also identifies three different focus variants within liberal theory: ideational liberalism, commercial liberalism, and republican liberalism. Ideational liberalism bases state preference and action upon the configuration of domestic social groups. Thus in turn, international policy and practice is an extrapolation of the domestic configurations of each individual state. Commercial liberalism sees changes within markets as the driving force for international and domestic action and policy. As the costs for certain goods, services, and actions changes governments act to facilitate or block certain exchanges through economic and security policies. Republican liberalism focuses on the state's form of domestic political representation. If the political structure of a state

---

9 Moravcsik (1997), p. 516
10 Moravcsik (1997), p. 524
11 Moravcsik (1997), p. 528
promotes the interests of a certain group, that group will utilize national policy to their benefit.\footnote{Moravcsik (1997), p. 530}

With these assumptions and focal points in mind we can better determine the role which IT and the Internet plays in a liberal-based world. Republican liberalism would focus on who is in control of any given state regime and look at the nation’s IT policy as an extension of practices which benefit those in power. Thus a country which is dominated by the economic upper classes would likely propose IT policy which benefits those groups. Commercial liberalism looks at IT policy as a tool for market regulation and control, thus the state would desire to maintain an ability to influence the ability of transaction over the Internet. Finally, Ideational liberalism views IT policy as an extrapolation of domestic social preference. Should a society desire free and unrestricted access, than the government should respond to the society’s request. In general it would appear that liberal theory sees the information technology and the Internet as a tool with which governments can express the preference of different actors; either societal groups, groups in positions of power, or markets. Thus government policy will reinforce the desire of these political actors.

A Convergence

Each of the models addressed above presents a different view of the international system. This analysis will focus on a view based upon the realist assertion that the nation state is the primary actor within international relations, and that the state is a rational actor seeking to maximize utility. Although the international system is populated with several different types of actors this analysis will view them as subordinate to the nation state.

The Internet exists outside the normal boundaries of the international state system. It is comprised of hardware, software, and individuals with potentially nothing else in common except the fact that they are all connected to a common computer network. This presents a potential problem to the traditional ideals of realist state theory: the Internet exists as an entity which exists both within state borders and outside of them. There is no noticeable difference between a website hosted within the borders of a capitalist country and one hosted within the borders of socialist one. Similarly, users from one country are more-or-less
indistinguishable from users in another country. The Internet is a platform which nominally erases the borders of traditional state geographies. The popularization of information technologies such as the Internet carries with it the potential to significantly impact the international system and the manner in which states define their own borders.

A Question of Sovereignty?

Political scientists have long debated the exact nature of the international system and the various roles of the actors which it encompasses. Regardless of which political model, school, or philosophy subscribed to any analysis of the international system cannot ignore the role which states play in determining global affairs. In realizing the significance of this role the complications of sovereignty enter into consideration. The exact definition of sovereignty has persistently been a popular topic for academic debate. Although there remain definite disagreements over the exact role of sovereignty, John Ruggie provides a definition which can be used as a broad base for further analysis. Ruggie defined sovereignty as “the institutionalization of public authority within mutually exclusive jurisdictional zones.”

The powers of states and the exact nature of sovereignty have never been static. Issues such as the migration of populations, the growing interdependence of economic systems, and the rise of sub and supra-state organizations have been grouped under the header of globalization as a new occurrence within the international system. These trends, however, have existed throughout history in some form or other. Intra-state relations and inter-state relations can be said to exist in different spheres; the proximity and rigidity of those spheres varies over time as the nature of the relationships between states change.

Within the political interstate system countries exist as distinct actors. A nation’s sovereignty has traditionally been defined by its borders and the limits of its ability to project physical power. With the increasing reliance of nations upon the world market sovereignty has come to mean something both broader and less coherent. States can no longer count themselves as completely separate and self reliant from the international system. Nations

---

13 Lake (2003), p. 304
15 Zekos (1999)
depend upon the exports and resources of other countries to provide their own citizens with the necessities of modern life. This realization has created a polarity within the contextual basis of sovereignty.

States within the international system realize two different forms of sovereignty. The first is an internal sovereign control over the populations and resources within their recognized territorial boundaries, the second is an external sovereign right to independent decision-making within the international system.

Internal sovereignty pertains to a nation's right and ability to control what happens within its borders. This normally encompasses the right to pass and enforce legislation and taxation laws. Weber saw this as a more general right to have a monopoly over violence\(^\text{16}\). At one time a country's sovereign internal rights gave it the ability to have complete independence in the decision making process. No matter the issue's significance or impact upon the country's citizenry they were largely left alone in terms of decision and consequence. Only recently has the international system become interested in the internal affairs of sovereign nations. Human and environmental rights are two of the larger issue areas which have become targets for intervention. The rationalization for intervention in these two areas comes from the potential impact to outside countries and the alleged greater good of the world population. For example damage to the local environment of a nation state has the potential to spread to other areas and impact the general future outlook of the global environment. Similarly human rights abuses are generally thought unethical and immoral by the world population and thus when significant human rights abuses are discovered outside intervention is sometimes called for by the international community. Moreover the potential for an exodus of refugees from the offending country to external nations increases the potential impact of human rights abuses on outside actors.

The realm of internal communication and information transfer is one of the traditional sovereign rights of the nation state. Governments are recognized to have the ability to establish and enforce legislation pertaining to the rights of its citizenry to communicate and transfer information. This specific area of sovereignty takes many real world forms. Controls over the media and free speech directly impact the ability of a nation's citizenry to

\(^{16}\) Weber (1946), p. 78
communicate with each other. Technology based legislation is similarly under the sovereign control of the state. The electromagnetic spectrum through which radio, television, cellular phone systems, and many other technologies communicate is also often regulated by the government. In the United States the FCC has been given governmental authority to partition use of the electromagnetic spectrum amongst organizations and technologies. In order for a radio or TV station to legally transmit in the US they must first be licensed by the FCC.

These forms of legislation have several purposes; they organize the use of public resources (such as the electromagnetic spectrum) and enforce certain content standards (such as the use of inappropriate language and adult content). Internal sovereign control over information gives nations the ability to regulate the content, context, and technology used to communicate.

External sovereignty pertains to a nation’s ability to make independent decisions within the international system. Nation states traditionally had the ability to act as equal and independent actors. Theoretically there exists no higher form of organization than the nation state. In this way, according to realist theory, the international system is anarchic. External sovereignty grants nations the ability to act as equal and independent actors within this anarchic system. Just as internal sovereignty is no longer absolute, neither is external sovereignty. The modern nation state comes under pressure from a myriad of actors in a variety of forms; other nation states, international organizations, and regimes of a variety of composition and purpose. International agreements and norms greatly affect the ability of nation states to act independently within the international system.

International regimes which create the standards and technologies that enable the Internet to function exert pressure upon individual states to comply with their standards. External nation states exert pressure and control through international markets and support.

The Internet enables populations to communicate and transfer information both inside and across the boundaries of sovereign states. In its raw and uncontrolled form the Internet does not have any underlying ability to regulate content.

CIA

The exact nature of security within the international system is often considered only in terms of physical security and warfare. When the sovereignty of information is brought
into question so is the related field of information security; or rather who has access to what
information. The CIA (Confidence, Integrity, and Accessibility) model of security is a
common method for assessing the strengths and weakness of secure computer systems. This
model addresses the three main responsibilities of any system where security is a major
concern. An application of this model to the current dilemma of the nation state and
information sovereignty can provide insight into the motivation of nations to “secure” their
information. Confidentiality concerns who has access to what data, integrity concerns
knowing that information can only be changed by authorized actors, and accessibility
pertains to preserving the ability to reach information.

Controls placed upon the Internet have a definite effect on the security of information.
Through an application of the CIA model of security we can better understand the affect
access controls have upon two groups: the Internet user (or the people affected by access
controls), and the nation state (the entity implementing access controls).

At some level the firewall has the capability to affect all three levels of the CIA
model for the end users of information technology. Confidentiality is inherently contradicted
in the analysis of information as it is being passed down line to the user. Filtering and
blocking, by nature, involves the analysis of information. Once filtering mechanisms have
been put in place it is trivial to add further features such as the logging or flagging of
information. Integrity is further damaged by these systems. The potential exists for access
control systems to alter information rather than simply denying access to it. For example, a
news article deemed offensive by the government could be effectively replaced by a
government rewrite which eliminates any offensive tone or information. Accessibility is
affected by the same system. Users cannot reliably access information on the Internet. The
prevention of access to certain information is inherent within the nature of access controls.
Although these systems are theoretically not limiting access to inoffensive information, the
added level of network analysis adds another point of failure for access to even normally
accessible information. Should the access control systems go down, it is quite possible that
the entire system would be shut down.

The issue must also be examined from the perspective of the nation state.
Governments must have reasons to implement restrictions to the access of information
technologies. Some of these motives become clear when the CIA model is applied to the
nation state; an entity whose goal is the altruistic protection and stability of the people it
governs. For governments, confidentiality is affected when a user has access to information
the government hopes to keep secret. The Internet as a medium for the fast and easy
transmission of information has the potential to quickly disseminate “state secrets” to those
without the proper access. For the many governments this not only includes the traditional
states secrets which have flavored spy movies for decades, but includes information
regarding opposition groups and any information which would affect the stability of a regime
and system. Integrity is violated when the Internet allows access to its people by outside
parties. This is inherent in the international nature of the Internet and other information
technologies. Not only do the citizens of a country have access to information spread across
the globe, but due to the two way nature of access within many information systems other
groups and nation states have access to the citizens of a sovereign country. This includes
groups as benign as spam mailers to groups as dangerous as opposition or terrorist groups.
Accessibility is affected when the Internet diminishes the affect of a native monopoly on
news and information.

A paradox exists between the security of the individual and the security of the nation
state. The CIA model expresses the obvious conflicts of interest. On one side the individual
wants security in the information he or she receives and generates, and on the other hand the
government (or extrapolation of society) desires some level of control over communication in
order to have stability and a presence in the dissemination of information. Access controls
are the nation states attempt to resolve the security issues made clear in an application of the
CIA model. Most of the outrage and concern by foreign media is a clear concern at the
individual’s level.
The Internet has experienced tremendous growth since its acceptance into popular culture. The World Bank reported that in 1991 there were roughly 4,300,000 users of the Internet. That number drastically increased in the coming decade to reach nearly 500,000,000 users worldwide in 2001\(^\text{17}\). (See Figure 1) This is a phenomenal amount of growth for any type of communications based network.

With over 500,000,000 users in 2001, the Internet is used by 1/12 of the world population. The distribution of users is not even across geographic or economic boundaries; however 1/12 of the world population is not an insignificant number of users. Increases in Internet users have far outpaced increases of the general world population. The Internet has

\(^{17}\) World Bank (2004)
consistently seen increases in excess of 59% from 1991-2001. The world population increases at a rate of between 1% and 2%.

![Figure 2. Countries & Internet Restriction](image)

**Internet Restriction (Chart: Countries & Internet Restriction)**

This paper uses data gathered by the Freedom House in their 2001 Press Freedom Survey. Within the annual Press Freedom Survey the Freedom House calculates a freedom of press rating for most of the countries in the world. Within the 2001 survey they also calculated an Internet restriction rating for many countries. They based their rating on an examination of “each country’s Internet penetration, regulatory environment and intent, and cost of Internet access, [they] categorized countries as Most Restrictive, Moderately Restrictive, or Least Restrictive”\(^{18}\) Each of the three restriction levels has certain characteristics are shared in common with other similarly rated countries:

\(^{18}\) Press Freedom Survey 2001
Most Restrictive countries may permit only the state-run Internet service provider (ISP) to carry citizens’ messages. Even if a private ISP operates, it may be under state surveillance. Citizens are subjected to fines, harassment, imprisonment, or worse for dissenting from official policies or for messages deemed seditious.19 Within this paper “Most Restrictive” countries are referred to simply as “restricted.”

Moderate restriction includes political as well as economic limitation on access to the Web and legal or administrative restrictions on content with punishment for violations.20

The least restrictive nations provide liberal access to the Web, and little if any content control.21 Within this paper “least restrictive” countries are refereed to as having fair restriction.

Of the 128 countries rated by the Freedom House 19 were said to have restricted Internet access, 53 moderate restriction, and 56 fair restriction (See Figure 2). The study only examined countries where enough information could be found to make an accurate determination of their restriction level.

This paper also uses information from the World Bank’s 2004 Economic Indicators database for more general social and economic statistics. The World Bank identifies over 200 distinct national identities within their country database and provides data on economic, social, and technological factors. Data is not available for all countries and all time periods, however in general the World Bank provides a useful standard from which to make a generalized analysis.

---

19 Press Freedom Survey 2001
20 Press Freedom Survey 2001
21 Press Freedom Survey 2001
CHAPTER 2. A TECHNOLOGY REGIME

Introduction

There are several technological factors which directly impact the ability of nation states to control the access of information over the Internet. The most influential factor is the existence of an international regime which enforces certain technological decisions upon international community members who wish to be connected to the Internet. These standards, in turn, limit the technical ability of states to control the information which flows over their localized region of the Internet. In particular the packet based routing behavior of the Internet, the fact that content is separated from traffic while it travels across the Internet, and the reliance upon physical neighbors for connectivity restricts the ability of nation states to exert domestic control over the Internet.

A Brief History of the Internet

In order to understand the reasoning behind current networking technologies and administrative procedures it is first helpful to have an understanding of the history behind the Internet. The Internet is something which defies a strict definition. Part of the problem stems from its constantly changing nature. Henry Perrit Jr. defined the Internet as "an international network of computers and computer networks connected to each other and sharing a common name and address space." Furthermore he adds that "the Internet is not a corporation or administrative arrangement; it is a method for connecting computer systems, and the phenomenon of very widespread adherence to that method." The Internet is the sum of its parts. The Internet had very clear beginnings, and an origin which would later affect not only its technological shape but its practical one as well.

During the early decades of the cold war the United States faced the problem of building a communications network which could withstand a devastating nuclear assault. State of the art networks of the time relied upon direct or obviously routed circuit connections to provide end-to-end communication. Researchers posed with the problem of

---

23 Sterling (1993)
developing a communications network which could withstand a nuclear assault found their
solution through decentralization. The Rand organization produced a report detailing a
computer network which would have “no central authority, and be designed to operate in
tatters.”  

This report was the theoretical beginning of what was to become the Internet.
Research into large computer networks was first inspired by J.C.R. Licklider, the first head of
computer research at the Defense Advanced Research Projects Agency (DARPA). Licklider
was interested in a computer network which spanned the globe and enabled its users to
access information and programs from other computers. Licklider passed on his interest to
his later successors at DARPA. Packet switching (a key technology which connects networks
on the Internet and is discussed in depth later) as a computer networking method was first
proposed by a researcher at MIT in 1961. The first recorded instance of connecting two long
distance remote machines via computer network occurred in 1965 between a computer in
Massachusetts and a computer in California. The expansion of “wide-area” computer
networking has increased from this initial population of two to over 500,000,000 users
according to 2001 data. One participant in this early experiment in computer networking,
Lawrence G. Roberts, went on to publish the plan for a computer network called
“ARPANET” in 1967.

The first node or connection to ARPANET was located in UCLA and established in
fall 1969. By the end of the year there would be a total of 4 nodes on the network. Expansion
continued each year; with 15 nodes in 1971 and 37 nodes in 1972.

Open-architecture networking was a key component of ARPANET. This technology
allows computer networks to be diverse on the micro-scale but interconnected via a common
protocol on the macro-scale. Thus computer networks could vary according to location,
resources, and need but still communicate with a larger scale collection of networks via a
common protocol. Open-architecture networking was first introduced by Robert Kahn

24 Sterling (1993)
26 World Bank (2004)
(DARPA) in 1972. This idea of combining or interweaving networks was called "Internettng."

Kahn first sought to implement open-architecture networking over packet radio networks. Due to the inherent unreliability of radio networking (signals can be jammed or blocked by physical obstacles) the then standard Network Control Protocol (NCP) was not an adequate solution to his problem. NCP assumed a reliable connection and was not robust enough to handle lost messages and relied upon the network to provide end-to-end error control. Moreover, NCP did not allow much routing flexibility. NCP's inadequateness led Kahn to develop a new protocol which would later become known as the Transmission Control Protocol/Internet Protocol (TCP/IP).

"Four ground rules were critical to Kahn's early thinking."

1. The base design and technology of a local network could differ from that of the Internet. No redesign of the local network would be necessary in order for it to be connected to the Internet.
2. The success of a transmission could not be guaranteed. If a packet could not reach its destination point, it is up to the originator to retransmit.
3. Gateways and routers would be designed as interconnection points on the network. They would be simple and require no memory of the traffic which passes through them.
4. No higher authority over the network would exist beyond the local level. Thus there could be no global form of control.

Although the TCP/IP protocol has evolved since Kahn's early design, all four of his ground rules continue to hold true.

**International Standards Regime**

The adoption of standards by the Internet community represents a great achievement in the spread of methods and systems. Despite potentially local differences in language, hardware, software, and purpose, all computers connected to the Internet are theoretically

---

able to communicate with each other. Without a system of standardization this would be impossible.

The Internet, however, cannot be considered simply a technical system which happens to have widespread acceptance. For the Internet to function and exist on a global level there must be a certain degree of acceptance, governance, and maintenance within the technical collaboration. As technologies and societies evolve their relationships with the Internet, so must the system as a whole change and evolve in order to persist across these dynamic changes. Timothy Wu proposes that “it may be useful to think of cyberspace as a kind of international regime.”

Krasner defined regimes as “sets of implicit or explicit principles, norms, rules, and decision-making procedures around which actors’ expectations converge in a given area of international relations. Principles are beliefs of fact, causation, and rectitude. Norms are standards of behavior defined in terms of rights and obligations. Rules are specific prescriptions or proscriptions for action. Decision-making procedures are prevailing practices for making and implementing collective choice.”

Krasner proposed the following causal factors which lead to regime development:

1. Egoistic self-interest – This refers to the desire of an actor to maximize their own interest without a concern for the utility of other actors.

2. Political power – Here power is divided into two different interest groups: power in service of the common good, and power in the service of particular interests. Power in service of the common good refers to the use of power to provide a common good or benefit the entire community. Power in the service of particular interests involves the use of power to increase the utility of a single actor.

3. Norms and principles – Principles and norms are the underlying and “defining” characteristics of a group or system.

---

28 Wu (1997), p. 656
4. Usage and custom – “Usage refers to a regular patterns of behavior based on actual practice; custom to long-standing practice.”

5. Knowledge – Within the context of regimes knowledge can be defined as “the sum of technical information and of theories about that information which commands sufficient consensus at a given time among interested actors to serve as a guide to public policy designed to achieve some social goal.”

The Internet and its wide acceptance within the international system meet many of these causal factors for regime development. The Internet fulfills the egoistic self-interest of state actors. By developing the basic networking technology which interconnects the Internet, countries increase their native IT capabilities. By disseminating this technology and allowing other countries to “get on line” the nation is increasing the total amount of information on the network without much negative impact on the domestic IT capabilities of the originator. Therefore by developing and allowing access to the technology an actor increases their own utility while also increasing the utility of other technological participants.

The technological and administrative norms of computer networking create a situation where a regime is likely to form. In order for network users to be reliably interconnected they must abide by a certain set of standards. These include both technological standards covering the hardware and software which collectively makes up the Internet, and the administrative standards which govern the allocation of network resources (such as IP addresses and domain names). Connection to the Internet creates a community which shares an adherence to these norms and standards.

Furthermore the Internet qualifies under the areas of usage, custom, and knowledge. Users of the Internet have become oblivious to the source or destination of their content. The basic Internet technologies of the world wide web, and email continue to dominate traffic patterns across the globe. Users are used to certain technologies and usage patterns. Moreover the knowledge required to use the Internet is more or less universal across borders. In particular the software used to access information on the Internet is more or less universal across national boundaries. Most Internet users make use of a very limited set of software

31 Krasner (1995), p. 18

programs to access and communicate information on the Internet. For example there are only 2 or 3 major web browsers from which users may choose in order to access the information available via the World Wide Web. These browsers are all somewhat similar in use and it is relatively easy for users to migrate between them. This creates a collection of users who are unified in usage patterns.

The Internet therefore satisfies several of the causal characteristics of an international regime. Its existence and wide spread popularity would point to the formation’s success. Wu found that “characterizing the Internet as an international regime seems eminently plausible. Those states which have permitted Internet access at all have implicitly agreed, at a minimum, to a set of technical standards that facilitate the transmission of data over the Internet.”

As a regime the Internet requires an adherence to certain technological standards for membership. These coincide with many of the protocols and administrative procedures discussed in the above short history of the Internet. Several of these technological requirements directly affect the ability of the nation state to control the information which flows over its domestic networks and onto the international networks.

**Packets & Switches**

Although information sent on the Internet will more than likely reach its final destination, its route and success is never guaranteed. At its most basic level the Internet uses packet based networking to move information from one point to another. Information sent over the Internet is split into small portions of data called packets. Each packet is addressed with information which identifies the sending computer’s address and the receiving computer’s address. The packet is than sent out onto the network to the originating computer’s gateway. The gateway is a form of a more general device called a router. Routers are typically simple communications devices which look at each packet and redirect to another router which is closer to the final destination. The packet reaches its final destination when a router with a direct connection to the destination computer receives the packet and forwards it to the final computer.

---

33 Wu (1997), p. 658
The path which packets take can vary according to many different factors. Routers have a very limited knowledge of the network. In most cases they cannot calculate the entire route a packet will travel. They simply act as waypoints to send a packet closer to its final destination.

Imagine a hypothetical train system which interconnects the cities of the United States. The system is huge and there is no map of the entire system. A train departing from New York bound for Los Angeles does not know the most direct route to its final destination; it simply knows that it should head west. At each intersection or train stop it can ask the local conductor for directions. No conductor knows the entire route the train should take but can get it one step closer to Los Angeles. If a certain line of the tracks is out of service the conductor can redirect the train around the problem area via a different route. Packet networking works in a similar fashion. Packets are sent from the source computer with no idea of the final route they will take. At each intersection of the network they are routed to a new intersection based upon a limited knowledge of the network’s architecture. Eventually they arrive at their final destination.

Packet networking limits the ability of any single entity to control the traffic on a network. Due to the decentralized nature of packet networks, it is very difficult for a single authority to control all the different potential routes of traffic a packet may take. There are only two points which a packet is more or less guaranteed to travel across: the router closest to the destination computer and the router closest to the originating computer. The packet is capable of taking any number of potential routes on its way across the network; even packets originating from the same computer, bound for the same destination are not guaranteed to travel across the same points on the network.

This form of networking fulfilled the requirements of the original DARPA project design for a computer network capable of surviving despite great infrastructural losses. Should part of the networked be destroyed or disconnected from the network, packets can travel on alternative routes which bypass the gaps in the network.

Forcing all network traffic to pass through a single point on the network (such as a monitoring station) is not practical because no single point on the network is capable of handling all of the network’s traffic.
By requiring the use of packet based networking to connect to the global network, the Internet limits any potential of network control to the physical boundaries of its borders. Once traffic leaves the area under which the nation may have influence over the network's routing behavior the nation releases any possibility of controlling or monitoring network traffic. Nations do retain the ability to enforce non-packet based networking within their domestic borders. Moreover the state may place requirements upon the routing behavior of internal packet and non-packet based traffic. If packet based networking is used within the domestic networking infrastructure (as is the case within most nations) the country makes any potential control very difficult. In order to have a guaranteed ability to monitor traffic they must have the ability to monitor any given routing point on the network. When the number of network users increases the difficulty in monitoring also increases. Additional users require the addition of additional infrastructure; complicating the network's architecture and routing potential.

Packet networking affects the nation's internal sovereign control over the information which flows within their borders. TCP/IP based packet networking infrastructure is established they lose the ability to accurately predict the paths which information will take. Should the government have a monopoly over the control of all the routing points of a network they could theoretically maintain some sort of guaranteed ability to monitor traffic. They could reroute suspicious traffic of interest through areas nodes with the ability to record or monitor data. Once traffic leaves this area of routing control the domestic network has no guarantee over the path traffic will take. Therefore should an unregulated packet networking infrastructure exist within the domestic sphere, internal sovereignty is directly threatened. Once the data leaves an area of controlled routing the data has the ability to pass through proxy routing systems which can obscure the final destination of information.

**A Network of Neighbors**

The Internet uses a variety of means to transmit information: fiber optic cable, telephone lines, radio, cable television lines, satellite, etc. Despite this potentially immense variety there are relatively few methods to interconnect the local networks which make up the Internet. These connections require incredible speed and reliability in order to be practical and effective. Modern systems almost exclusively use high speed cabled connections to
connect to the Internet backbone. This cabling requires a physical route and connection from one point on the domestic network to some point on an external network.

The end user connects to the Internet through an Internet Service Provider (ISP). ISPs maintain the connections and infrastructure necessary to establish connections amongst their customers. When information must flow between ISPs the data must pass through a Network Access Point (NAP) or Exchange Point (EP). This is analogous to airplane hubs. If a passenger wishes to fly to a location not directly supported by his or her local airline he or she can fly to a hub, get off the local airline’s plane and use a different airline which provides service to the customer’s final destination. Similarly, if an Internet user wishes to send information from their computer connected to ISP A to a computer connected to ISP B they must route the data through at least one EP to bridge the gap between ISP networks. The complexity of the connections increases as networks are bridged.

Countries can be viewed in abstract terms as single sets of domestic networks. In order for Country A to communicate with Country Y they must be either directly connected to each other’s networks or share connections in common through the global network. This creates a loss of control over the individual nation’s connection to the external Internet. Should Country A’s neighbors decide to cut off its connections to the network, Country A will lose the ability to communicate with points outside of its domestic borders. Therefore in order to prevent a disconnection Country A is bound to follow the norms and standards accepted by their neighbors. If Country A was to provoke its neighbors by permitting or practicing unacceptable behavior on the network, Country A’s neighbors could simply solve the problem by disconnecting Country A from the rest of the world. Should Country A somehow offend all of its physical neighbors it will be very difficult to maintain a reliable connection to the global Internet.

This reliance upon “voluntary” interconnection affects the external sovereignty of nations. Nations must keep in mind the satisfaction of their neighbors when designing network infrastructure and policy. There choices within the global Internet are somewhat restricted by the whims of those who provide border connections.

---

Baker (2000)
Unobvious Content

Levels of Connection

In order for information to pass from one Internet point to another it must travel through several layers of connectivity. The data begins on the user’s computer as a request to their network interface. The network interface could be in the form of a modem which connects to the phone line, a cable modem which connects to the cable TV infrastructure, Ethernet card which connects to an Ethernet connection, or any other number of network capable devices. The network interface then sends data out through the “local loop carrier” or local infrastructure. The local loop carrier is comprised of whatever infrastructure the message must pass through in order to reach the user’s Internet Service Provider. If a telephone connection is used the local loop carrier is the wiring from a user’s home to their ISP’s phone. After traveling across this infrastructure the data has reached the Internet Service Provider’s internal network. If the data is destined for a location outside of the user’s ISP’s internal network, the data than travels on to other ISPs through the customer’s ISP’s backbone connection.

The network does not understand the information which is crossing over it. It doesn’t even necessarily understand what kind of information is being transmitted. The network is dumb.

Modern computer networks such as the Internet are based upon the OSI model of networking. The OSI model describes the different abstraction levels of information which cross over computer networks. There are seven levels in total\textsuperscript{35}:

1. **Physical** – The connection which stretches from point A to point B. On a small scale Ethernet based network this level would consist of the cabling which interconnects computers.

2. **Data Link** – This level is abstracted as the connection from one network adapter or interpreter to another. For example on an Ethernet network, this level exists between the Ethernet card located in computer A and the Ethernet card in computer B. The adapters in each computer rely on the physical layer

\textsuperscript{35} Forouzan (2003), p. 20
to actually transmit information. The adapters however, only understand the existence of other adapters and usually assume the reliability of and do not interface with the physical layer.

3. Network – The network level of the OSI model abstracts by network type. On the Internet most networks utilize a TCP/IP network for communication.

4. Transport – The transport level deals with what type of packets or information is sent across the network. It is a sort of wrapper for the actual data portion of the information sent. UDP and TCP are the most common transport types.

5. Session – The session allows several different network connections to simultaneously connect across the network to a single user or client.

6. Presentation – The presentation level is meant to transform data into a mutually agreed upon format.\(^{36}\)

7. Application – The application level of the OSI is the highest level of abstraction within the OSI model. This is the level in which data is actually understood and utilized by the program on the user's computer. For example a web browsing application "sees" data as web pages, not bits and bytes of information streaming across the network. Most applications allow the previous levels of the OSI model to actually transmit, receive, and interpret information into a format usable by the application.

The 7 levels of the OSI model do not necessarily understand each other. For example the physical layer does not understand anything about the higher levels of abstraction. It exists simply to transmit data from one point to another. Similarly the datalink and network levels only understand what is necessary to send information from one point to another, they do not deal with the type or content of the information that is being sent. Only once the information reaches the session level does it begin to become coherent or understandable by the client. The application level is the final level of abstraction and represents the final format of data that reaches the client program. Only the client and server applications know for sure what the information being transmitted means.

\(^{36}\) Forouzan (2003), p. 29
Encryption or other forms of masking the true content of data can occur at many of the OSI levels. Encryption can be built into levels including and above the OSI's network level. This creates a complication for any type of monitoring. Most forms of encryption contain no method for which an unauthorized third party to easily decode the content of a message. Although it is usually possible to break encryption through repeated brute force attempts at guessing the password or key, this method is often extremely time consuming and thus impractical.

This form of information abstraction affects the internal sovereignty of nation states. In relegating the true purpose and meaning behind data to the upper application levels of the OSI model, the content and contextual reference necessary to understand information only exists at the source and destination of Internet traffic. There is no inherent ability for data to be understandable at any level below the application level. Thus nation states do not have any guarantee over the ability to monitor information after it leaves its source or before it reaches its destination. Despite there being no guarantee much of the traffic which passes across the Internet is easily placed into context based upon the packet's header information. For example it is usually easy to differentiate between web, email, and FTP traffic. Thus despite the OSI model some traffic can be intercepted and understood without the need for the client or server application to interpret it.
CHAPTER 3. REGIME ACCEPTANCE

Pressure from Market Forces

A major factor driving the acceptance of technological norms and standards are world economic markets. The technological regime mentioned in the previous chapter was responsible for the acceptance of a number of technologies which directly impact the ability of nation states to control content and information (Packet based routing, OSI abstraction levels, etc). These standards not only became prevalent because of technological reasons (they were designed to solve a problem posed by DARPA but continued into the public sector as the primary answer for large scale networking) they eventually picked up the influence of world wide markets.

By promoting worldwide standards the market is able to benefit from the increased efficiencies presented by economies of scale. When a majority of the world population uses a single technological standard companies are able to produce products with little domestic market differentiation; the same networking product produced for the US market will work with little or no change in Europe or Asia.

Economic markets support the technological regimes for several other reasons as well. The main factors influencing markets toward this specific set of technological standards are a desire for security, transparency, and stability.

Security

Just as security is a concern for physical and monetary transactions, security is also a major concern over computer networks. This is especially true when real world forms of transaction are expected to take place securely over the Internet. Market actors demand that their transactions take place in an environment where they can have a reasonable amount of security. The open ended nature of current TCP/IP implementations of the Internet and the OSI networking model allow for an organization to implement a large number of different security strategies. One of the most common is encryption. Data can be encrypted on one end of the Internet connection and decrypted on the other end with a reasonable expectation of security. The OSI model allows the organization to focus upon security at the application level and largely ignore the network infrastructure.
The CIA model can once again bring to light a number of the security concerns faced by organizations on large scale networks. Confidence concerns who has access to what information. The open ended nature of the current Internet system allows companies to design networked systems with proprietary security – proprietary in the sense that only their permitted associates are allowed access to the data. Whether an organization uses one of the openly available encryption technologies or invests the time and money to develop their own system, the freedom with which they can choose a solution allows them to determine their own level of confidence. Integrity is insured via similar means. By controlling who has access to what information organizations also control who has an ability to change information. Although the current networking system is susceptible to information attacks involving the interruption and monitoring of traffic, a variety of solutions are widely available to address these concerns. Encryption and error correction can be combined to almost insure the delivery of secure content. Accessibility, or maintaining an accessible store of information, is one of the more major concerns of the current system. It has become more and more frequent for denial of service attacks to restrict the availability of information on the Internet. These DOS attacks exploit weaknesses in the TCP/IP networking protocols to “clog” the lines and prevent access to a certain resource such as website or database server. Although this is a flaw inherent in the networking infrastructure, new technologies are being developed to combat the problem and promise companies an increased level of insured accessibility on the Internet. The Internet satisfies all three CIA demands.

**Transparency**

Market actors also seek transparency in networking architecture and technology so that they can observe and understand network interactions. This is similar and somewhat related to their demand for security. The realization of network security requires a certain description and understanding behind the technologies involved in networking so that security can be insured.

The TCP/IP protocol and the general infrastructure of the Internet is based upon designs which are openly accessible to anyone interested in analyzing them. In this manner the physical and software infrastructure of the Internet is open to the analysis of organizations. They can have an understanding of the infrastructure which equals that of
those who designed it. By allowing organizations to realize this level of knowledge the Internet permits them a sense of safety in knowing that there are in fact very few unknowns and surprises in the system.

Nations who openly place access controls on the Internet put into question the security of the protocols and infrastructure of the Internet. Companies wishing to have confidence in the security and integrity of the network infrastructure will be wary of investing in an area with unknown infrastructural elements which could potentially affect the delivery of their information. Thus international organizations seeking to establish an information presence within a nation state will advocate an open form of control which can produce reliable and predictable results. For this reason organizations will demand transparency in infrastructure and information controls.

**Stability**

Market actors also seek stability in networking technology and policy. Markets invest enormous amounts of money to create the infrastructure and technology necessary to realize market transactions over computer networks and thus expect the conditions under which they invest to remain somewhat stable. Technology based information controls inherently cause complications and thus inefficiencies within IT networks. These controls also create potential additional points of failure within the network. Depending upon how the system is set up, should a control point fail the networks which rely upon the control point could fail as well.

**Sovereignty**

These pressures upon governments affect the internal sovereign choices that nations make. Markets require or lobby governments for their cooperation in providing IT networks which allow them security, transparency in networking, and stability. This pressure affects the rational decision making process of the nation state by shifting the reward/payoff for acquiescing to the technological regime of the Internet.

External sovereignty is also affected due to the requirement for border connections to the global network to meet basic network standards. The nation’s choice for internal networking is somewhat open to domestic government preference or propriety. The external links to the global network, however, must comply with standards in order to interoperate and communicate successfully with the world network.
CHAPTER 4. CASE STUDIES

China

The People's Republic of China is a country rated as having severe restrictions on the Internet. The Freedom House justified this rating based upon the following restrictions:

"New Chinese laws require Internet companies to secure licenses and to be held responsible for "illegal" content carried on their systems. They must keep records of users and their messages. ... For sending or receiving messages critical of Beijing or of Communist policy, however, a Chinese Web surfer can face harassment or up to 10 years in prison. Last June, the founder of the first human rights Web site in China, Huang Qi, was accused of "subverting state power." His last message: "Thank you all, thanks to everyone devoted to democracy of China. They [the police] are here now, so long."" 37

According to World Bank data China had in 33,700,000 Internet users in 2001. This is roughly 2.7% of the Chinese population. Aside from the legal restrictions mentioned by the Freedom House, China also has several well documented technological restrictions.

Government Restrictions

In 1997 the Chinese government established certain guidelines regarding the material which should be accessible to the public. These national regulations are meant to influence both individuals accessing the Internet and Internet providers. Both individuals and providers are held responsible. The guidelines themselves are meant to be implemented by the Internet Service Providers. The implementation of these regulations is manifested by China's firewall. These restrictions mandate that an Internet provider or access point prevent access to:

1. Information that goes against the basic principles set in the constitution;
2. Information that endangers national security, divulges state secrets, subverts the government, or undermines national unity;
3. Information that is detrimental to the honor and interests of the state;

37 Press Freedom Survey 2001
4. Information that instigates ethnic hatred or ethnic discrimination, or that undermines national unity;

5. Information that undermines the state's policy towards religions, or that preaches the teachings of evil cults or that promotes feudalistic and superstitious beliefs;

6. Information that disseminates rumors, disturbs social order, or undermines social stability;

7. Information that spreads pornography or other salacious materials; promotes gambling, violence, homicide, or terrorism; or instigates crimes;

8. Information that insults or slanders other people, or infringes upon other people's legitimate rights and interests; or

9. Other information prohibited by the law or administrative regulations.

This relatively short list of restrictions is broad enough in scope to limit access to almost any information which can be rationalized as destabilizing or offensive to the state.

**The Firewall**

The exact manner in which China's firewall operates is kept a state secret. Precise knowledge as to the manner in which China filters and monitors information would greatly simplify the task of bypassing or compromising the firewall. Thus most of the information available concerning China's firewall was gathered through observation, speculation, and common sense.

The most basic manner in which the firewall works is by blocking entire "portions" of the Internet. This is most likely done through a list of web sites and their associated IP addresses (one of the most basic forms of identification on the Internet, it is akin to an Internet postal address). This list is then cross checked with any attempts to access the web. If the requested website is on the banned list, the user is prevented from accessing it. In many systems similar to the Chinese one (such as the one existing in Saudi Arabia), a user is presented with a message saying the website the user attempted to access has been blocked. The Chinese firewall does not, however, alert the user that the website has been blocked.

---

38 Zittrain (2003)

This prevents the user from knowing at what level the connection failed. As far as the user knows, he or she may have entered a wrong web address, there could be network problems, or the website could be down for technical reasons. This is perhaps more effective than the Saudi Arabian system because if a user attempts to access a site and finds that it is blocked, he or she can at least infer some small amount of information regarding the content of the site. The Chinese system prevents the user from realizing even this small amount of information. It most likely lets the request timeout or sends an inaccessible or not found message back to the computer. This type of firewall is both cheap and easy to implement. It operates at a very low network level (at the Network level (3) of the OSI model) and involves very little processing power because there is no analysis done on the actual information. The originating address is the only concern of the firewall, and this is simply cross checked with a database. This type of filtering can occur without any actual understanding of the information being transferred. The database of banned sites is most likely created by a hybrid process of human made entries with a simple automated web spider that traverses the web looking for sites which contain illegal material.

A higher and more complicated form of filtering has recently been reported in China\textsuperscript{40}. Some areas report that sites are no longer simply blocked by their Internet address, but by the very content of the information transferred. This is known as “keyword” filtering. The filtering system examines the actual information being transferred and determines whether the content of the information contains certain banned keywords. If a web site or message is found to contain some of these keywords, access is prevented. This is more complicated than the simple IP based filtering mentioned above in several ways. The filtering system must understand the traffic being sent. This is done at the application level of network traffic and requires a thorough understanding of the different protocols involved in network traffic. The filter would intercept traffic either on its way from or to a user, analyze the traffic, and determine whether the contents of the traffic violate the filtering rules. If a violation is found any number of options are open to the filter. It could simply keep a log of the violations or throw away the traffic which didn’t pass the filter. At this level the filter also has the capability to alter the contents of the traffic.

\textsuperscript{40} Zittrain (2003)
Both the simple IP firewall and content filter could be established at different points on the network. The Internet Service Provider could be mandated to include these mechanisms in their systems, or the government may establish them independently of the ISPs. It would seem most likely that the government maintains a base IP firewall at the local point where the Internet backbone feed China and than place more burdensome restrictions on ISPs. For example the traffic is filtered at the IP or address level when it enters China, and processed at the content level immediately before it is sent to the user at the Internet Service Provider. This would give the government some base insurance that they have the ultimate control over what enters and leaves the country, but shares the burden for more accurate and individual filtering with the ISP.

Through this analysis we are able to draw a fairly complete picture of the Chinese firewall. The restrictions reportedly vary across China. The most advanced filters have the capability to block specific content within a website rather than the website in its entirety, initiate “time outs” where a user’s access is limited for a certain amount of time after searching for “banned” keywords, and monitor chatrooms and restrict the posting of dissident comments. This dynamic form of filtering is likely the most advanced in China and not yet implemented nationwide. In areas with small “loyal” Internet populations there probably exists simpler, less sophisticated and less costly versions; for example simply an IP or name based firewall.

**Saudi Arabia**

In 2001 the World Bank reported that there were 300,000 Internet users, or 1.4% of the population, in Saudi Arabia. The Freedom Press report identified Saudi Arabia as having a moderate level of restriction. In the Saudi Arabian case this level of restriction translates into a firewall based content control system not dissimilar in purpose from the Chinese example. There are a few key differences. The Saudi Arabian firewall notifies the user when a site has been blocked. This allows the Internet user to differentiate between sites which simply happen to be inaccessible for an indeterminate reason and those sites which have been actively blocked by the government firewall.

---

41 Baranowski (2002)
The Saudi Arabian government has established an Internet Services Unit (ISU) charged with the responsibility of providing Internet services within Saudi Arabia.\textsuperscript{42} The unit has a number of responsibilities; among them is the establishment and maintenance of a national firewall which prevents certain websites from being accessed from within Saudi Arabia. The ISU describes the filtering system and policy:

"All incoming Web traffic to the Kingdom passes through a proxy farm system implementing a content filtering software. A list of addresses for banned sites is maintained by this filtering system. This list is updated daily based on the content filtering policy. A list of pornographic sites is provided periodically by the filtering software provider. However, this list is not comprehensive due to the high proliferation and diversity of pornographic sites. Therefore, KACST (King Abdulaziz City for Science and Technology) maintains a web-based form that users can fill-out to report sites they feel should be blocked. Hundreds of requests are received daily. A team of full-time employees at KACST study these requests and implement them only if justified. As for non-pornographic sites, KACST receives orders to block them from related government bodies (refer to content of filtering policy)."\textsuperscript{43}

Saudi Arabia has passed legislation which prevents users from publishing or accessing information of the following types\textsuperscript{44}:

1. Anything contravening a fundamental principle or legislation, or infringing the sanctity of Islam and its benevolent Sharih, or breaching public decency.
2. Anything contrary to the state or its system.
3. Reports or news damaging to the Saudi Arabian armed forces, without the approval of the competent authorities.
4. Publication of official state laws, agreements or statements before they are officially made public, unless approved by the competent authorities.
5. Anything damaging to the dignity of heads of states or heads of credited diplomatic missions in the Kingdom, or harms relations with those countries.

\textsuperscript{42} The Internet Services Unit (2004) \textit{Homepage}

\textsuperscript{43} The Internet Services Unit (2004) \textit{Local content Filtering Procedure}

\textsuperscript{44} Arab Gateway (2001)
6. Any false information ascribed to state officials or those of private or public domestic institutions and bodies, liable to cause them or their offices harm, or damage their integrity.

7. The propagation of subversive ideas or the disruption of public order or disputes among citizens.

8. Anything liable to promote or incite crime, or advocate violence against others in any shape or form.

9. Any slanderous or libelous material against individuals.

The Saudi Arabian government also requires that Internet service providers follow a set of rules meant to protect the “constituents of the native network:”

1. Service providers shall determine Internet access eligibility through access accounts, user identification and effective passwords for the use of the access point or subsequent points and linking that through tracing and investigation programmes that record the time spent, addresses accessed or to which or through which access was attempted, and the size and type of files copied, whenever possible or necessary.

2. The use of anti-virus programmes and protection against concealing addresses or printing passwords and files.

3. Endeavour to avoid errors in applications that may provide loopholes that may be exploited for subversive activities or to obtain data not permitted for use for whatever reason.

4. Restriction of the provision of Internet services to the end-user through the Internet service unit at King Abdulaziz city for sciences and technology.

5. Keep a manual and electronic register with comprehensive information on end-users, their addresses, telephone numbers, purpose of use, and private Internet access accounts, and provide the authorities with a copy thereof, if necessary.

6. Not to publish any printed directories containing subscribers’ and end-users’ names and addresses, without their agreement.

45 Arab Gateway (2001)
USA

The United States is identified as having fair restrictions by the Freedom House report. In 2001 the World Bank statistics showed that there were 142,823,000 Internet users in the US (50% of the population). Although legislation has attempted to control certain forms of content and communication on the Internet, these controls generally fall in line with prior legislation regarding previous forms of media. Most of the attempted legislation has sought to control "indecent" material on the Internet and prevent its viewing by inappropriate persons (for example children).

The United States has been subject to several rounds of legislation which sought to limit access to the Internet in several different contexts. In 1996 the Communications Decency Act (CDA) was passed in an attempt to protect minors from indecent material in the online world. The CDA made it illegal to transmit "indecent material" to minors. On June 26, 1997 the CDA was struck down by the Supreme Court as imposing unconstitutional restrictions upon a "unique and wholly new medium of worldwide human communication."

In 1998 the Child Online Protection Act (COPA) was passed. COPA creates criminal penalties for the commercial distribution of material deemed harmful to minors:

"Whoever knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, makes any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors shall be fined not more than $50,000, imprisoned not more than 6 months, or both."  

"Material that is harmful to minors.--The term 'material that is harmful to minors' means any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind that is obscene or that—the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest; depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent

46 EPIC (1998)
47 EPIC (1998)
female breast; and taken as a whole, lacks serious literary, artistic, political, or scientific value for minors."\textsuperscript{48}

The COPA is currently being challenged in court and has already been deemed unconstitutional by several government entities. Individual US states have also enacted various forms of Internet access control regulations. These regulations generally attempt to control "decency" on the Internet; some have attempted to regulate or censor the Internet within public institutions such as libraries.

\textsuperscript{48} EPIC (1998)
CHAPTER 5. CONCLUSION

Regime

The Internet is more than simply an agreement on a certain set of standards; it is a relationship among states which holds them to a general and long term obligation to follow the Internet’s set of norms and principles. Krasner defines this long term obligation as the key difference between a “regime” and a simple “agreement.” The Internet can be viewed as an international regime based upon the technical, administrative, and usage standards which allow the Internet to function and interconnect. Wu notes that under the institutionalist’s view of Realism “states will adhere to the rules of this regime if and only if it is in their best interest to do so.” The decision for a state to accept an international regime is a cost/benefits calculation; the state will decide if the potential benefits gained from becoming a member of a regime outweigh the losses associated with joining it. In the case of the Internet, states have the potential to lose some of their sovereign control over the flow of information. Attempts to re-exert control over the Internet can result in a decrease in economic and other expected benefits. Again Wu notes that “the institutionalist model predicts that power-maximizing states will act to regulate cyberspace as much as possible without threatening the other benefits that the Internet delivers.” Therefore the Internet is a regime whose membership contains many levels of compliance and exception; those who choose membership still have an ability to retain some control over their absolute adherence to standard practice.

As a function designed to maximize the utility of a state, those nations who choose to place controls on the Internet do so as a result of several different contributing factors. General comparisons between the Freedom House report and the World Bank statistics can reveal several of these factors.

50 Wu (1997), p. 656
51 Wu (1997), p. 659
52 Wu (1997), p. 660
Figure 3. Populations with Internet Restriction

Figure 4. Internet User Populations with Internet Restriction
**Contributing Factors**

**Population**

*User Populations (Charts: Internet User Populations with Internet Restriction, and Populations with Internet Restriction)*

User populations (the number of users within a given nation state) appear to have a significant impact upon the level of restriction within the state. When the Freedom House data concerning Internet restrictions is matched with the World Bank statistics regarding the number of Internet users in each country and also with general population statistics we can see that a majority of Internet users live within countries with “fair restriction.” (See figure This indicates that countries with “fair restriction” have a much higher percentage of the world population of Internet users. There is a direct relationship between the percentage of Internet users a country has and the level of restriction.

Nations with “fair restriction” have a larger percentage of their population online (an average of 23% of the population uses the Internet) than users within restricted (2%) and moderately restricted (5%) nations. This does not necessarily indicate a direct causal link, however the relationship is prominent. This relationship could be indicative of several different general scenarios.

- The more users a country has the more difficult it is for that country to place cost effective controls upon the general population.
- The more users a country has the more pressure they place upon the regime to offer less controlled access to the Internet.
- Fewer restrictions placed upon access will result in a increased percentage of the population wanting access.
Figure 6. Restriction vs. Gross National Income Per Capita

Economy

*Income (Chart: Restrictions vs GNIPC)*

There also appears to be a relationship between the per capita income of a nation and the degree of Internet restriction realized in that country. The average income of a resident living in a country with “fair” Internet restrictions is a little less than $13,000 USD whereas the income of a resident living under moderate and severe restriction is just under $3,000 and $1,500 USD respectively. Again this relationship is not necessarily causal however it is certainly strong and could be indicative of several things:

- With higher incomes the advantages Internet access brings to the general population and thus the nation state are greater (for example more commerce occurs over the Internet or more private investment in infrastructure can offset the need for the nation state to expend its own funds) thus as income increase the cost related to restricting Internet access increases.
• Countries with a higher per capita income naturally have a higher percentage of their population with computer and Internet access. Countries with low incomes simply do not have the population base necessary to warrant full regime acceptance by the nation state.

![Graph showing restriction vs. high tech imports]

**Figure 7. Restriction vs. High Tech Imports**

**High Tech Imports**

Should economic markets have an effect on the Internet restriction level of a country, than this should be reflected in the amount of high tech imports a country receives. If a country seeks to receive offshore investment in the form of high technology (and especially information technology) goods than they should be under pressure from the economic community to reduce Internet controls. When comparing the restriction level of countries (via the Freedom House report) with the percentage of high tech imports (see Figure 7) a country receives (this was calculated by taking the percentage of high tech imports a country receives and dividing by the total imports of a country – both figures from the World Bank statistics). Due to the unavailability of a high tech import statistics for many countries, these results are by no means conclusive; however there is a definite difference between the fair
and moderate level (10.41% and 5.75% respectively). The severe level’s percentage (8.44%) is surprisingly higher than the moderate level. This can be accounted for by the fact that only two countries with severe restriction levels had high tech import statistics available (China 16.51% and Azerbaijan 0.37%). Both the deviation between these two countries is great and the low number of samples results in a higher margin of error. Some general conclusions can be drawn however:

- The higher the amount of high tech imports a country has, the more pressure will be exerted upon them by the international market to not restrict Internet access. This enables the international market to preserve its security, transparency, and stability.
- The general relationship between high income countries and lower restriction has already been noted. Generally more developed countries have a higher percentage of high tech imports, thus this relationship could simply be a result of a general link between “developed” nations and unrestricted access.

**Government Regime Type**

There appears to be definite link between the regime type of a nation’s government and their degree of Internet “freedom.” The nations rated as having restricted Internet access appear to have a large number of authoritarian regimes amongst them. The Freedom house rated 18 countries as having restricted access. They are: Algeria, Angola, Azerbaijan, Bahrain, China, Congo, Cuba, Ethiopia, Kazakhstan, Kenya, Lao PDR, Sierra Leone, Sudan, Suriname, Swaziland, Tajikistan, Tunisia, and Turkmenistan. Most of these countries are considered as having authoritarian regimes and do not generally offer their citizenry a high level of personal freedom, hence restrictions on the Internet fall in line with previous regime decisions to restrict other personal freedoms.
In analyzing the general characteristics of countries with fair, moderate, and heavy restrictions on the Internet there appears to be a general link between "development" and free Internet access. The term "development" is not precise and refers to several different general characteristics of a nation: an advanced economy which can provide its citizenry with a relatively high standard of living, government leaders are generally chosen through a democratic process, a large percentage of the population has access to a computer; other personal freedoms are not significantly infringed upon, etc.

This general relationship also indicates that countries which don’t restrict other forms of communication generally don’t restrict Internet communication (See chart: Internet and Press Freedom). The Freedom House also noted this correlation. Moreover the Internet is generally freer than the press. It must be noted, however, that the Freedom house rates 187

---

53 Freedom of the Press Report 2001
countries with freedom of the press ratings whereas they only rate 131 countries with Internet restrictions ratings.

**The Impact of Information Sovereignty**

The ability of a nation state to control the information which passes across and into its borders brings with it a potential for both great benefit and great abuse.

The ability to monitor and control information grants the nation state an ability to extend some of its more traditional roles into the world of information. These could involve everything from the provision of basic infrastructure-related services to the policing of online criminal offenses. Many of the current problems which plague the online world could potentially be solved if the nation state were to preserve an ability to control information on the Internet. The originators of unsolicited email, or spam, could be tracked down with little trouble. Online crimes could be investigated more easily and with an increased efficiency.

A nation which maintains control over the flow of online communications has the ability to abuse a number of basic human rights. When there exists an ability to monitor and control communications the potential exists for abuse from the governing powers. The most infamous example of this is the dystopia of George Orwell’s 1984. Orwell presented a world in which the government controlled and monitored all communications to the point of having a thought police which punished any form of subversive thought. With the growing importance of online communications within the daily lives and normal communication patterns of many people, having a complete ability to monitor online communications would make an Orwellian future much easier to bring to reality.

The simple ability to abuse control does not guarantee that a dystopian future will become a reality. The tradeoffs between the beneficial side of information controls and the potential abuses which become possible must be carefully considered when any sort of controls are under consideration.

**Future Considerations**

**Bypassing Software**

There are several ways in which technology based Internet restrictions can be circumvented or bypassed. The simplest way is through the use of web proxies or mirrors in
an outside country. A web proxy acts as a go-between for a web user. The user sends a request for a web page to the proxy machine, which will in turn fetch the page and send it to the user. Thus the simple IP firewall does not know the final destination requested by the user. These proxies could be blocked by the IP firewall in the same way that it blocks a webpage, however their relative abundance on the Internet makes them difficult to locate.

A similar problem exists with mirroring or caching pages on the Internet. For example a popular web page often has several mirrors, or copies of itself, located at different places. This ensures that users from different areas of the globe have fast access to the site. It also makes the job of an IP filter more difficult because a user can access the same information at different places on the web. Similarly many locations cache web pages to keep a history of the Internet or for building search engines. Places such as the Internet Archive cache pages to build “historic” snapshots of the web. The search engine Google makes its web cache available to users in case a website has changed or is inaccessible.

Web translation services can be used to provide a similar service. A clever web user could have a banned web page translated from Chinese to Chinese by any number of online translation services. This would effectively provide them a proxy by which to view any site banned by the IP firewall.

All of these methods provide some degree of freedom from behind an IP firewall. These “tricks” are not inherent weaknesses in the firewall but simply weaknesses in the selected denial of pages. Should the firewall manage to find ALL proxies, mirrors, etc than it would be almost completely effective. These methods would not, however be effective against a content filter. These “tricks” only change the apparent source of information, not the information itself.

In order to penetrate a content filter you must use more complicated means. The creative use of alternate spellings and encoded text is one way. The most effective way is through the use of cryptography or steganography. When modern forms of encryption are implemented a user can be relatively sure that only those with access to the necessary keys, passwords, etc will be able to view the content of a message. This would prevent a content filter from flagging restricted material because it could not read the true contents. Should the content filter decide to block ALL encrypted material the user would have to use something even more complicated.
Steganography is the science of hiding information within various media. For example it is possible to encode data within an image without changing the image in any noticeable way\textsuperscript{54}. This disguises information within a “harmless” looking package. This information could also be encrypted for an added layer of security.

The problem with both cryptography and steganography lie in their hidden nature. In order for an encrypted message to reach a large audience, that audience must know the secret key or password; similarly for a steganographically encoded message to reach a large audience that audience must have the correct software to extract the message and know the location of the message. Distributing this information to a large audience without informing the government is a very difficult problem.

**Arms Race**

Information technologies can be controlled by the nation state. This control, however, must be active and evolve as information technology evolves. Thus, any particular technological solution to the control of information technology will likely not be valid as the nature and speed of IT increases. Legislative controls can exist without enforcement; however have little impact unless actively enforced. This constant improvement in technology is a fundamental shift from previous communications technologies. The printed word, although it has benefited from several improvements reducing cost and production time, has changed very little from its beginning. Information technology changes constantly in terms of method of transport, speed, breadth, and nature. Thus there is a conundrum in the nation state’s goal to enforce its legitimate control over the flow of information; the technologies needed to control information technologies must advance at least as quickly as information technology itself. Whether or not states are willing to invest the resources necessary to develop and implement controls is a question left to individual states.

**“Laws of Censorship”**

Although the technical capabilities of a firewall can be refined over time, and increase with need and advances in processing power, there are other factors which intrinsically limit

\textsuperscript{54} Johnson, “Steganography”
the extent to which information controls can be implemented. The following “Laws of Anti-Censorship” have been proposed:

1. The difficulty of blocking an anti-censorship technology is proportional to its ties to commerce.
2. A circumvention technology will be blocked up to the limit of resources the enemy is willing to invest in blocking the technology.
3. The amount of effort an enemy will put in to defeating a system is proportional to the users using that system.

The first law expresses a very important point: countries which participate in the world economic markets will have to succumb to economic pressures when censorship affects business. For example, the Chinese government is trying to prevent the widespread use of encryption technologies through import restrictions. This is a result of the impact encryption has upon monitoring technologies; the government loses the capability to monitor and censor information when it is beyond their recognition due to encryption. Business however demands encryption as the only safe way to guarantee confidentiality in things like monetary transactions and the transmission of personal information. Without this guarantee e-commerce cannot take hold within China. Therefore the Chinese government must play a careful balance between its control of the sovereign Chinese portion of the Internet and the commercial freedom which business demands.

The second and third laws bring up another point; with increasing percentages of the world using the Internet, governments must expand their controls to maintain any sort of effectiveness. This costs money. There comes a point where the cost/benefit ratio becomes too burdensome to continue. The same is also true of technologies which attempt to bypass the technological controls. If a new circumvention technology requires a tremendous investment in monitoring technology to offset, than the cost/benefit ratio again becomes burdensome.

55 Baranowski (2002)
56 Crampton (2002)
A New Taxonomy

Although the Freedom House provides a very thorough and useful statistical base for analyzing Internet restrictions any future study would benefit from a more structured approach to the problem. An approach which categorized restrictions into different categories such as technical, legislative, or access based and rated each restriction's severity would allow an analysis with both deeper insights into the effects of restriction in general and the effects of specific forms of restriction. Nations do not always provide easily accessible information about their Internet restrictions; therefore any future survey will suffer from this inherent problem. Likely the user is the best resource for real world information regarding usage patterns within states. An open survey which allowed users to note or mention any general or specific controls on their Internet access could allow a broad base of informants and statistics. This data could then, in turn, be collected and summarized into general country and global reports.

Conclusion

Nations wish to preserve their control over the flows of information; however several technological and social factors force them to make a cost/benefits decision on whether or not to allow unrestricted access to new technologies such as the Internet. Chapter 1 of this thesis examined the Internet as a fundamental shift in the communications capability of humankind and argued that the Internet can be considered as a technology and standards regime which ensures the interoperability and technical standards of domestic computer networks which connect to the global Internet. In order to gain the full benefits available from the information revolution they must subscribe to the technological, administrative, and usage standards which allows the Internet to function. In subscribing to this regime they give up a certain amount of control over the flows of information within their once sovereign area of information control. Many of the Internet’s base technologies directly affect the nation’s ability to monitor and control the flow of information. An examination of the technological background of the Internet was presented in chapter two. This examination suggests that this new form of communication impacts the sovereign ability of the nation-state to control the flows of information both within and across its borders. Chapter three examined the role which international markets play in promoting the Internet regime. Markets desire
compliance with the international regime in order to ensure transparency, security, and stability. Nation-states make a rational cost/benefits decision on the form which networking takes within their domestic boundaries and on what controls are placed upon access to the network. Controls placed upon the technology or access of users affects the payoff of benefits from these new forms of information technology. There have been varied and diverse responses to the question of network access; from national firewalls and strictly controlled access privileges, to legislative barriers and freedom of information movements. Chapter four introduced case studies of internet controls in China, Saudi Arabia, and the US as examples of three different levels of control. Finally chapter five presented aggregate data which indicates a relationship between nation-state controlled access to the Internet and several different economic and social factors. The number of Internet users in a country, per-capita income, high-tech imports, and the overall regime type all seem to have a definite correlation with the degree of Internet restriction. The Internet has the potential to greatly affect the level of control that the nation has over information. National control over information technologies has the potential for both positive and negative consequences, any nation wishing to exert some form of restriction or control should carefully consider the potential harm and potential good arising from that control.
REFERENCES


