NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

ASSERTING NATIONAL SOVEREIGNTY IN CYBERSPACE: THE CASE FOR INTERNET BORDER INSPECTION

by

Oren K. Upton

June 2003

Thesis Advisor:	Mikhail Tsypkin
Thesis Co-Advisor:	Dorothy Denning

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2003	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Title (Mix case letters) Asserting National Sovereignty in Cyberspace: The Case for Internet Border Inspection			**5. FUNDING NUMBERS**
6. AUTHOR(S) Oren K. Upton			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			**12b. DISTRIBUTION CODE**

13. ABSTRACT ***(maximum 200 words)***

National sovereignty is a fundamental principle of national security and the modern international system. The United States asserts its national sovereignty in many ways including inspecting goods and people crossing the border. However, most nations including the United States have not implemented any form of border inspection and control in cyberspace. This thesis builds a case that national sovereignty inherently and logically gives a sovereign state, such as the United States, the right to establish appropriate Internet border inspection stations. Such stations would be used to inspect only legally vetted inbound traffic, and block contraband, in a fashion analogous to the current system for inspection of people and goods that cross US borders in the physical world. Normal traffic crossing the border would have no content inspected and no record would be kept of its passing. This thesis answers key questions about feasibility, proposes a high level structure for implementation, and describes how such a system might be used to protect reasonable and legitimate interests of the United States including both security and individual rights. One chapter will build the logical case for Internet border Internet inspection. And other chapters will discuss technical, legal, and political feasibility.

14. SUBJECT TERMS Internet, inspection, border protection, homeland security			**15. NUMBER OF PAGES** 95
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited.

ASSERTING NATIONAL SOVEREIGNTY IN CYBERSPACE: THE CASE FOR INTERNET BORDER INSPECTION

Oren K. Upton
Captain, United States Air Force
B.A., University of Texas at San Antonio, 1993

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN NATIONAL SECURITY AFFAIRS

from the

NAVAL POSTGRADUATE SCHOOL
June 2003

Author: Oren K. Upton

Approved by: Mikhail Tsypkin
Thesis Advisor

Dorothy Denning
Co-Advisor

James J. Wirtz
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

National sovereignty is a fundamental principle of national security and the modern international system. The United States asserts its national sovereignty in many ways including inspecting goods and people crossing the border. However, most nations including the United States have not implemented any form of border inspection and control in cyberspace. This thesis builds a case that national sovereignty inherently and logically gives a sovereign state, such as the United States, the right to establish appropriate Internet border inspection stations. Such stations would be used to inspect only legally vetted inbound traffic, and block contraband, in a fashion analogous to the current system for inspection of people and goods that cross US borders in the physical world. Normal traffic crossing the border would have no content inspected and no record would be kept of its passing. This thesis answers key questions about feasibility, proposes a high level structure for implementation, and describes how such a system might be used to protect reasonable and legitimate interests of the United States including both security and individual rights. One chapter will build the logical case for Internet border Internet inspection. And others chapters will discuss technical, legal, and political feasibility.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

ACRONYMS

ARPA	Advanced Research Projects Agency, conducts research for Dept of Defense
ARPANET	ARPA Network, predecessor of the Internet
BBN	Bolt, Beranek, and Newman, research team that developed ARPANET and commercial Telenet network structures
BCIS	Bureau of Citizenship and Immigration Services
CBP	Customs and Border Protection, replaced US Customs Service
CD	Compact Disk, medium used for digital information like music and Computer programs
CERN	Conseil Europeen pour la Recherche Nucleaire (European Council for Nuclear Research), a high energy physics laboratory
DARPA	Defense Advanced Research Projects Agency, alternate name for ARPA
DOD	Department of Defense
DOJ	Department of Justice
FBI	Federal Bureau of Investigation, one of many Federal investigative Agencies that investigate violations of federal law
IO	Information Operations, military operations in information realm
IP	Internet Protocol, a specific format for Internet packet headers
IW	Information Warfare, part of information operations
NCP	Network Control Protocol
NSA	National Security Agency
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
WWW	World Wide Web

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I am very grateful for the advice and assistance of my thesis advisors. Professor Mikhail Tsypkin's cooperation and encouragement was very helpful as I developed my thesis from early ideas into final form. I greatly appreciate Professor Dorothy Denning's advice and encouragement that helped me move my thesis away from extraneous issues, and helped me focus on ideas that I really was more interested in developing. My advisors provided valuable insights as I developed this thesis.

I am very appreciative of those who answered questions related to the technical and legal issues. Capt Francis Afinidad, U. S. Air Force, answered my technical questions; and Russ Jokinen, Customs and Border Protection, helped me understand current law regarding Customs authority.

I also appreciate the assistance of my friends Dan Helms and David Britton who provided aid and encouragement

I would also like to thank my wife, MiKyong, and my children for their patience and understanding, as I worked through the writing process.

Saving the most important for last I want to acknowledge that if I have any good ideas to offer, I credit them to Providence, the source of all original good ideas.

THIS PAGE INTENTIONALLY LEFT BLANK

I. OVERVIEW

A. INTRODUCTION

National sovereignty is a foundational principle of national security and the modern international system. This principle is most strongly expressed in connection with the laws and practices of nations as they protect their geographical border. The international system, international law and practice, and constitutionally vetted United States law clearly recognize the right of the US as a sovereign nation to protect its borders and establish systems for controlling goods and people that cross them. Since national sovereignty is such a vital principle, it is a curious aspect of the emerging 21st Century world that within the realm of cyberspace most nations, including the United States, have either ignored or abdicated the normal responsibility of inspection and control regarding data crossing these same boundaries via the Internet. The central idea of this thesis asserts that national sovereignty inherently and logically endows a sovereign state, such as the United States, the right to establish an appropriate regime of Internet inspection stations. These stations would be used to inspect suspicious inbound traffic and block contraband analogous to the standard inspection regimes used to inspect people and goods entering the US through physical borders. Two questions arise when considering this idea. Are Internet border inspection stations feasible? And would they be worthwhile? This thesis will offer answers to these questions and other related questions.

B. INTERNET HISTORY AND CONVENTIONAL WISDOM

If national sovereignty is as clear and important a principal as is argued here**,** then why has it not been asserted in the form of Internet border inspection stations up to this point? Chapter II will seek to provide an answer to this question by examining the history and path of development of the early Internet. Understanding the way the early Internet developed will show why there has been little consideration of asserting national sovereignty, and no consideration of Internet border inspections until now. It will explain

why the current environment makes the question meaningful and relevant today. The Internet was initially built by researchers and academics who established the early structures without any significant thought about borders. Their primary goal was to build a communication architecture that would facilitate the free flow of ideas and reliably transport data. The Internet has changed from this early environment into the current environment, in which security concerns play a central role.

Chapter II will also describe how national sovereignty has been asserted in cyberspace in two forms other than Internet border inspection. It has been asserted by the United States and other countries in the form of legal jurisdiction related to the Internet, and by some authoritarian regimes in the form of controlling what would be considered in the United States to be protected speech. Chapter II will also describe some other important trends in asserting national sovereignty on the Internet including the current US National Cyber Security Strategy.

C. THE CASE FOR INTERNET BORDER INSPECTION

After establishing the history and the path of development of the Internet and the ways that national sovereignty has been asserted on the Internet, the groundwork will have been laid to build the case for Internet inspection at the border. Chapter III will build this case by first laying out the principle that it is logical to use legal precedents set in the physical world to derive principles for the Internet. Examples from case law that show this will be described. In *O'Connor v. Ortega*, a search was conducted on an individual's office including the desk and file cabinets[1]. This case had nothing to do with computers but was later used extensively as having established the precedent for determining the threshold for needing a warrant for cases in which criminal searches were conducted on government property, including computer hard drives and information stored on computer networks. Similarly, other cases have established precedent for communications media like mail and telephones, and these precedents have been used to provide legal guidance for communications on the Internet.

1 *O'Connor v. Ortega,* 480 US 709 (1987)

After establishing that there is firm legal ground for using legal precedents established in the physical world and extending them to the realm of cyberspace, we will look at the current physical inspection regime at the borders of people and goods. The US Customs and Border Protection (CBP) agency, formerly the US Customs Service, is charged with the role of inspecting goods as they cross the border. In this role they can potentially inspect every good that legally crosses the border. Even though they do not in fact inspect every good, they examine a small but significant percentage of all goods. Since they have the right to inspect all goods, but lack the resources to inspect all, they only inspect those goods that arouse a "reasonable suspicion". The source of this suspicion can come from unusual information in customs documents or from intelligence information. This targeted approach attempts to strike the best balance between keeping out illegal goods, such as drugs and illegal weapons, and not significantly impeding the high volume of legitimate goods crossing the border. This physical model can be used to derive a principle of inspecting Internet traffic, which can include information goods of real value like software and music that cross the border via the Internet. The high volume of physical goods that cross the border can be compared to the high volume of Internet traffic crossing the border, where there is a corresponding need to minimize Internet inspections to those based on intelligence or other specific legally vetted criteria to ensure that legitimate Internet traffic is not significantly impeded. The physical inspection model will be used to derive appropriate principles, which are then applied to the Internet. Another physical world analogy that uses inspections is the processes for allowing persons to cross the border. The Bureau of Citizenship and Immigration Services (BCIS), formerly known as the Immigration and Naturalization Service (INS), has the authority and responsibility to inspect persons who seek to legally cross the borders of the United States. One of the primary goals of this policy is to keep out criminals and other undesirable persons from coming into the US. Criminals can "virtually" cross the US border by using the Internet, bypassing normal BCIS procedures; and then use computer tools to break into computers and commit crimes including trespass, theft, fraud, or other malicious activity on computers and against victims located within US borders, even though the criminal remains physically outside the US when they are initiating this activity. This ability to cross the border is narrow but significant,

and the relevance will be described as it relates to Internet border inspections. Both the Customs and BCIS models of inspection will be described in more detail, and applied to build the case for establishing an Internet border inspection.

Even though there are important and useful analogies for inspection at the borders in physical space that could be used for formulating the appropriate structures for border inspection in cyberspace, there are of course some significant differences between physical space and cyberspace. The physical metaphors are useful and even can serve as legal precedent but they are not exact analogs. The final part of Chapter III will discuss some of the most significant differences. Wiretap laws and telephone systems also are models from which legal precedent and logical analogies can be derived for cyberspace. A telephone can be used as an instrument of crime, but most telephone crime occurs during the course of a telephone conversation. There are exceptions that might involve voicemail but non-conversational based telephone crime does not compare in scale to the hacker activity on the Internet. Hackers can much more directly engage in trespass, theft, espionage, or destruction, without anyone on the other end being aware of the crime at the time. The similarities and differences between the telephone network and the Internet will be discussed. This section will also discuss the relevance of these similarities and differences as they apply to border inspection.

After having discussed the physical world models and the ways they can be used to derive and set legal precedent for a model of inspection in cyberspace, Chapter III will discuss current real structures on the Internet. Precedents have already been set by laws for devices like network firewalls, which are used by various users and enterprises on the Internet. Precedents such as this will be discussed to explore how legal and technical structures already on the Internet could be applied at a national level rather than just a local level. Network firewalls do function as a local network boundary inspection station, and often much more, but it will be useful to describe the similarities and differences between national Internet border inspection and the function of firewalls. From all the examples given in Chapter III a case will be built describing the logic of Internet border inspection.

D. USES OF INTERNET BORDER INSPECTION

Once a logical case has been built to establish a precedent for border inspection in cyberspace, the case begs the question: "What would such an inspection station be used for?" If such inspection is not necessary or useful, then it would not be rational to put such a structure in place. It is useful to emphasize the point that Internet border inspection could be used for abuse or it could be designed for very beneficial purposes. A general implementation with some specific characteristics will be described in this thesis. The design would seek to minimize the potential for abuse while still obtaining significant potential benefits. The idea of establishing a national level system that could monitor some traffic on the Internet conjures up in many the fear that it could be used for some nefarious Orwellian purpose to keep tabs on the activities of normal users of the Internet. The structure proposed in this thesis would be based on inspecting Internet traffic only from specific foreign Internet Protocol (IP) addresses. The implementation would not examine the content of any traffic crossing the border except the traffic from legally vetted foreign Internet addresses. The overwhelming majority of Internet traffic would pass the inspection station without any examination of content and without any record of its passing. This proposed structure is a stark contrast to the implementation of Internet controls established by authoritarian regimes. Regimes such as China have established extensive measures to monitor and control access of their citizens as they connect to the Internet. Some critics have euphemistically called this the "Great Firewall of China". The restrictive policies and intent of the Chinese system have been used to restrict free communication of political ideas and monitor and restrict the communication of peaceful political opposition groups.

There is no intent in this proposal to use Internet border inspection stations to restrict or even monitor legitimate Internet traffic, just like it is not the intent of US Customs to monitor or restrict traffic in legitimate goods. The intent of this Internet border inspection proposal would be to support properly judicially reviewed and appropriately overseen legitimate inspection, law enforcement, and intelligence activities. A later chapter will describe some of the technical and administrative measures that would work to prevent the abuse of this system.

Just as US Customs tries to prevent contraband from crossing the border for physical goods such as drugs, the Internet border inspections could prevent contraband such as child pornography from crossing the border by blocking Internet traffic crossing the border from known child pornography sites. Such a measure would not prevent all child pornography from entering the United States, but it could be used to gain a significant new ability to counter the volumes of child pornography currently crossing the border via the Internet.

Another way that Internet inspection could be used is similar to the way physical searches detecting contraband are used. Sometimes Federal Agents working for Customs do not block contraband from coming into the US, but instead they allow the contraband to cross while they keep it under surveillance to determine the intended recipient. A similar method could be used to follow Internet contraband to the person requesting it to aid in legitimate investigation and prosecution of criminals. It also could be used to monitor Internet communications crossing the border from foreign Internet addresses which had been reviewed through due process legal procedures and determined to be involved in communication between terrorist leaders or hostile foreign powers outside the United States to their operatives inside the US. Imagine US Federal Agents being able to monitor Internet traffic from a particular Internet address of Al Q'aida controllers in a foreign country to all of their operatives inside the US. Currently if a terrorist operative has been identified inside the US and a request for monitoring the operative's communications passes through a due process legal review, then Law Enforcement investigators could monitor all communication to and from the operative only, they could not monitor all communication from the controller in the foreign country, but only the communication to the single identified operative. It would be a boon to law enforcement if they could identify a communications point such as an IP address in a foreign country used by hostile agents. They could then identify all the Internet communication the hostile agents were sending into the US by watching for Internet traffic crossing the US border from that hostile IP address. This hypothetical scenario would include full due process to ensure legitimate Internet traffic that crosses the border would by default not be monitored at all as was previously described. Chapter III will also include a description of some other ways the Internet inspection process could potentially be used

for legitimate assertion of national sovereignty as well to include blocking of hostile Internet addresses and the potential implementation of information embargoes against hostile powers.

E. FEASIBILITY OF INSPECTION

An idea may be logically derived in principle and even potentially useful, but if the idea is technically or legally infeasible then it amounts to fantasy or science fiction. Chapter IV will examine technical feasibility of Internet border inspection, Chapter V will examine the legal feasibility, and Chapter VI will discuss important issues related to political feasibility.

Chapter IV is not intended to be a technical paper and will not delve into low-level technical details. It will describe some of the high level issues and the principles of technical implementation. There are some with technical backgrounds who will understand the nature of the Internet's structure and even some of the details of the equipment that passes the data from place to place around the globe in a manner that largely ignores legal structures such as national borders. There are others who have legal or political backgrounds who are not familiar with the technical details. We will seek to strike a balance by explaining the key high-level technical aspects to those who are not familiar with such aspects without going into too much technical detail. At the same time we will point out the key technical aspects that show that this idea is technically feasible. Technical issues that will be addressed include a discussion of the structure of the Internet backbones such as the trans-oceanic cables and other backbone elements that cross the border, where Internet border inspection stations could be set up; and the handling of the packets of data in that structure. Almost all packets would pass through the inspection station without any content being examined and no information from legitimate packets would be retained. Only packets from previously identified suspicious sources would be examined in accordance with appropriate legal procedures. These and related details will be examined in the discussion of technical feasibility.

Chapter V examines the legal feasibility. This will not be a detailed legal brief, but should provide a framework for examining the key legal issues and will provide some

additional understanding for readers who are less familiar with some of the legal issues related to the Internet. This examination will look at both, the key constitutional provisions that relate to border inspection and communication such as the Internet, and how a technical implementation of this idea would avoid overly broad inspection to ensure protection of constitutional rights. Chapter V will also examine the international law framework dealing with cybercrime to show that there is no current legal bar to implementation from this realm. Since the current laws within the United States are not currently sufficient to implement Internet border inspection, some of the changes in the law needed for implementation will also be described.

F. POLITICAL FEASIBILITY

Political solutions are not as precisely analyzed as technical solutions, but are just as vital to implementation. Chapter VI will discuss the importance of the political aspects, and will identify the key political issues that will need to be considered while designing a system for Internet border inspection. Issues of privacy and free speech are considered in the context of this proposal. Some will fear that implementation of this structure will be like the establishment of an American version of the "Great Firewall of China", which is used to restrict free expression. We will describe why this structure is fundamentally different and how it can provide a net benefit rather than a net detriment to the national interest of Americans. Another issue that will be discussed is the role of proper legal oversight and training in preventing potential abuse. Politics of course can extend beyond the borders of a country and there is likely to be some significant resistance from certain international actors outside the United States if the US were to assert its national sovereignty even more explicitly on the Internet. The United States is already an information superpower, and it plays a dominant role on the Internet**.** Exerting national-level controls on Internet traffic would increase US power over the Internet. Some nations are concerned about the growth of US power and may feel threatened by the US building up even more. Chapter VI will discuss such issues and how they might be addressed. If such concerns are not adequately dealt with up front, the whole idea may be held back indefinitely.

G. CONCLUSION

Chapter VII will discuss some of the overall conclusions and provide policy recommendations. It will also point out areas that this paper could not address in appropriate detail. These areas are ripe for further discussion or study

. .

THIS PAGE INTENTIONALLY LEFT BLANK

II. INTERNET HISTORY AND CONVENTIONAL WISDOM

Although sovereign states have the right to inspect traffic in people and goods crossing its borders, traffic on the Internet has not been inspected. This thesis asserts that logical precedent can be derived from inspection of people and goods and applied to the Internet. But if this is as clear a principle as asserted here then it is important to understand why inspection has not yet been implemented. To understand this it is necessary to understand the historical development of the Internet. This is not an exhaustive history but rather one that describes the path of development and motives of those who contributed to building the Internet. The goal is to explain why development did not at first lead naturally toward the notion of applying the principles of security and national sovereignty, but instead at first emphasized other principles such as the free sharing of ideas, and later privacy. It is easy to see that in recent years the costs and value of resources on the Internet have fundamentally changed the nature of the Internet from the academic and research environment where it was born, into an Internet where huge economic and security interests now play an increasingly central role. While it was not originally a place that may have needed inspections at the borders, it is now an environment where such ideas deserve more serious consideration. This chapter will also describe the current conventional wisdom concerning the Internet related to border inspection.

A. BRIEF INTERNET HISTORY

The concepts leading to the Internet were developed in the early 1960's by researchers and academics working under contract for the Department of Defense (DOD). DOD delegated the work to the Advanced Research Projects Agency (ARPA). ARPA was the central agency sponsoring the research and much of the initial work was done for ARPA by RAND Corporation, a defense think tank. There were two motives initially for building the structure that became the Internet. The first was to build a telecommunications command and control structure that could survive a nuclear attack. The second was to be able to share the scarce computer resources in that period among

researchers and academics across an all-digital network. One of the first documents describing this was written by Paul Baran at RAND in 1964, "On Distributed Communication"[2]. This document described these motives and discussed key technical details such as the multi-path packet switched data network that formed the Internet. The RAND document states "the Memorandum is directed toward examining the use of redundancy as one means of building communications systems to withstand heavy enemy attacks." It goes on to establish "The requirements for a future all-digital-data distributed network which provides common user service for a wide range of users having different requirements is considered".[3] This document described the foundational concepts that would eventually be developed into the architecture of the Internet. It is important to note that these initial steps of development envisioned a network that would be built within the US borders, and thus there was no need to even consider border inspection. In addition, the second goal of sharing computer resources set the path toward openness and trust, again without regard to borders or inspection.

In 1966 the plans for the ARPANET had been developed and by 1969 DOD had built ARPANET, a network used to conduct research on computer networking. By the end of the year ARPANET had four nodes up and running. This was a single geographically dispersed network, but it was not yet a network of networks, or Internet. However ARPANET and the networks built from the same principles would become the backbone of the Internet, thereby establishing a precedent for a structure based on openness and trust.

In 1971 ARPANET had grown to 15 sites with 23 host computers. The network was used for remote login, file sharing and data transport between hosts, and electronic mail. Email emphasized its nature as a communications medium for research, rather than its nature as a communications medium for military command and control, and became one of the most popular features of the network. Email traversing the network allowed for the potential exchange of private information. Privacy may not have been an important concern at this point of development, but later privacy advocates would be very concerned about the private nature of some communications, such as email.

---

[2] Paul Baran. *On Distributed Communications*. 1964, RAND Corporation: Santa Monica, CA.

[3] Ibid. Preface & Summary.

Development continued and more site nodes and computer hosts were added. The driving principles of research, openness, and trust continued; and in 1974 the first international borders were crossed when the University College of London, England, was connected to ARPANET. Research was the goal, and because there was no economic traffic, criminal activity, or contraband, there was no reason to consider international border inspections. The primary boundary of national sovereignty had been crossed without a real need or significant consideration for border inspection, and this helped set a precedent for treating Internet traffic differently from people and goods that cross the same physical borders. Significantly the primary connections between the nodes of the ARPANET were dedicated telephone lines used for data only. This also helped to establish the precedent that computer networks were a communications medium, more like the telephone than a medium where information goods, like software and music, would later cross legal boundaries on a routine basis. It was primarily just a communications medium at the time, but it grew to become much more. Now it is a medium where goods and contraband can cross borders, and crimes can be committed without any check at the borders. The interpersonal communication aspect of the ARPANET was shown to be a growing part of the network in the results of a 1973 ARPA study, which showed email composed 75% of all ARPANET traffic[4].

The structure of networked computers was expanded to the commercial sector in 1974 when the company BBN opened Telenet, the first public packet data service. BBN was originally started as a research team led by MIT professors Richard Bolt, Leo Beranek, and Robert Newman. The BBN team built key components of the early ARPANET, and members of the expanded team continued to play key roles in the early development of ARPANET and other networks like it.

By 1979 the expanding network structure began to show other moves away from its original research purposes. At this time USENET was established, which set up a news group service. This service collected messages related to a specific topic that any user could access, and this service expanded to encompass a vast array of topics. Entertainment debuted with the first multi-user computer game called MUD, also known

[4] Timeline of Internet Development, http://www.zakon.org/robert/Internet/timeline/, 4 May 2003.

as MUD1. In this period of the mid-70's a new phase began and the motives for further development began to change. This started the network that would soon be called the Internet down a path that was more commercial, and away from the almost pure research or national defense origins of the ARPANET.

At the same time the physical structure of the Internet was expanding the software and technical standards were being developed. The protocol for sending data across these networks had developed over the years and in 1982 DOD decided to change from the older Network Control Protocol to the newer Transmission Control Protocol/Internet Protocol (TCP/IP). This was a protocol that would increasingly be used across the ARPANET and is still the primary method of sending data across the Internet.[5] Since TCP/IP was implemented to facilitate the transmission of information from one network to another this could be described as a change that marked the beginning of a true "Internet", and this is when the term was first used. Also in 1982 four European countries created new cross border connections as the United Kingdom, Netherlands, Denmark, and Sweden built the European UNIX Network (EUnet). In this time period the same conditions existed which had previously made international borders a barely significant consideration, and inspection was still almost certainly not even a passing thought.

As the year 1984 arrived, the Internet had grown to 1,000 host computers and connected networks across several countries. During this year many people reflected on George Orwell's fictional setting of total authoritarian world domination, and almost perpetual surveillance using modern technologies described in his book "1984".[6] The Internet had not taken on any of the aspects of Orwell's dystopia at this time, but critics of government involvement in the Internet would later use Orwellian terms such as "Big Brother" to voice their concerns about the potential for oppressive government surveillance on the Internet. 1984 was also the year that Russia connected to USENET, which by now also included West Germany, Japan, and South Korea. Also in this year the author William Gibson wrote the book Neuromancer and coined the word

---

[5] Dern, Daniel P. *The Internet Guide for New Users*. McGraw- Hill, Inc., New York, 1994.

[6] Orwell, G. *Nineteen eighty-four*. 1984, Oxford New York: Clarendon Press; Oxford University Press.

"Cyberspace".[7] Personal computers were becoming affordable to a growing mass of home users. While most home users did not typically connect to the Internet *per se*, a parallel community of computer bulletin boards was being built by individual computer users with modems who allowed others to dial directly into their computer to share information, play games, and engage in other activities. There was a significant and growing amount of private information both on the Internet and in bulletin board systems (BBSs). Later these communities would merge as dial up connections to the Internet became more commonly available and the type of content once put on bulletin boards began to be accessible on the Internet. Still at this time minimal security was in place in many parts of the Internet. Good network computer citizenship was a primary source of security on the Internet, and strong computer security was not a primary consideration in most software development efforts. Another significant change occurred when the administration of the ARPANET backbone structure was turned over to the National Science Foundation. The ARPANET had grown far beyond the DOD's original structure for military research, and survivable command and control. Now this structure would be managed more like a public asset than a military network.

Before the end of the decade two events would occur that would highlight a new need for security on the Internet: the Morris Internet Worm in 1988 and the Hanover Hackers in 1989. By 1987 the number of hosts on the Internet had grown to 10,000, and passed 100,000 by 1989.[8] This virtual explosion of new users changed the character of the normal Internet user. The normal user had been part of the community of academics and researchers who took responsibility and good network citizenship more or less seriously. The new users were much more often curious high school or college students, and some of these took responsibility and network citizenship as challenges to be circumvented, not embraced. This change allowed the curious computer savvy individual without necessarily any research, academic, or other official position to connect and join the growing mass of users. In this mass user environment they could expect to be more anonymous than ever before. This anonymity was not really a part of the early Internet, which was built on research and openness standards. But in the growing mass of users at

[7] Gibson, William. *Neuromancer*. 1984, New York: Ace Books.

[8] Timeline of Internet Development, http://www.zakon.org/robert/Internet/timeline/, 4 May 2003.

this time, anonymity became part of the Internet culture, and it would remain a part of the culture from that time forward. This sense of anonymity motivates many otherwise law-abiding citizens to go poking around corners of the Internet where they are not allowed. Some later go on to engage in criminal hacker activity. The sense of anonymity was definitely a factor in the thinking of Robert Morris when he released his self-replicating Internet worm that overloaded very large parts of the Internet in 1988. It was an even stronger factor in the Hanover Hackers starting their espionage activity, as they gained unauthorized access to numerous sensitive computer systems and copied files for East German intelligence handlers.[9] These events showed some people that the Internet environment of freedom and openness now required more substantial security measures. However, even though some were convinced of the need for security, the culture would only gradually change over the next decade. Attacks were felt by some to be bad Internet citizenship and aberrations, not necessarily the shape of things to come.

The community of individuals concerned about free speech and privacy on the Internet had grown significantly by 1990 and a formal organization, the Electronic Frontier Foundation (EFF), was established with the goal of protecting civil liberties on the Internet. The efforts of the EFF along with other groups helped propel the Internet down the path of emphasizing civil liberties. The year 1990 also saw the first commercial provider of Internet dial-up access. This would start the merger of the bulletin board community with the Internet community. Many people were already part of both communities, but the growing number of home personal computers with modems could now start to connect directly to the Internet.

Starting in 1990 and continuing through 1991, as the US reacted to the Iraqi invasion of Kuwait, five hackers from the Netherlands established computer connections across international borders and broke into computers at 34 American military sites.[10] They gathered information on locations of US troops and ships, and other information of military importance. Some accounts allege that they offered to sell this information to

---

9 Cliff Stoll. The cuckoo's egg: tracking a spy through the maze of computer espionage. 1st ed. 1989, New York: Doubleday.

10 Dorothy Denning. Information warfare and security. 1999, New York Reading, Ma.: ACM Press ; Addison-Wesley. p. 3.

Iraq.[11] US investigators identified the individuals they believed were responsible, but the hackers could not be prosecuted, because the Netherlands, where they lived and initiated the crime, did not have laws against such intrusions at the time. National sovereignty was asserted to protect the citizens of one country from being prosecuted by another country, even though the individuals had electronically crossed the border, connected to computers, and stolen information on US soil. This event illustrates one of the primary ways the principle of national sovereignty has been most consistently asserted related to the Internet, in the form of establishing legal jurisdiction for crimes and investigations. It also highlights the potential importance of security on the Internet. Security had been an important concern to a very small but important community of experts in the Internet community before this time, but this community had grown significantly by this time. Despite this, security would not be an important issue in the awareness of most users until much later.

The World Wide Web was developed in 1991 by researchers at CERN, the European Organization for Nuclear Research. This event would lead to expansion in the popularity of connecting to the Internet beyond a relatively small population, who enjoyed the technical nature of the Internet, to a mass of less technically oriented users. The Internet up to this time was almost entirely composed of text based content and programs. With the advent of the Web, users would begin to interact with the Internet in what would develop into the now familiar "point and click" environment. Though many technical people are aware that the Web is just one application running on the Internet, a vast portion of those who use the Web think of the Web and the Internet as being the same thing. There are of course many other aspects of the Internet besides the Web. Even non-technical users use applications such as email that typically use different services for sending information. The importance of the distinction is not about the technical aspects but more about the users who connect to the Internet. The vast majority do not understand or care about the technical details taking place behind the scenes. The technical tools and techniques used for criminal activity are also not of interest to them. They are more concerned with privacy and free access. These users also connect to web sites either more or less aware of their anonymity. They are even advised for privacy

[11] Ibid. p 4.

purposes to remain anonymous. Establishment of Internet inspection at the border will probably be uncomfortable to such users, even if it will be unlikely to impact them at all. Only if they have a good understanding of the idea and the current threat will they be likely to consider it palatable.

The development and expansion of the Web and the growing number of people connecting to the Internet began to catch the attention of businesses and the news media by 1993. This period could be described as a new phase of the Internet. It would be from this time forward that commercial interests would grow to dominate the Internet. Now e-commerce represents countless billions of dollars of total value depending on how you appraise the infrastructure. By 1994 Web traffic had become the 2nd most popular service on the Internet, and it would be the most popular service by 1995.[12] 1994 would be the year that the first cyber-bank would open for business, representing the ability to directly conduct monetary transactions. 1995 would see a number of Internet related companies enter the stock market as Initial Public Offerings. Netscape would be the third largest ever IPO share value at the time. The commercial aspect of the net was rapidly developing.

The vast expansion of the Internet in new countries and the growth of content on the Web led a number of countries to assert their national authority by restricting access to the Internet. By 1996 certain oppressive regimes had placed restrictions on political and religious content. This is significant because it represents the beginning of a trend for nations asserting more strongly their national sovereignty on the Internet, in a new form that was more than just legal jurisdiction. Like all government assertion of national sovereignty, authority can be used for purposes that appropriately balance freedom and security, or it can be used for oppression. The principle of asserting national authority without consideration of its purpose is morally neutral. The purposes and ends can make it morally good or bad. Nonetheless nations started in this period to more strongly assert their sovereignty and authority, and this trend has continued.

Many developments occurred over the next few years but most were continuations of trends already identified previously or they were of a more technical

12 Timeline – History of the Internet. http://www.zakon.org/robert/internet/timeline/. May 10, 2003.

nature. In 1999 two events helped mark the growing importance of security in Cyberspace, the release of the "Melissa" virus, and the "information war" that was waged between US led NATO forces and their sympathizers against Yugoslavian Serb forces and their sympathizers regarding Kosovo. Computer viruses, and other malicious code, had been part of the Internet environment since the "Morris Worm", but that event had impacted the Internet community when it still was largely composed of researchers and academics. The "Melissa" virus was an event that impacted a greatly expanded population of computer users and organizations. The Computer Emergency Response Team (CERT) located at Carnegie Mellon University described the impact.

> The Melissa virus represents a new level of sophistication in the progression of computer viruses. Melissa's impact is so great because it exploits, in a very simple and clever way, the power that has been built into the flexible and expressive technologies in use on the Internet today. It also exploits the high level of connectivity brought about by the Internet and the informal rules people commonly use when handling electronic mail.[13]

The US Department of Justice in December 1999 received a guilty plea to federal and state charges from the creator of the virus, David Smith, and reported the estimated damages at more than $80 million. Robert Cleary, the US Attorney who led prosecution of the case, stated, "The Melissa virus demonstrated the danger that business, government and personal computer users everywhere face in our technological society… Far from being a mere nuisance, Melissa infected computers and disabled computer networks throughout North America."[14] A key impact of "Melissa" was that it brought security concerns into the mass consciousness of average Internet users. Internet security moved from being just an abstract idea, to an issue that had real and tangible impacts on many individuals at the same time from a single source.

In the same year, the US military led NATO forces in Operation Allied Force, a campaign to stop Serbian forces that sought to push the ethnic Albanian majority out of the territory in Yugoslavia known as Kosovo. This military action was primarily conducted in the form of a NATO air campaign of precision bombing. However a small

---

[13] Testimony of Richard Pethia before the Subcommittee on Technology, Committee on Science, U.S. House of Representatives April 15, 1999.

[14] Press Release US Dept. of Justice, http://www.usdoj.gov/criminal/cybercrime/melissa.htm . May 8, 2003.

but significant part of the military strategy and tactics of both sides included the use of methods referred to in the US as "information warfare". This term meant many things when it was used at the time, and these are not discussed here, but it included the use of cyberspace to gain military and diplomatic advantage. Both sides conducted information operations on the Internet. Hackers sympathetic to the Serbian cause conducted denial of service attacks on US and NATO Internet sites, and defaced other web pages with content expressing anti-US and anti-NATO sentiments. The Serbian government controlled content on many web pages and other media within their border for propaganda purposes. US forces also used the Internet to get out its messages through web pages and email to support public affairs and psychological operations.[15] All of this activity was significant in the context of this analysis, because national sovereignty was expressed again in a new form in cyberspace, this time in the form of countries using the Internet in support of military and diplomatic objectives during a time of war.

Security awareness in the community of Internet users has now moved from a peripheral interest to an issue of central importance in the last several years. Some of the events that demonstrate this are the reactions to the various major computer virus events, which have regularly impacted Internet operations for individuals and organizations worldwide. The year 2001 had several major malicious software events including "Code Red", "Nimda", "Sir Cam", and "BadTrans". Partly as a reaction to these and other virus and computer hacking incidents, significant changes have been made on the part of software developers to make security a more central concern in software development. Microsoft announced in Jan 2002 that it would make "trustworthy computing" the highest company priority.[16]

Another event occurred outside of cyberspace in 2001 that has had important implications for security and asserting national sovereignty. The attack on the United States on September 11, 2001 by international terrorists would have profound implications both outside cyberspace and within. The results of this highlighted the importance of security to the people from the top levels of government to the common

[15] Denning, D.E. *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*. in *Internet and International Systems: Information Technology and American Foreign Policy Decisionmaking Workshop*. 1999. Georgetown Univ.

[16] http://www.computerworld.com/securitytopics/security/story/0,10801,67461,00.html

citizen of the United States, and for many people around the world. The US government responded in two key ways related first to the Internet, and second to national border inspections. The first was the passage of the USA PATRIOT Act.[17] This act significantly updated laws related to investigating terrorism, but also updated laws related to the Internet. These changes streamlined certain legal procedures and changed the way intelligence investigations and criminal investigations could be coordinated. The USA PATRIOT Act aided law enforcement officials significantly in investigating terrorism and other crime both in and out of cyberspace. The US government also reevaluated the importance of border inspections for both people and goods. A new cabinet level position was created and a major reorganization of governmental structures was implemented creating the Department of Homeland Security. These changes mark a very significant increase in the importance of security and inspection procedures at the borders.

In summary this history has described the current environment in which inspection of Internet traffic at the borders will be considered. The Internet initially was established on a path of openness without regard to borders. It developed as an increasingly important mode of communication in which privacy was a growing consideration. It continued to grow as an increasingly important commercial interest in which security was seen as a secondary concern to progress. Crime and malicious logic started and grew on the Internet and security became more important. While the initial and early path of development did not need to concern itself with borders and inspections, the current environment is one in which ideas like this need new consideration.

B. CONVENTIONAL WISDOM

A review of the history of the Internet provides some understanding of the conventional wisdom regarding the appropriate role of government and inspection on the Internet. It is important for this thesis to point out that there are two perspectives in evaluating the current conventional wisdom. There is a broad perspective which

[17] H.R. 3162. *USA PATRIOT Act*. 2001. p. 184.

examines the larger issues related to government surveillance, which are currently being debated in discussions about the USA Patriot Act[18] and the research on Total Information Awareness[19] project. And there is a narrow perspective, which would examine conventional wisdom on the specific issue of Internet border inspections. From the broad perspective there is a significant amount of debate, and a significant body of conventional wisdom from opposing sides of the debate. As for the narrow perspective, there has been almost nothing written about this specific topic. All conventional wisdom would be derived from the broader debate and consideration of ideas discussed in this thesis.

1. Conventional Wisdom: The Broad Perspective

The historical review describing the initial development of the Internet showed that the Internet was established as a place of openness and free sharing of ideas without consideration of border inspections. This has been extended by some into the idea that the Internet is something completely new and outside the normal paradigms of law and communication. One privacy advocate, John Barlow, described this view in a 1996 Time magazine article.

> The real issue is control. The Internet is too widespread to be easily dominated by any single government. By creating a seamless global-economic zone, borderless and unregulatable, the Internet calls into question the very idea of a nation-state. No wonder nation-states are rushing to get their levers of control into cyberspace while less than 1% of the world's population is online.[20]

Those with opinions that oppose or question the government's ability to even attempt to monitor Internet communication have been organized into groups like the Electronic Frontier Foundation (EFF), which Barlow co-founded, and the Electronic Privacy Information Center (EPIC), among others.[21]

There is another large part of the Internet community that is strongly concerned about the security on the Internet. While small in the early seventies, this community has

---

[18] USA PATRIOT Act – text. http://thomas.loc.gov. 9-May-03

[19] Total Information Awareness, DARPA, http://www.darpa.mil/iao/TIASystems.htm. 9-May-03

[20] Barlow, J.P., *Thinking Locally, Acting Globally*, Time Magazine. Jan 15, 1996. p. 57

[21] EPIC Online Guide to Privacy Resources. http://epic.org/privacy/privacy_resources_faq.html. May 10, 2003.

grown into a diverse, multi-billion dollar per year computer security industry.[22] Perhaps because of its size and diversity, the security industry has not produced a consensus of opinion on the proper role of government monitoring. Some support a strong role for government in providing security and others see a greater role for the private sector in providing security. These solutions are not mutually exclusive, and in fact can be very complementary. But there can be a significant difference of opinion.

From all the diverse opinions, three general positions may be described. The first group is composed of privacy advocates who have great concern about the government's ability to monitor, particularly in light of the USA PATRIOT Act and the Total Information Awareness project. The second group is made up of security advocates who support enhanced laws to update and streamline the technology and due process procedures used to investigate crime on the Internet. The third opinion group, also security advocates, seek private and local solutions to security challenges as opposed to government solutions. Though they are not necessarily in strong opposition to the government, they may believe in at least minimizing the role of government surveillance as a solution. The US government tried to find a consensus of opinion on security at large as it developed the National Strategy to Secure Cyberspace.[23] This document describes a wide range of cyber security measures that can be taken at many levels, from governments and international cooperation, to organizations and business, and down to the individual level, encouraging private users to increase the security of their own computer systems. This document describes security monitoring on the Internet in terms of gathering data and reports of hostile activity, and seeks to do this as a cooperative effort between the public and private sector in a structure they call the National Cyberspace Security Response System. The strategy tries to address the concerns of privacy advocates as well by appointing a Privacy Officer who will oversee and address privacy concerns, and it seeks to cultivate other cooperative efforts between the public and private sectors. The National Strategy document and consensus approach do not significantly address the role of government in monitoring *per se*, and the strategy does not even consider the idea of Internet border inspection.

---

[22] Denning, Dorothy E., Cyber Security as an Emergent Infrastructure. Draft of September 6, 2002, p. 1

[23] National Strategy to Secure Cyberspace. http://www.whitehouse.gov/pcipb/. May 10, 2003.

2. Conventional Wisdom: The Narrow Perspective

The conventional wisdom related to the specific idea of Internet border inspection can be summarized fairly succinctly. A review of literature revealed that some have written about the ideas of national sovereignty and the Internet.[24] This literature primarily addresses legal jurisdiction or addresses larger political science considerations. There is a larger body of writing which deals with matters regarding national security, which specifically addresses information operations or information warfare, and this describes government roles in national defense on the Internet, but this literature does not significantly address the specific role of Internet border inspection. Another body of writing has described the policies of authoritarian countries like China that have established a national infrastructure to monitor and block Internet access with the intent of limiting freedom of political expression and organization. Other countries prohibit Internet access to sites that offend government political or religious sensibilities. The literature search did not uncover anything that specifically addressed the issue of Internet border inspection within the US. Only one article was found that described defining "Electronic Borders" on a national scale within the United States for security purposes.[25] Experts who were interviewed during the course of research for this topic, who are familiar with issues of Internet security, often expressed opinions related to the technical, legal, or political difficulties of implementation, but none identified any significant literature on the topic.

---

[24] Jerry Everard. *Virtual States: The Internet and the Boundaries of the Nation-State*. Routledge, New York, New York. 2000.

[25] J.E. Molini. *Electronic Borders: Defining and Protecting National Networks*. Computers & Security, 1997. **16**(3). p. 189-196.

III. THE LOGICAL CASE FOR BORDER INSPECTION

The logic of establishing Internet border inspection is built by extending current legal concepts that apply to physical border inspections to cyberspace. This chapter will build a logical case for Internet border inspection and describe how such a system might be used. Descriptions of legal principles are not intended to be a formal legal analysis but rather to provide a general understanding of the relevant ideas. This chapter will not address all of the legal aspects that would need to be considered before establishing such a system; a more detailed discussion is deferred until Chapter V. This chapter will also not address all of the technical issues, leaving those for Chapter IV.

A. THE LOGICAL CASE FOR BORDER INSPECTION

1. National Sovereignty

The idea of Internet border inspections rests upon the fundamental principle of national sovereignty. The current international system, and the structure of national laws, including the United States Constitution, broadly recognizes this principle. National sovereignty was established as a foundational part of the international system in the negotiations of the peace treaty of Westphalia, which was the settlement at the end of the Thirty Years War in Europe in 1648.[26] This set up a kind of 'golden rule' of the international community among sovereign states. The specific nature of the principle of national sovereignty has changed somewhat since that time, but still remains a foundation of the modern international system. States that have achieved international recognition are acknowledged as having sovereign rights at their borders and in all territory within. This idea has a vast array of implications, most of which do not apply to this discussion, but there are certain key elements which do apply. A sovereign nation-state has the right to maintain secure borders. This includes the legal right to permit or not permit any or all people, goods, or communications from crossing the borders. A state may choose not to fully exercise this recognized right, or a state may not have the means to enforce

[26] Watson, A., *The evolution of international society: a comparative historical analysis*. 1992, London ; New York: Routledge.

complete compliance. It may also choose to pass laws restricting the application of this principle for the benefit of its citizens, or enter into international agreements that also limit the application of this right. However, exercised or not, the principle remains, and the right of a state to exercise control of its borders is strongly recognized. The governments of countries usually in fact typically exercise this right in many ways short of the maximum extent. No person, good, or traffic inherently has the right to cross the border of a sovereign country without permission, according to this principle, but governments choose to limit the application based on their own laws and international agreements. In the United States, there are numerous ways the government has chosen not to apply the right, and some important ways the government exercises the right. If a national government like the US government decides to allow at least some goods, people, and traffic to cross the border, and still maintain the right to deny entry of others, then logically it must inspect the people or goods to determine what will be allowed to pass.

2. Physical Border Inspection

The two most visible ways the US government performs this are through the inspection of goods, which is delegated to the US Customs and Border Protection (CBP) agency, formerly the US Customs Service, and the inspection of people, which is delegated to the Bureau of Citizenship and Immigration Service (BCIS), formerly known as the Immigration and Naturalization Service (INS). A huge volume of goods crosses the US borders, and even though Customs has a right to inspect all of it directly, they let the vast majority enter or leave with only a cursory inspection of accompanying documents or another expediting procedure. These documents could include a customs declaration or a bill of lading by the party responsible for the goods indicating that no illegal goods are crossing the border, or similar information input into the Customs computer system. Of course a system that does not inspect all goods crossing the border will encourage some, who are not concerned about breaking laws, to attempt to bring across illegal goods. To deter this behavior and actually attempt to keep out a maximum amount of illegal goods, Customs uses a screening process that looks for suspicious activity that may be an indicator of attempted smuggling, and they use their inspection authority to examine in greater detail those goods that arouse reasonable suspicion. The

US Customs describes this authority as "broad authority to conduct searches of persons and their baggage, cargo, and means of transportation entering the United States. The courts have also held that this search, seizure, and arrest authority is not dependent upon either probable cause or a search warrant as is required by police."[27] US Customs also inspects suspicious goods or shipments that have been identified by intelligence information to be possibly carrying illegal goods. This model, of inspecting a small portion of the massive traffic in goods based on reasonable suspicion or intelligence information, shows two things relevant to building the case for Internet inspections. First, it shows a current example of real inspections at the borders. Second, it shows elements of a model of how Internet border inspections might work. Internet inspections would also have to deal with very large volumes of traffic, and would need to minimize inspections to only traffic that is suspicious or had been identified by intelligence information as warranting inspection. This implementation of this idea will be expanded upon in the discussion of technical feasibility.

It is important to understand some key points related to US Customs authority. The laws that describe Customs authority are not the original source of the right to inspect. The original right to control the borders is inherent to the US Government as a sovereign country. Congress has been delegated under the US Constitution the right to pass laws related to control of the borders. Congress has further delegated a portion of that authority to be executed by Customs and Border Protection agents under the executive branch of government. As long as there is no limitation set by the US Constitution on what can be inspected, Congress has the authority to pass laws regarding inspections and other controls at the border, including potentially Internet border inspections

In close parallel with the authority granted to Customs, the Bureau of Citizenship and Immigration Services has been delegated the authority to inspect persons seeking entry into the United States. "An inspector has authority to search without warrant the person and effects of any person seeking admission, when there is reason to believe that grounds of exclusion exist which would be disclosed by such search."[28] The authority of

[27] US Customs Inspections - Right to Search. http://www.customs.ustreas.gov/. May 10, 2003

[28] Immigration Inspection Program authority. http://www.immigration.gov/. May 10, 2003.

CBP and BCIS is part of the Constitutionally vetted authority to perform inspections and searches that would normally not be allowed without a warrant if they were conducted within the territory of the US, but this extraordinary authority is allowed at the borders. The border is a special legal zone for inspections.

3. Extending Inspection to Cyberspace

We have at this point described the extraordinary authority to inspect and search people and goods in the physical realm at the borders. Next we will examine how this could be extended to cyberspace. The US legal system is derived from the British Common Law tradition. This means that legal decisions are derived primarily from interpretation of written law, but additionally the precedents set in one case can be considered and held as legally applicable in the judicial decisions of subsequent cases. US Supreme Court cases are the most familiar form of this to most Americans who are not legal scholars. A well-known non-cyber related example is when the Supreme Court heard the case of *Roe vs. Wade*[29] and described certain legal principles in the majority ruling. This particular case is used only as an example of well-known case law, not for any principles applied to cyberspace. All other courts throughout the US must consider the principles from *Roe* when they are relevant before they can make a final ruling. Even new cases, where new reproductive technologies have direct bearing on the case, can look within the whole body of previous rulings to find legal principles that might be appropriately applied, even though the current laws on the books did not anticipate the new technologies. The point here is legal principles and current laws are considered together to make legal decisions, and legal principles derived from one case can be extended to other situations.

From the common law legal tradition cases involving the proper method of obtaining search warrants for evidence contained on computers could be adjudicated even though new laws had not yet been passed that particularly detailed how Congress wanted search warrants to be handled relating to computers. The US Department of Justice (DOJ), Computer Crime and Intellectual Property Section (CCIPS) published a guide for law enforcement officials which gives examples of legal principles drawn from cases and applies them to computer crimes, even though some of them were decided outside the

realm of computers.[30] One case that exemplifies this shows how legal precedents in the physical world provide legal principles for cyberspace, and thus legally valid guidance. In the case *O'Connor v. Ortega*,[31] the courts ruled on the legality of a search of the government office and desk of a government employee, Magno Ortega. No computer was involved, but the principles were established describing when the government can search without a warrant an office assigned to one of their employees. The US Ninth Circuit Courts of Appeals upheld a lower court decision that found that the warrantless search of the government office assigned to Ortega was illegal in part because he had a "reasonable expectation of privacy" in that office. This case has been extended to apply to government computer hard drives and network storage devices, and is used to guide legal officials and investigators in deciding when they might need a warrant to search such devices. The point here is that legal principles were derived from a case in the physical world and they have been applied to the computer world. This can be extended to argue that the legal principles that already allow physical inspections at the border might also apply to the Internet. The border is a zone of special legal jurisdiction based on national sovereignty. Physical inspections have been established and it is reasonable to explore the idea that the same principles might apply allowing inspection of Internet traffic at the border as well. New laws would have to be written specifically authorizing such inspections, but the primary guiding legal principles may already be established.

4. Information Goods Crossing the Border

The argument given so far could start to build a case for Internet border inspection if one or both of two conditions exist. First, if the traffic on the Internet is similar enough to people and goods which currently cross the border; and second, if inspection properly extends beyond people and goods to also fit the traffic on the Internet. The first condition will be examined by answering the question: Is the traffic on the Internet similar enough to people and goods which currently cross the border? First we will examine goods. Many people primarily think of the Internet as a communications medium. There is at least one fundamental difference between the Internet and other electronic

---

[29] *Roe v. Wade*, 410 U.S. 113 (1973).

[30] US Dept of Justice. *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*. http://www.cybercrime.gov/s&smanual2002.htm. July 2002

[31] *O'Connor v. Ortega.* 480 US 709 (1987).

communications media: on the Internet you can actually buy, sell, ship, and receive information goods like software and digital music, and this is now commonplace. Over the telephone you can make arrangements to purchase goods but it would not be considered common to receive the goods themselves over the phone. The value of goods moving over the Internet has also continued to grow. Goods crossing the border may not be a large part of the Internet traffic but there is no question that goods with real value are crossing the border via the Internet, and they are crossing without any of the normal inspection procedures that would accompany the same material transported in the form of physical goods such as CDs or DVDs. Another specific good that can cross the border in either physical form or electronic form is child pornography, and it is contraband in both cases. If routine physical inspections identified child pornography crossing the border the goods would be seized. On the Internet there is no such inspection regime. The point here is *not* to propose that Internet inspection be established to routinely inspect content for child pornography. Physical border inspections and proposed Internet border inspections do not need to examine content unless there is a reasonable cause to do so. Instead the point to be made here is that the Internet is a place where goods with real value cross borders, and these need not inherently be considered outside the normal purview of border control. Secondly, if contraband were identified trying to cross the border, it is reasonable that a sovereign government should be allowed to block its crossing the border on the Internet. The technical details of the second point are of course important, and these will be discussed in detail in the chapter on technical feasibility. The principle being established at this point is that real goods cross the border on the Internet and a sovereign state reasonably has an interest in those goods.

There may be a fairly clear argument that goods of real value and contraband cross the border on the Internet, but it would not be apparent at first that people cross the border. In order to explain this idea, legal principles must be derived from physical space that would also apply to cyberspace. In this case we must consider some of the principles of why people are inspected at the border. People attempting to cross the border are either citizens or non-citizens. Citizens are allowed to enter but their person or property may be inspected if there is a reasonable suspicion that they may be attempting to carry contraband into the country. Non-citizens are allowed to enter if they meet a more

rigorous set of requirements intended to keep out undesirable persons.[32] There are nine broad categories of grounds for denying entry into the country: criminal activity, national security, health, lack of labor certification, likelihood of becoming a public charge, previous immigration violations, lack of proper documents, permanent ineligibility for citizenship, draft evasion and some other uncommon situations.[33] The description of the categories is useful in two respects. First it shows that the categories for exclusion are reasonable and not simply arbitrary, and second it includes two categories that can be highlighted. Individuals can be disallowed entry into the United States for criminal related reasons and national security related reasons.

5. People Crossing the Border via the Internet

Since a person does not physically travel through the Internet, it must be demonstrated that a person can function in cyberspace in a way that is at least analogous to travel through physical space. On the Internet an individual can connect from a computer at their location and then establish an interactive session to a computer in another physical location. This is normal with many Internet services, but with some, the individual can have user level or complete administrative level control over the remote computer system. This is also one difference that separates the Internet from normal telephone communication. This control can be authorized, which poses no threat, or it can be unauthorized, often gained using hacker tools. This unauthorized activity crosses the threshold into criminal activity and can even move into the realm of posing a threat to national security. If the hacker is in one country and he uses tools to gain unauthorized access into a computer in another country, he has effectively crossed the border and he now has almost total control of a computer located in another country with almost all of the same power as if he were physically sitting at the keyboard. With this control he can steal or corrupt information, or even destroy all of the information on a computer. If the computer system is used to control a physical process, for example, power distribution, the hacker can also incur damages in the physical world. His ability to cross the border is limited on the Internet, but it is still potentially significant. The normal border inspections, which could deny him legal physical entry, to prevent criminal activity or

[32] Immigration and Nationality Act section 212, Title 8 U.S.C. section 1182.

[33] Overview of U.S. Immigration Law. http://www.twmlaw.com/resources/generalcont.htm. May 17, 2003.

threats to national security, are not applied to keep him out on the Internet. He could be a known hacker, indicted for criminal activity or national security violations, which would prevent his legal entry into the United States. He could even be coming from a known Internet address. But there is currently no way to track or stop him from crossing the border on the Internet and stealing computer information or engaging in other malicious activity inside computers located on US soil. In a limited but real sense people are routinely crossing the border into the US and committing crimes on US soil with no means to inspect or stop them. The idea of people crossing the border on the Internet should not be over extended, but it is appropriate to consider it a border crossing within the narrow confines of the environment where it occurs, the Internet. If a known hacker outside the United States had exclusive use of the same Internet address for a hacking spree into the US, it would seem prudent to allow increased inspection of Internet traffic from that IP address. It is reasonable that a sovereign state should have an interest and potentially be able to block hostile criminal or national security related activity from crossing the border, if there is a feasible way to achieve this without undue constraints to non-suspicious traffic. Again the technical details are important and are described later.

It is useful to make an interim summary of the analysis so far before extending the argument further. Up to this point the case has been laid out that national sovereignty gives a state the right to strongly protect national borders, and this includes expansive authority for inspection at the borders. The US has delegated a portion of this authority to US Customs and BCIS, granting them the responsibility to inspect goods and people crossing the border. The US legal system uses common law tradition, which can derive legal principles from one case and apply them to another situation. Thus the idea of potentially extending border inspections to cyberspace can be considered reasonable. Further, such inspections might apply to information goods crossing the border as well as a limited notion of people crossing the border. However, one of the strongest counter arguments to all of this is that the Internet is still primarily a communications medium and thus a special case, which should be exempt from inspection. The case for Internet inspection will need to be extended to adequately address this counter argument.

6. Other Communications Media

There are two communications media, which between them parallel almost all of the important elements of the Internet. These are the telephone and regular mail. Mail will be examined first. Mail is a communications medium that has many similarities to the Internet. Both can be used for everything from very private communication to very expensive commerce. Mail is sent by identifiable packages, typically with outer wrappers that may not disclose explicitly the contents, and which have specific and unique addresses identifying to whom and from whom the package is sent. The Internet uses information packets also, with information headers that do not explicitly disclose the contents, and these also have specific and unique to and from Internet addresses. Mail also travels across borders in vast quantities that would make detailed inspection of more than a small percentage impractical and undesirable. The same might be assumed about Internet packets. A characteristic of mail that may be less generally well understood is the fact that mail crossing the borders is subject to increased inspection authority as well. Within US borders the US Postal Service Inspectors maintain the authority to inspect specific packages, but it would require a legal due process procedure based typically upon probable cause to be able to examine the contents of a package. However current US law extends the authority of US Customs to inspect mail along with other goods crossing the border into the country.[34] There have even been recent changes to US Customs law that grant this authority, and Customs now has the authority to inspect outbound mail that appears to be sent for commercial purposes if there is a reasonable suspicion that it may contain contraband. This authority to inspect inbound mail crossing the border without a warrant based on a "reasonable suspicion" is part of current laws and regulations and has been held to be constitutional in *Ramsey v. U.S.*[35] We can derive from this the idea that if communication on the Internet is like mail, then it would be logical that inbound traffic could be inspected.

What then about the comparison of the nature of the Internet with the telephone? The telephone and the Internet also have many parallels between them. Both are electronic communications media. Internet connections often send digital signals or

[34] Customs Inspection of mailed parcels. http://www.customs.ustreas.gov. May 17, 2003.

[35] Ramsey v. U.S., 431 U.S. 606 (1977).

modulated analog signals of digital information over telephone lines, and the Internet is used to send voice signals just like telephone conversations, so there is in fact a significant real overlap. Telephone conversations strongly resemble the interactive sessions established on the Internet. The similarities and overlaps are so strong that most laws and legal opinions addressing interception of Internet traffic closely parallel telephone wiretap laws. In this case, wiretap laws have many characteristics more like surveillance of an individual than border inspection, but it is easy to consider the telephone and Internet similar media.

If the telephone is the best parallel in many ways then certain details must be considered describing how the two media are the same, and how they are different. Telephone conversations are not inspected at the border. Should we thus conclude there should not be Internet inspections? This is too great a logical leap also. It has already been established that the Internet is a place where it is common for goods both legitimate and contraband to directly transit across borders, and goods themselves do not directly cross the border via the telephone. Also, we should consider the possible reasons telephone conversations are not inspected at the borders. National sovereignty is asserted at the borders for two primary reasons, to collect tariffs and duties, and for security. With regard to tariffs, there is no need to monitor the content of telephone conversations to gather the fees set by the government, as there are other telephone billing structures which allow a country to collect taxes on international telephone calls. So we can see that telephone conversations do not need to be inspected at the border for tariffs and duties. But we also see that the telephone is not so special that it is exempt from all assertion of national sovereignty, because taxes are collected.

With regard to the issue of national sovereignty being expressed to protect national security, the border for technical reasons is not a convenient place to monitor content. If the government has sufficient probable cause for monitoring the content of a telephone conversation crossing the border to intercept a conversation, for example, between an international drug trafficker and his US operative, then this is most conveniently done through the wiretap procedures already established, which would monitor the telephone at a local telephone company not at the border. It can be surmised that no procedure for inspecting telephone conversations has been established at the

border *per se* for convenience rather than necessarily some special property of the medium. Another difference between the Internet and the telephone is that while the telephone may be used to commit a crime, like telemarketing fraud, this type of crime involves someone on the receiving end of the conversation that is aware of the activity and in the position to make a choice even if they are unaware of the criminal intent of the perpetrator of the crime. However on the Internet there is now a large and growing threat of hostile probes and subsequent criminal hacking activity being perpetrated daily and the vast majority of such crime occurs with little or no awareness of the crime until it is complete. There are some fundamental differences between the majority of telephone crimes and Internet crimes. The nature of the threat reasonably should be taken into consideration.

When the threat is taken into consideration even the content of telephone communications can be a target of Communications Intelligence (COMINT). In the wake of September 11th there has been an increased public awareness of the ability of the National Security Agency (NSA) to target and intercept potential terrorist cellular phone conversations. Senator Orrin Hatch was just one highly visible example of a government official acknowledging such a capability, even though he was then criticized for the public nature of his acknowledgement. No matter what the source, this capability has more or less officially been acknowledged for a number of years. George Washington University maintains an archive of declassified and sanitized NSA documents obtained through the Freedom of Information Act. These documents provide an important understanding of some of the ways that COMINT, which would include telephone communication, is monitored and some of the important restrictions against monitoring "US Persons"[36] in the course of NSA COMINT collections.[37] This type of collection demonstrates the fact that telephone communications outside the US borders is in fact not a medium that is so special that it cannot be monitored. These collections are not

[36] A US Person is described in US law and government regulations, and is intended to set apart a broader scope of individual legal entities for legal protection than just US citizens. A U.S. Person is defined as one of the following: a US citizen; an alien who is known to be a permanent legal resident of the US; an unincorporated association/organization substantially composed of US citizens and/or resident aliens; a US corporation/business, unless controlled by a foreign government.

[37] National Security Archive Electronic Briefing Book. http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/. May 21, 2003.

conducted under the authority of US Customs, which operates under Title 19 of the US Code, but they are legally conducted under national security and intelligence authorities and restrictions, which are granted under Title 50 USC. The purpose of monitoring is to protect the US from national security threats primarily outside our borders. NSA is strongly restricted against collecting intelligence on US Persons unless they are terrorists or agents of a foreign power. This difference in legal authority between Title 19 and Title 50 is not trivial but it does not obviate the point that telephone conversations are not so special that a sovereign nation like the United States cannot gather some information under specific circumstances to include national security. Even if Internet border inspections were implemented through other means and under different agency authorities, such inspection could be used to counter national security and criminal threats. It is reasonable for a sovereign nation to consider the content of certain national security related electronic communications outside its borders.

One other important difference between the telephone system and the Internet, which has been indicated so far but not explicitly stated, is the Internet is a much more complex environment than the telephone system. A clear and explicit recognition of this complexity leads to an understanding that any one previous communications medium does not fully establish all of the appropriate precedents for handling the Internet. The Internet is not a monolith, and it is overly simplistic to treat it only like the telephone. A more sophisticated approach is necessary in formulating laws and structures to properly handle the complex issues of the Internet. There are some aspects of the Internet which are virtually identical to telephone communication like Voice Over Internet Protocol (VOIP). There are other ways that it is very much like mail, with email being a clear example, or IP packets at a different level of detail. Also, it is in some ways like physical goods crossing borders, and in other ways it is like people crossing the border. In fact there is a specific internationally recognized process for identifying specific Internet communication protocols and establishing technical standards for handling them, to include VOIP, email, and a host of many others. "The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols. The IANA is chartered by the Internet Society (ISOC) and the Federal Network Council (FNC) to act as the clearinghouse to assign and coordinate

the use of numerous Internet protocols."[38] The Internet has potentially up to 65535 unique ports that can be used to pass IP information, and hundreds if not thousands of these ports have already been registered to use specific services. For example email typically is sent over port 25, and web traffic is sent over port 80 as a standard. The point should not be overblown here to assert that there are thousands of unique ways from a legal perspective to handle the Internet, but it does seem reasonable to assert that it is a more complex medium than any one previous communications medium like the telephone or mail, if each one is taken on their own. The complexity of the Internet is thus deserving of a more sophisticated treatment. It seems reasonable that appropriate principles and precedents from previous communications and transportation media should be applied to appropriate communications within the complex structure of the Internet.

7. Precedents from the Internet

A final consideration will be discussed in building the logical case for Internet border inspection. Previously we have considered the legal principle of national sovereignty and physical border inspections and extended this to the Internet. Then we considered the similarities and differences between the Internet and other communications media. However, there are already many significant principles and precedents in place for handling traffic on the Internet. One law that gives a more detailed description of how the Internet is handled is the Electronic Communications Privacy Act (ECPA). This law specifies, among other things, the various legal authorities and limitations regarding monitoring of traffic on the Internet. It describes authorities and limitations not only for law enforcement, but also for Internet service providers. In addition any organization that provides Internet services like email or web access within the organization has been granted the authority to monitor incoming traffic, which can include content, if the monitoring can be reasonably shown to be part of maintaining security on their network. This includes the authority to set up computers that can examine communication coming in and out of their networks at the "border" of their Internet structure, called "Firewalls". These firewalls are routinely set up as part of a multi-layer security structure designed to protect the network from hostile network

[38] IANA Internet Protocols RFC 1700. http://www.iana.org/. May 21, 2003.

attacks or other malicious activity. Other computers are sometimes set up as intrusion detection systems, and these also are authorized to automatically monitor traffic including content, for the express and narrow purpose of protecting the network. These authorities are already granted to legal entities such as organizations that provide Internet access to users inside the organization. In fact building up this type of security infrastructure is a very large part of the National Strategy to Secure Cyberspace.[39] The point here is not to confuse the issues of authority between the government's authority to monitor and the private entities authority to monitor. Instead the point is that there is already an established principle recognizing the legitimate interest in monitoring Internet traffic at the "border" of a legal entity. If security is a legitimate interest and held to be valid for entities within a sovereign state, then it certainly seems reasonable to assume that the sovereign itself would have a similar right if it were established within an appropriately narrow framework.

Previously we have pointed out that different government agencies operate under different legal authorities (e.g. Customs operates under Title 19 USC, and NSA operates under Title 50 USC). This may initially be considered inappropriate mixing of legal authority at the border when considering inspection in cyberspace. In fact these different authorities are complementary when considering how different agencies use them to provide protection at the border in physical space. They could be considered complimentary in cyberspace as well. The case has been built so far primarily on the logical extension of Customs type authorities from physical space into cyberspace. However if there were a technical means for monitoring traffic at the border, different agencies, each with their different authorities and restrictions, could operate to protect the legitimate interests of the United States and it citizens each within their own sphere of interest. For example, US Customs could inspect traffic for goods and contraband crossing the border under a modified Title 19 authority that specifically granted them the Internet inspection authority. Law enforcement could operate at the border against hackers crossing the border to commit crimes, under a modified Title 18 USC authority, and they would do so under the limits of needing a judicially approved warrant to conduct such criminal investigations. Intelligence agencies could operate at the border,

[39] National Strategy to Secure Cyberspace. http://www.whitehouse.gov/pcipb/. May 17, 2003.

under their Title 50 USC authorities and restrictions, to gather information about terrorists and agents of a foreign power operating in the United States. And the Department of Defense could operate at the border, under their Title 10 authorities and restrictions, to protect the United States against Information Warfare attacks during a time of war or hostilities. The technical methods of conducting such operations will be discussed in Chapter IV.

An argument has been built here that takes the current practices of physical border inspection and describes a reasonable extension into cyberspace. This has been compared to other communications media to parse out significant similarities and differences, thus establishing a reasonable consideration for Internet border inspection. Finally the current established practices and principles of Internet traffic have been considered, which might reasonably be considered to extend to the sovereign state at the borders. This builds the case that it is reasonable to consider Internet border inspections, but the case is not complete until it is understood what the sovereign state would do if it asserted such authority. The last part of this chapter will consider this issue.

B. THE USES OF INTERNET BORDER INSPECTION

The idea of Internet border inspection is one that immediately triggers a cautious response in people who have a respect for values of freedom and privacy. This is natural because without much thought the idea of expanded opportunities for government surveillance brings with it ideas of how individual Internet activities like web surfing and email could be monitored without the individual being aware of it. The idea of some faceless government bureaucrat reading innocent but private emails sent to friends or family outside the borders is offensive. While people may be visiting web sites of personal interest that may be entirely legitimate and wholesome, few people would want the government to have a record of individual web activity. These are just a couple of a broader host of entirely legitimate concerns. The case for Internet border inspection must consider concerns like these. A structure that does not properly address these concerns should be considered illegitimate and should not be implemented. However, these issues are not completely new, and there are principles and structures that have already been

established as legitimate, which can guide the development of the conceptual structure of establishing Internet border inspection. Certain details of a more technical nature are addressed in a later chapter but the general purposes are addressed in this section.

It has been previously discussed that border inspection is currently conducted for several reasons, of which three primary reasons will be addressed here. Borders inspections are used to protect national security, to prevent criminal activity, and to collect appropriate taxes on goods. The last one is a good example of how the logic may be sufficient, but if there is not a practical means to implement Internet border inspection for tax collection, then inspection for this specific purpose should not be implemented. There is more than one problem with Internet border inspection for taxes. One is that the government has up to now been interested in fostering commerce on the Internet in part by specifically allowing most goods not to be taxed. Additionally the way this proposal envisions inspections is specifically narrow and may not easily address all the appropriate Customs duties concerns. However there may be a way to separate certain traffic that is primarily goods based upon the registered and standard Internet service that carries it. For example peer-to-peer software is typically used to share information goods, such as music and software, across the Internet. The standard port for sharing these files is IP port 1214. Customs could potentially monitor this port from certain suspicious IP addresses to exercise their inspection authority. They may not be able to collect Customs tariffs and duties but they might be able to identify contraband or other illegal goods crossing the border in significant enough quantities to take other legal actions against the criminals trafficking in such goods.

1. Inspection of Incoming Goods

The other two issues related to border inspection are protection of national security and prevention of crime. Proper handling of these two issues is among the most important duties of a sovereign state. As was discussed previously, US Customs already deals with the issue of inspecting the enormous volume of traffic in goods and mail crossing the border. They choose to allow the vast majority of it to pass without any detailed physical inspection of the goods. The criteria they use to determine the small proportion of goods they will inspect in greater detail is based on "reasonable suspicion," sometimes specifically bolstered by intelligence information. Neither the shipper nor

Customs may know before a shipment of goods is processed through Customs if it will be inspected in detail. If the accompanying documents or other required Customs forms have some information that is reasonably suspicious, then Customs officials can inspect the shipment. Also if US Customs receives specific criminal intelligence information that indicates a certain shipment may contain contraband like illegal drugs, then they are very likely to pick that shipment for inspection out of the vast number of shipments crossing the border daily. With this example in mind, it seems reasonable to propose an Internet border inspection structure that would let the vast majority of Internet traffic pass without any inspection and no record kept of its crossing the border. However, if there was some specific national security or criminal intelligence information that indicated that a certain Internet IP address outside the US borders was trafficking in information of a contraband nature or engaging in criminal activity within the US, then inspection seems very reasonable. Because IP addresses are a cornerstone feature of the Internet architecture, IP addresses could be used as part of a method of implementing inspections. The specifics of implementation are discussed in the next chapter, but at this point it may suffice to state that there are reasonable grounds to assume that IP-based inspections may be technically feasible. It must be emphasized that normal traffic would not be inspected at all and no record would be kept of normal traffic crossing the border.

2. Inspection to Prevent Terrorism

Examples of how this might work may be useful to describe. In the overview, the example was given of imagining that there is a known IP address outside the US used by controlling elements of Osama bin-Ladin's Al-Q'aida terrorist organization. Other individual criminal or national security threats could be easily imagined with known IP addresses identified through intelligence. These could include a variety of threats from drug traffickers, to hackers on a hacking spree, to spies using computers to gain access to sensitive information. Once the suspicious IP address is identified, it could be provided to those charged with operating the Internet border inspection, who in turn could load it into the appropriate Internet routers at the border. The routers would then divert that traffic into a system for more detailed inspection. Internet border inspection would thus be specific and based only on validated intelligence information passed through an

appropriate due process. Only content from the suspicious IP addresses would be examined. All other traffic would pass by unexamined and uninspected. Such inspections would be reasonable, and would appropriately respect the freedom and privacy issues that immediately concern many people.

3. Inspecting to Keep Out Contraband

In addition to the inspection purpose just described, Internet border inspection could be used to keep out contraband. Again we can imagine an IP address that might be a web site containing child pornography. Since there is a legitimate government interest in preventing such contraband from entering the country, the appropriate border routers could be set up to disallow all traffic coming from that IP address. Alternatively, the traffic could be shunted to another server for a more detailed inspection. In a similar fashion, an IP address that was identified as being the source of known hostile hacker activity could likewise be blocked or monitored and appropriate information passed to law enforcement officials. Doing so might aid in investigating and prosecuting the individual responsible for the hacking activity.

4. Inspection to Prevent Crime

There is daily hostile hacker-related probing and intrusion activity from outside the US coming across the borders. A normal part of Internet Service Provider customer agreements in the United States includes the acknowledgement by the customer that hostile activity, such as probes and intrusions, is against the acceptable use policy and is grounds for terminating the customer's account. We can see then a logic that indicates that there are reasonable grounds for disallowing even probes that do not meet the level of criminal activity. We can imagine then that if a foreign IP address were being routinely used for probing and intrusion attempts, even if it did not reach the level of criminal activity, may still be considered among the traffic to be monitored or blocked. If this were implemented, then specific IP addresses might be blocked initially for some reasonable short period like 15 days. If the IP address were identified again as continuing the activity a longer period might be considered like 30 days or longer. If the owner of the IP address became interested in reversing the block, a procedure could be established to request the block to be removed. Reasonable grounds need to be established for

blocking and proper oversight should be maintained, but hostile probes and other hacking activity should be among the activities considered as potentially legitimate for blocking.

5. Information Blocks and Embargoes

Studies in international relations describe a sovereign state as a primary actor in the international arena. States are considered to be able to legitimately use certain instruments of national power to protect their national interest, as long as that does not unduly infringe upon the rights of other states. National power is parsed in different ways but one way describes the instruments of national power as being military, economic, diplomatic, and information.[40] Typically information power has been seen as including the US using intelligence information to support allies and interests even when it may not want to use more direct means to influence the outcome of an international situation. Economic power includes among other things the ability to impose economic sanctions on another county to achieve a desired outcome. If there were a method already in place to allow IP addresses to be blocked at the border, then there would be a new method of using information as an instrument of national power. Another international actor that is not cooperating with the United States could be subject to an information embargo if appropriate Presidential and Congressional action were taken to authorize it. For example, criminal investigators in the United States have in the past investigated computer hacker activity and traced the activity back to a likely subject in another country. If the foreign country does not have laws against the crime, then the US government is usually stymied in taking further action to investigate or prosecute the individual. The US has worked in international forums like the Council of Europe and bilaterally to encourage other countries to update their laws. However, some countries may not assign Internet-based crime the same priority as the US. These countries may do so in part because the hackers may avoid targeting their own country and prefer instead to focus their hacking efforts on the target rich environment in the US. It would typically be seen as an inappropriate response to use economic or military instruments of power to encourage unresponsive foreign countries to give a higher priority to updating their laws against hacker activity. It might be much more appropriate to use exactly the same instrument of power, access to US-based information on the Internet, as the potential

[40] Joint Pub 0-2, *Unified Action Armed Forces (UNAAF)*, 24 Feb 1995

incentive to update their laws. If they do not respond then they could face an information embargo. All IP address ranges from the unresponsive country could be blocked or subject to increased inspection. Because the US is a dominant power on the Internet, this could be a substantial incentive. Unresponsive countries could easily see updating their laws and prosecuting computer crimes as much more in their national interest, if even the threat of sanctions could be applied. This is not currently a viable method of exerting national power, but a robust Internet border inspection regime could make it viable.

C. CONCLUSION

The case has been made that there is a reasonable basis for considering Internet border inspections. The purpose and use of Internet inspection was pointed out to be a critical part of a sufficient rationale for inspections. An Internet address IP-based description has been described and shown how it would work to support criminal investigations and national security. The appropriate use of this could clearly and reasonably support US national interests. Such a system of IP-based inspections would also not unduly inhibit other legitimate Internet activity crossing the border. With proper administration and oversight this could be a significant net benefit to US security and national interests. Even if all of the applications discussed were not implemented, there seems to be a reasonable case for further discussion of the topic.

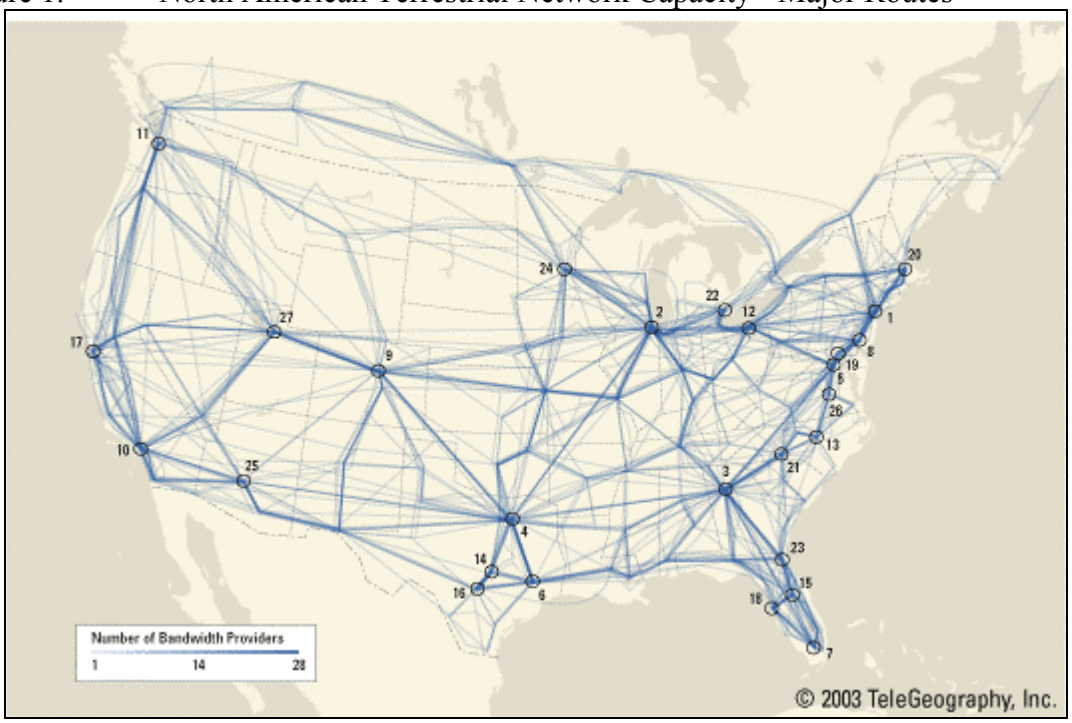
IV. TECHNICAL FEASIBILITY

Careful technical implementation of Internet border controls is key to their being both feasible and legal. This chapter will address the key technical question of feasibility, but as this thesis is not primarily a technical thesis, it will not address detailed technical issues. There are many who are unfamiliar with the backbone structure of the Internet who would be first inclined to believe that border inspections are not even possible. There are others with technical knowledge who believe that such inspections might be possible in some areas, but they can easily imagine a host of ways to get around an inspection regime. Both of these issues and others will be addressed in this chapter. Also this chapter will provide a high level technical discussion of the use of routers as a feasible method for conducting inspections based primarily on Internet IP addresses.

A. INTERNET BACKBONES AND TRANS-OCEANIC CABLES

To explore the feasibility of Internet border inspection, one of the key facts to know about the Internet is that the vast majority of non-local traffic typically travels along major Internet backbones, both within a large country like the United States and internationally (see Figure 1). These backbones function much like the interstate highway system handles automobile traffic. The average user connects to an Internet Service Provider through a dial-up, Digital Subscriber Link (DSL), or cable connection, which is like driving out of their driveway and onto local neighborhood streets. The ISPs either have their own major Internet backbone connections, or they connect to major providers that do. This is like people driving from their neighborhood streets to major city streets, and then to the major highways. To extend this street metaphor, though, you would have to imagine major highways crossing the Atlantic and Pacific Ocean to connect to the other continents. The Internet connects the major domestic backbones at geographic hubs, and then these send and receive the information across dozens of undersea cables from the border of the United States to Europe, Asia, the Caribbean, South America, and Africa.

Figure 1. North American Terrestrial Network Capacity - Major Routes

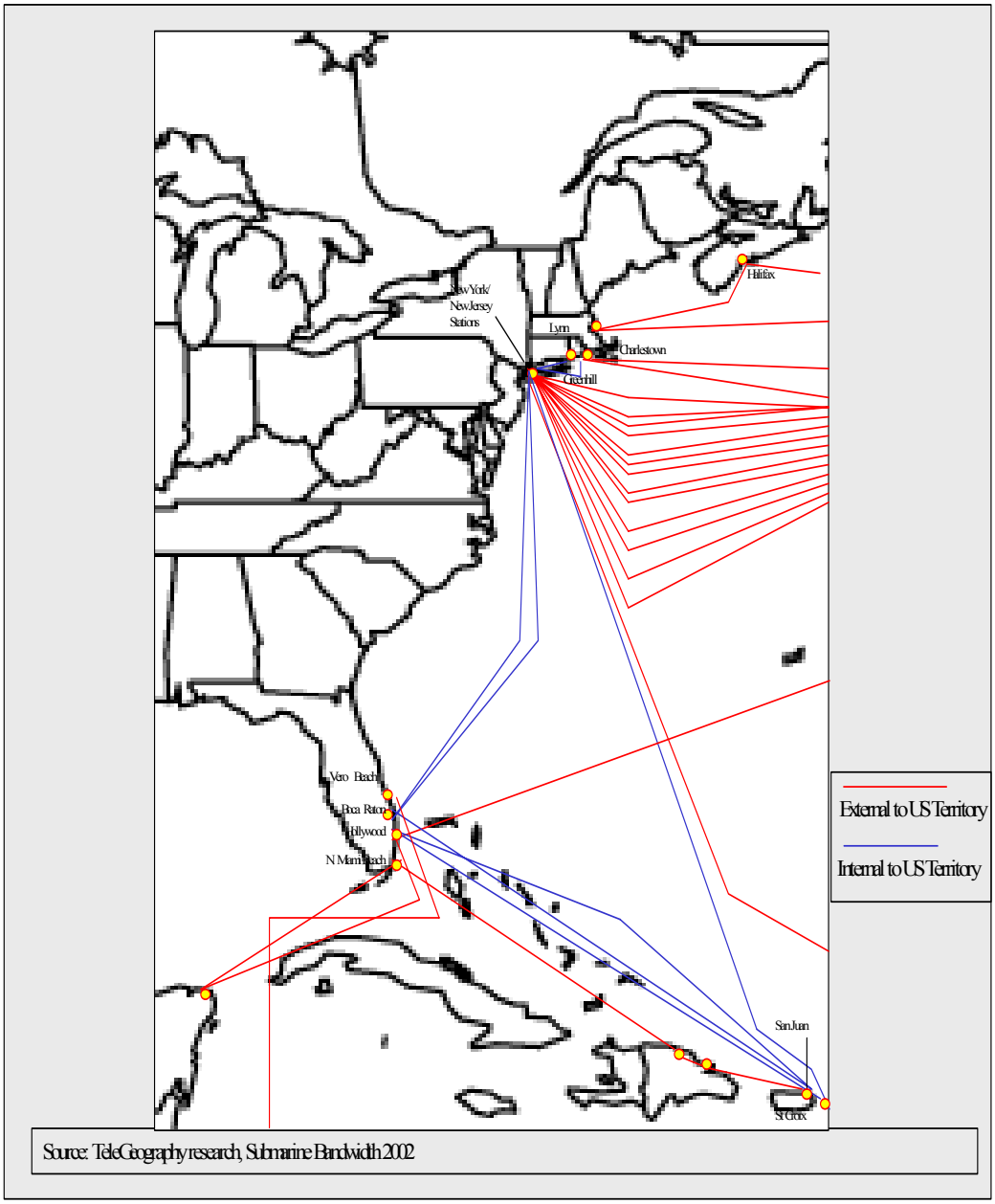


Notes: Map depicts network providers who offered private line connectivity to three or more states at 155 Mbps (or higher) as part of their standard offerings. The map is designed to illustrate intercity connectivity and does not necessarily reflect the exact physical routing of fiber. Source: From TeleGeography's *Terrestrial Bandwidth 2002* © TeleGeography, Inc. 2002 Used with Permission of Telegeography. www.telegeograpy.com

When considering the trans-oceanic cables that cross into the United States it is useful to consider separately those cables that cross into the continental US on the Atlantic coast from those that cross into the continental US on the Pacific coast. On the Atlantic coast there are approximately 28 trans-Atlantic and trans-Caribbean cables carrying both Internet and telephone traffic that come into the continental United States (see Figure 2). These cables cross into the continental United States on the Atlantic coast in 10 locations, but they are largely concentrated into 8 of these locations along the east coast of the United States. These are most concentrated at the New York / New Jersey stations, where 14 of the 28 cables connect representing significantly more than half the bandwidth and traffic entering the continental US on the Atlantic coast.[41]

41 TeleGeography, *Global Internet Geography 2003, International Internet Statistics and Commentary*. 2003, TeleGeography: Washington, DC. p. 250.

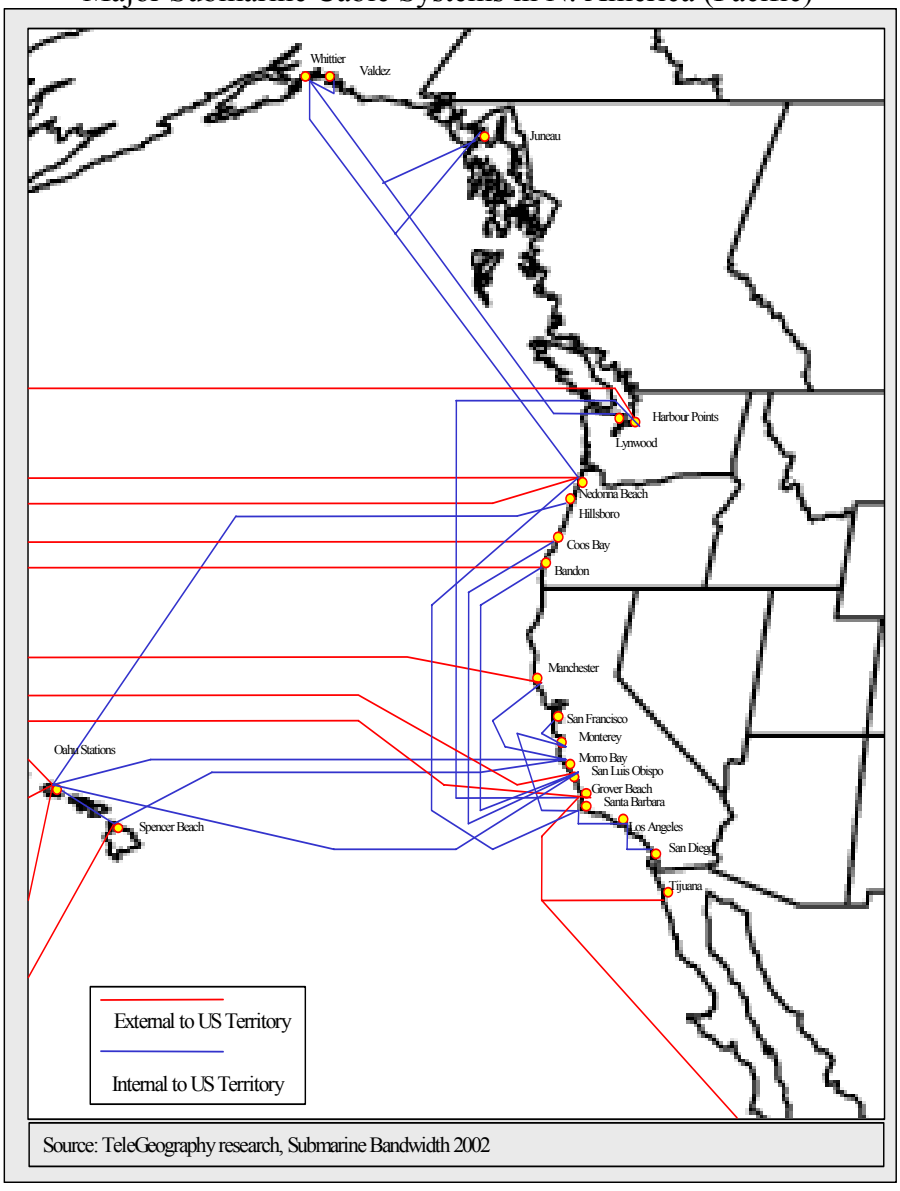
Figure 2. Major Submarine Cable Systems in N. America (Atlantic & Caribbean)



On the Pacific coast, 12 trans-Pacific cables cross into the United States and connect to 8 locations (see Figure 3). There are other Internet backbone connections that first cross the border into US territory at Hawaii and Guam. This mildly complicates matters but is really not very different than physical goods crossing the borders, which also may cross US borders first into a US territory rather than the continental US. When considering the US and its territories, in both the Pacific and Atlantic, there are less than

30 locations in the US and its territories that carry all of the Internet traffic crossing the border into the US via submarine cable. These are fairly concentrated as well with 7 of the 12 crossing the Pacific connecting in three locations in the continental US, and 20 of 28 cables arriving in three continental US locations in the Atlantic. This represents a very large concentration of Internet connectivity crossing US borders.[42]

Figure 3. Major Submarine Cable Systems in N. America (Pacific)



[42] TeleGeography, *Global Internet Geography 2003, International Internet Statistics and Commentary*. 2003, TeleGeography: Washington, DC. p. 249.

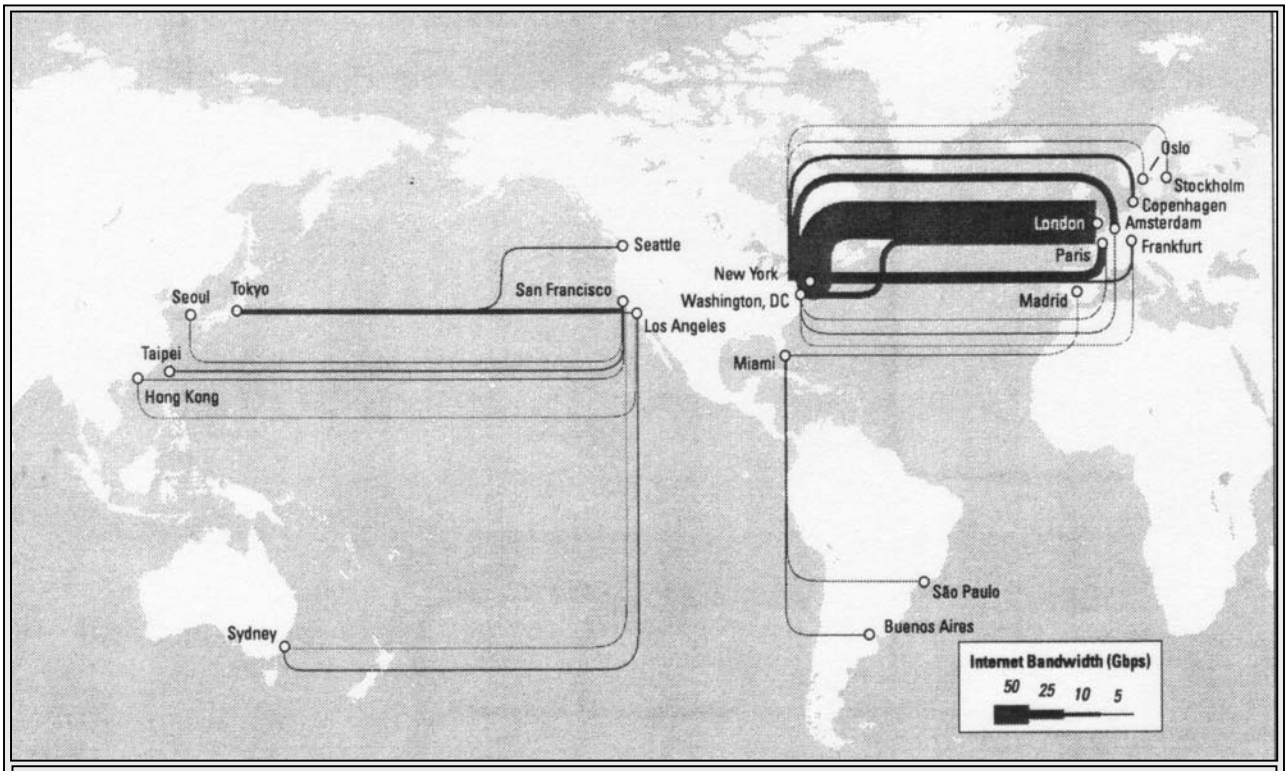
In addition to the trans-oceanic cables, significant trans-border connections enter the US from Canada and Mexico. Again there is a reasonably high concentration of the traffic via a backbone network. There are four Canadian cities that connect to three US cites and these connections represent 79% of the total Canadian international bandwidth. It is a similar situation with Internet connections to Mexico. There are primarily four backbone connections that represent the bulk of the Internet traffic connecting the US and Mexico.[43]

There are of course many other international Internet connections besides the submarine cables. These include international corporations with dedicated leased telephone lines, satellite data links, and long distance modem connections from foreign countries. These alternate links, however, represent a small fraction of the total Internet traffic crossing the borders in and out of the US (see Figure 4). Implementation of Internet border inspections cannot be considered invalid because it is not a 100% solution. This can be compared again to border inspections in the physical world. There is a small but significant percentage of the total number of people and goods crossing the border into the US who do so illegally, but this does not invalidate the current regime of inspecting people and goods crossing the US border. Internet border inspection can start with a solution that covers the overwhelming majority of Internet traffic crossing the border via submarine cables first, and then later consider solutions for inspecting other methods of transmission at a later time. The relatively small bandwidth of modem and satellite connections and relatively higher cost make both of them inefficient and expensive ways to cross the border without inspection, and they are unlikely to ever constitute large portion of Internet traffic.

To summarize, close examination of the Internet backbone structure reveals a significant concentration of cross border traffic. Thus, the bulk of Internet traffic could be inspected with a reasonable number of inspection stations.

[43] Ibid. p. 63, 25.

Figure 4. Map of Major Interregional Internet Routes to North America, 2002



Notes: Map includes interregional Internet routes with at least 1,500 Mbps of aggregate capacity. Figures represent Internet bandwidth connected across international borders to each Consolidated Metropolitan Statistical Area or equivalent. Domestic routes are omitted.
Source: TeleGeography research, *Global Internet Geography 2003* Copyright TeleGeography, Inc. 2002

B. TECHNICAL IMPLEMENTATION OF INSPECTION

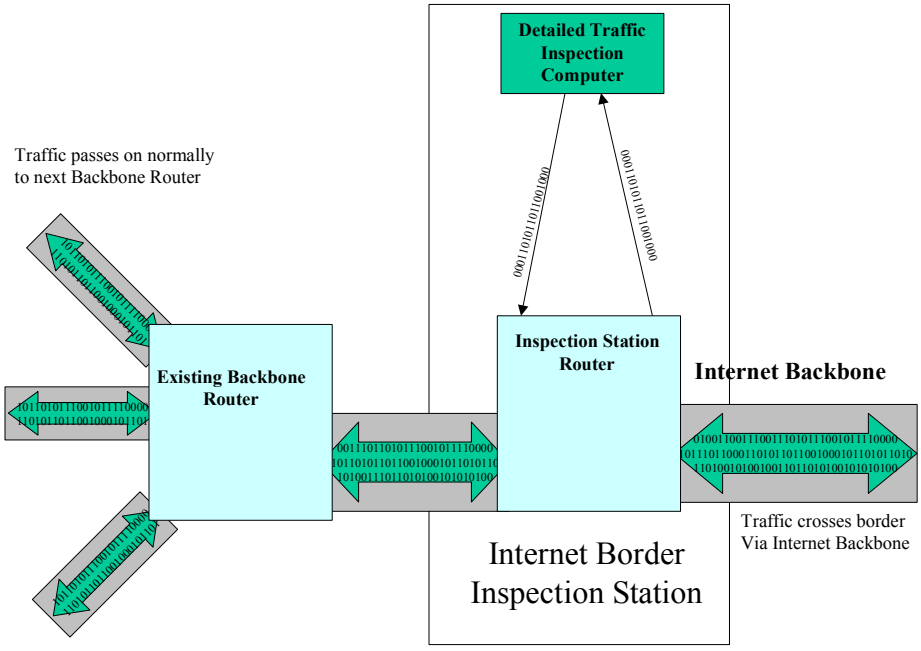
The next question is: how would inspection take place? The idea that inspection would be based primarily on Internet IP addresses was discussed previously. There are two types of Internet devices that could be used for supporting Internet border inspection: firewalls and routers. Firewalls are typically very sophisticated packages of computer hardware and software that perform a wide variety of network security functions. Many organizations use them to protect their internal networks from hostile activity on the Internet at large. Some firewalls examine all the incoming content for purposes that include protecting the network from computer intrusions and email viruses, and they can be configured to perform these functions in real time. They can also be set up to block certain traffic and allow other traffic to pass unhindered. The sophistication and complexity of these firewall products significantly enhances security, but the content analysis and other complex functions in firewall products impose a heavy performance

penalty. Also, if they are not properly configured or are not robust enough to handle high volumes of Internet traffic, they can significantly slow down traffic passing through from outside to inside the firewall. Establishing such a system on a national basis would be potentially expensive and complex both technologically and legally. A firewall-based solution would border on being unfeasible for both technical and legal reasons.

A router-based solution is another alternative, and this is the one suggested here. A router examines packet header information such as IP addresses, but not message content. A router processes a data packet like a mail sorter. It looks at destination addresses and quickly passes the packet on to the next appropriate router until the packet reaches its destination. Routers already exist all across the Internet passing traffic from place to place, and they are an integral part of the infrastructure. Traffic coming across the trans-oceanic cables or other backbone structure at some point shortly after crossing the border must pass through a router to be directed to the next step in the best path along the Internet from origin to destination. When any packet arrives at this router, it will be directed to another location based upon the relatively simple rules specifically listed in the routing table of each router. The routing table compares the packet's destination IP address to the rules and sends the packet on to the next router that the rules have identified as the best one along the path. Routers can also route information based on the source IP address if this is set up in the routing table. As long as there are not too many different rules in the routing table then the router performs this function quickly and efficiently. Internet border inspection based on IP address could be established by setting up an appropriate router at a nexus to the border and adding a rule which would reroute a packet, with a predetermined source IP address, out of the main traffic stream and instead into a second government inspection station computer. In the inspection station, the traffic could be inspected to determine if it should be allowed to pass, or if some other action should be taken based upon approved legal measures. Routers could also block traffic from a specific IP address or even a range of addresses if the appropriate rule were set up in the routing table. A key point to be made here is that the vast majority of traffic would pass through the router unimpeded and no content would be examined, nor would any record be kept of its passing. Only the traffic from legally vetted suspicious IP addresses would be shunted aside and examined. From the point of view of the router,

the process would be just another rule, and unless there were too many new rules it would not impede other traffic at all. No new technology would need to be invented because routers are already part of the foundation of the Internet structure, and routing tables are a standard method of routing traffic. Internet border inspection stations based on routers would basically be almost identical to the existing traffic routers at the border, but they would have additional rules input from time to time to allow alternate routing of specified IP addresses. A second computer in the border inspection station would receive the shunted packets, allowing content to be examined or whatever other action was determined to be legally appropriate. To be effective all inspection station routers would need to have the same list of IP addresses input into the routing tables. Thus if an IP address was determined through legal means to be subject to inspection, something like an Internet border inspection "all points bulletin" would be sent to all the various inspection stations and the rules for the routers would be updated. The "all points bulletin" notifying the inspection stations of the new suspicious IP address could be sent through administrative channels; and personnel at the inspection station who have physical access to the router could update the router rules. Then each inspection station router would shunt all traffic from that IP address to the appropriate secondary inspection station computer for more detailed inspection processing. Internet border inspection routers in conjunction with secondary inspection station computers could be effectively used to efficiently and effectively inspect traffic from predetermined IP addresses coming across the border (see Figure 5). The "all points bulletin" notifying the inspection stations of the new suspicious IP address could be sent through administrative channels; and personnel at the inspection station who have physical access to the router could update the router rules.

Figure 5. Conceptual Diagram of Traffic passing through Internet Border Inspection Station

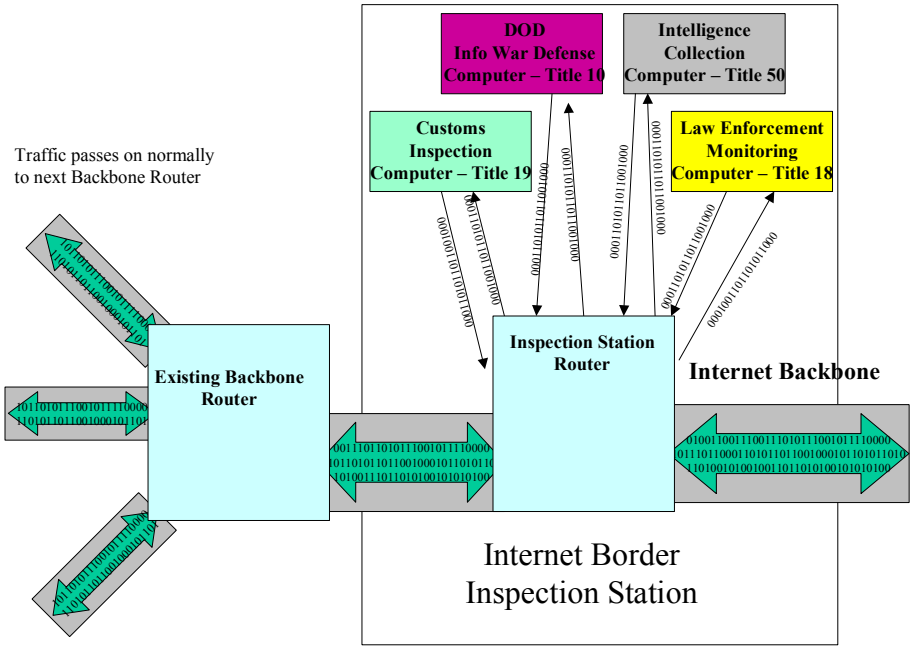


On a relatively smaller scale, certain elements of such a system are currently being used to protect at least one US government enterprise network. The US Air Force uses routers at the borders of its network to block hostile source traffic similar to the manner described. The router does not shunt aside traffic for inspections, but Air Force routers, on the "border" between the Air Force network and the rest of the Internet, routinely have new rules added and deleted to block or unblock specific IP addresses or address ranges. The source IP addresses and address ranges selected to be blocked are those that have been the source of aggressive probes and other hostile hacking activity. There is of course a huge difference in scale between the network of one government agency and the entire US Internet backbone structure, but the routers used on the backbone networks are also necessarily orders of magnitude more powerful than those on even a large enterprise. Routers are already handling the backbone traffic, and thus it is reasonable to consider that those at Internet border inspection stations could handle and route a limited list of IP addresses deemed appropriate for inspection or blocking.

One additional level of complexity can also be considered at this point. It was mentioned in the previous chapter that different government agencies operate under

different legal authorities and limitations. Since routers can route to different destinations based on rules, the same router could be used to route different traffic to different secondary computers (See figure 6). Legal due process would be used to determine if a government agency had legal authority to inspect certain traffic from specified IP addresses. If the agency had that authority the router could be updated and traffic could be sent to one the appropriate secondary processing computer. For example, if US Customs had information that child pornography was coming across the border from a specified IP address, they would update the router to allow traffic from the foreign IP address to only go to the secondary inspection station for US Customs. If Law Enforcement had information that a hacker had exclusive use of a specific foreign IP address and was using it to cross the border and engage in hacking activity in the United States, they could obtain a warrant that would grant them legal authority to modify the routing tables so that the hacker's traffic was routed to their inspection station. In practice, the inspection station router might be operated by an independent service provider, which would handle requests from the different government agencies in much the way that telecommunications providers respond to requests for subscriber information, pen registers, and content-based wiretaps, or it could be a new router owned and operated by the government. The use of the router in this fashion would allow each agency to operate at the border under their appropriate authorities and limitations. Thus each agency could assume appropriate responsibilities to protect the borders, and they could prevent or take counteractive measures against some portion of the hostile and criminal activity that comes into the United States from outside the border.

Figure 6. Alternate Conceptual Diagram of Traffic Passing Through Internet Border Inspection Station (Using Separate Legal Authority)



C. CONCLUSION

Two primary technical issues have been dealt with here. It can be seen that there is a significant concentration of Internet traffic from foreign countries, including traffic on trans-oceanic cables, into a reasonable number of routers that could serve as Internet border inspection stations. Also, the primary inspection process has been described as router based with a second computer that would only examine traffic identified for secondary inspection. Because routers already can perform the functions of routing based on IP header information such as IP addresses it is reasonable to suggest that routers on backbones with relatively minor modifications may feasibly work as a primary component of Internet border inspection.

THIS PAGE INTENTIONALLY LEFT BLANK

V. LEGAL FEASIBILITY

Although many of the legal aspects of Internet border inspections have been mentioned already, there are a few issues deserving a more detailed treatment. This chapter will address constitutional feasibility and potential constitutional challenges. The issue of how Internet border inspection would fit within the framework of existing international law will also be addressed. Finally, even if the concept is not in conflict with either the Constitution or international law, it would still need explicit authorization through new legislation. While some of these ideas were mentioned in previous chapters this chapter will provide more detail and discuss the issues in direct relationship to legal feasibility.

A. CONSTITUTIONAL FEASIBILITY

Previously, the concept was discussed that Internet border inspection is a logical extension of the legal principles, such as national sovereignty, that allow physical border inspections. National sovereignty is a principle that is not explicitly mentioned in the United States Constitution. However the idea was definitely current at the time, and the Declaration of Independence alludes to this when it refers to the establishment of the United States as "…Free and Independent States, they have full Power to levy War, conclude Peace, contract Alliances, establish Commerce, and to do all other Acts and Things which Independent States may of right do." The Constitution describes these various powers and among all of these grants specifically to Congress the power "To regulate Commerce with Foreign Nations…". This power is particularly relevant to Government regulation of the borders. This power has been held by various Supreme Court decisions to be very broadly applied, especially in cases governing the relationship of the Federal Government with regard to the individual states within the United States. One of the primary limitations on the authority to regulate commerce has arisen from individual rights of people within the borders of the United States.

Constitutionally vetted US law has already allowed appropriate agencies, which have jurisdiction at the border, broad authority to inspect based on the "commerce clause" and the various clauses that describe both the Legislative and Executive branch's authority to protect the country from foreign threats. It is considered legally significant that the "commerce clause" was part of the original text of the Constitution, and the Fourth Amendment was added later, with no specific mention of limiting Congressional authority "to regulate commerce". This is held to indicate that the framers of the Constitution intended the Federal government to have some additional authority at the border, including expanded authority to search. This expanded authority has been codified into law, and the US Customs and Border Protection web page describes the statutes delegating this authority.

> The Congress of the United States has given the U.S. Customs Service broad authority to conduct searches of persons and their baggage, cargo, and means of transportation entering the United States. This authority is contained in Title 19 of the United States Code, Sections 482, 1467, 1496, 1581, and 1582.
>
> The courts have also held that this search, seizure, and arrest authority is not dependent upon either probable cause or a search warrant as is required by police officers. One reason for this broad authority is the vulnerability of our borders to the illegal entry of a vast amount of dangerous and prohibited items.
>
> We endeavor to use this authority wisely and with respect for human dignity. It is, however, the responsibility of a trained, professional Customs officer to determine the actual parameters of an examination. The officer is not permitted to release a traveler for entry into the U.S. until he or she is satisfied that no Customs or related Federal or State laws have been violated. [44]

Similarly the Bureau of Citizenship and Immigration Services describe their authority.

> An inspector is responsible for determining the nationality and identity of each applicant for admission and for preventing the entry of ineligible aliens, including criminals, terrorists, and drug traffickers, among others. U.S. citizens are automatically admitted upon verification of citizenship; aliens are questioned and their documents are examined to determine admissibility based on the requirements of the U.S. immigration law.

[44] US Customs Inspections - Right to Search. http://www.customs.ustreas.gov/. May 10, 2003.

> Under the authority granted by the Immigration and Nationality Act (INA), as amended, an Immigration Inspector may question, under oath, any person coming into the United States to determine his or her admissibility. In addition, an inspector has authority to search without warrant the person and effects of any person seeking admission, when there is reason to believe that grounds of exclusion exist which would be disclosed by such search.[45]

Case law has upheld these authorities, indicating that the Government's right to regulate commerce and protect the nation, outweigh the individual's rights to be free from inspection at the narrow nexus of the border. If the constitutional protections against unreasonable search and seizure, the right to due process, and other individual rights are not considered to be abrogated in physical border inspections, then it seems reasonable that appropriately narrow Internet border inspections should also survive a constitutional test. However, this has not been tested in any court.

B. POTENTIAL CONSTITUTIONAL CHALLENGES

There are some ways that Internet border inspection could cross the threshold into unconstitutionality. The two areas that must be carefully considered in design and implementation are IP address blocking and content examinations. First we will consider the blocking of IP addresses. As was previously described, it seems reasonable that the government has a legitimate interest in potentially blocking contraband like child pornography from crossing the border. However, blocks must be applied narrowly so that computers with IP addresses hosting political, religious, or other types of recognized protected speech are not also blocked. If the same foreign computer hosted both contraband and protected material, then instead of just blocking the foreign IP address, all traffic from the suspicious IP address might be sent to secondary inspection where it would be examined before being allowed to pass. Examination could include an examination by a Customs official, or it could be aided by automated analysis that could compare incoming files against a database of known contraband files. Law Enforcement agencies already have such databases of child pornography images and an automated means for conducting such comparisons. If any contraband were found during

[45] Immigration Inspection Program authority. http://www.immigration.gov/. May 10, 2003.

inspection, requests for contraband material could be passed to law enforcement, following a cyberspace parallel of the "plain view" legal doctrine, which allows material found in the course of a legal search to be used in other law enforcement actions. Any legitimate material that was found in secondary inspection would be allowed to pass with an effort to minimize interruption of traffic. This may result in delays that would interrupt interactive sessions like chat, or even web access, but only to and from the suspicious IP address. All traffic from non-suspicious IP addresses would of course go by without any interruption at all. The fact that there would be some interruption from suspicious IP addresses would create an incentive for operators of foreign host computers to not provide contraband material.

Other IP addresses that the government has a legitimate interest in blocking are host computers that are the source of hostile hacking activity. Since almost any computer is potentially subject to compromise, it could serve as a pass through point for hackers. Appropriate international legal coordination and investigation would be among the first legal responses before blocking, but especially for countries that do not provide adequate legal cooperation, blocking would be an appropriate recourse. Some legitimate material might be made unavailable until hostile activity ceased to originate from that host, but the primary intent would clearly be to stop hostile activity and not to block access to legitimate material. Thus there would be an incentive for operators of foreign sites to have adequate security policies and measures so their materials can enter the US. It is important to recognize that blocking intended to deny access to legitimate protected material, rather than blocking to prevent entry of contraband or malicious activity, could cross a constitutionally protected threshold, but reasonable and narrow blocks should pass constitutional muster.

The second area that could make Internet border inspection constitutionally challengeable is in the examination of content. This issue has largely been addressed in the description of the primarily IP-based inspection regime. If Internet inspection were primarily based on an examination of all content, or content in which there was no reasonable grounds for suspicion, then it would possibly be considered too intrusive into individual privacy. By examining content only from suspicious IP addresses, most legitimate traffic goes by unhindered and unexamined. This method seems to strike a

reasonable balance between allowing some inspection for legitimate government purposes and protecting legitimate rights to privacy. Legitimate and narrow blocking and content examination are reasonable and should be constitutional.

C. INTERNATIONAL LAW

Even if Internet border inspection would survive a constitutional test there are other legal realms where it could be blocked. The most important area that should be considered is international law or treaties. Treaties that are ratified become the law of the United States and may hold the US Government to standards that may not be as amendable as domestic law. The most prominent agreement that the United States has participated in negotiating with respect to the Internet is the Council of Europe *Convention on Cybercrime.* This treaty does not specifically mention the idea of Internet border inspection, and the idea was likely not considered at all during negotiation. However, a section of the treaty requires signatory states "to empower its competent authorities to: collect or record through application of technical means on the territory of that Party…"[46] This provision of the convention was not likely originally drafted with the intent of describing border inspections, but the language gives one example from the treaty showing that collection of traffic by competent authority was intended, and not prohibited. There is some language in the treaty that describes the importance of privacy concerns. However a reasonable analysis of the overall language of the treaty would indicate that as long as reasonable measures by competent authorities are taken, to ensure due process and a normal respect for individual rights, there should be no conflict between the treaty and the implementation of Internet border inspection. It is important to also note that even though the United States participated in negotiations leading to the writing the Convention, the US Government has not formally signed the treaty nor ratified it at this time.

[46] Council of Europe Convention on Cybercrime. http://conventions.coe.int. May 10, 2003.

D. NEW LEGISLATION

An additional area to consider regarding legal feasibility is the need for appropriate new authorizing and funding legislation. Internet border inspections could not be implemented without legislation specifically granting such inspections. Congress would have to identify an appropriate agency to be responsible for conducting the inspections, and then would have to explicitly grant inspection authority to that agency. Since setting up and maintaining Internet border inspection stations would also require computing resources and personnel, specific budget authorizations would also have to be passed. The process of actually passing the authorizing and funding legislation would be necessary before any Internet inspection could take place, and of course passing such legislation is by no means a trivial task. The task of passing such laws, however, is primarily a political question and not a question of legal feasibility. The issues of political feasibility will be addressed in the next chapter.

E. CONCLUSION

We can conclude from the preceding analysis that appropriately narrow Internet border inspection can reasonably be considered a part of legitimate government interests to regulate commerce with foreign nations and to protect the United States from criminal and national security threats. Also, such inspections are not in conflict with current treaties dealing with the Internet. If inspections were explicitly authorized in new legislation they are likely to be legally feasible.

VI. POLITICAL FEASIBILITY ISSUES

The idea of Internet border inspection is not simply addressed as a narrow technical or legal question. The Internet is multifaceted, and a host of entities have specific interests in both how the Internet changes and stays the same. The amount of actual and potential commerce has brought the Internet to the attention of corporations and businesses large and small, but significant commerce always brings with it the interest of governments as well. The Internet is also a huge edifice of knowledge, perhaps one of the largest collections of human thought and energy in history. This fact combined with the reality that the Internet is also a major communications medium, together bring in the interest of millions of individuals and organizations. The communications and knowledge aspects also attract the interest of both business and government. Any time there is such a diversity of interests, political issues emerge which must be addressed. This chapter will discuss some of these issues as they relate to Internet border inspections.

Discussion of political issues related to this topic cannot be addressed in the same way as technical or legal questions. Technical questions generally can be answered in a fairly definitive fashion as either currently possible or more or less potentially feasible. Legal questions have a significantly larger amount of judgment in them, but still there are going to be some things that are clearly on one side of legality or the other.

Political issues, though, have an essentially different character. Implementation of an idea may be practically impossible in one political context, and then a single event may fundamentally shift the political situation, opening a window of political opportunity for a relatively brief time. If political leaders do not take that opportunity to make a significant change, then the window of opportunity may not open again for decades, if ever. Other political ideas develop as more of a product of larger historical and social forces that make realization almost inevitable. Political issues can also be influenced by almost completely unrelated political and social events. With this type of complexity one cannot speak of political feasibility with the same precision as technical and legal feasibility. This chapter will thus not necessarily prescribe solutions to all of the political

issues, but it will try at least to identify some of the key issues affecting successful implementation.

There are at least five issues that would have to be addressed to sufficiently satisfy appropriate interest groups concerned about the implementation of Internet border inspection. These are: concerns about freedom of speech and privacy, need for proper legal oversight, concerns of international actors, comparisons with other nations that have implemented restrictions on the Internet, and concerns about cost and necessity.

A. FREEDOM OF SPEECH AND PRIVACY

Freedom of speech and privacy issues were discussed briefly in the chapter on legal feasibility. However, there is much more to protecting these rights than just a theoretical test of constitutionality. Just because something is not prohibited in the Constitution does not necessarily mean that it should be implemented. Government may have the authority under the Constitution to take a number of actions that Americans would prefer the government not actually put into practice. Issues related to privacy can easily fall into this category. Privacy groups watch for changes in law and society that impact privacy. They pay attention to changes related to Government monitoring on the Internet, and they would likely be interested in discussions about Internet border inspection. It is important to have people that pay attention to such issues and advocate the protection of privacy. Such concerns should be taken seriously, but also must be weighed against the reasonable interests and responsibilities of the US Government to protect the people, commerce, intellectual property, information, and computers within the borders of the United States on behalf of the people. There are significant interests at stake, which need to be properly balanced. The IP address based approach of inspecting at the border seeks to start the discussion near that balancing point.

There will be some who may never be convinced of a need for Internet inspection at the border. Some privacy advocates may feel that they have a role to oppose any additional government authority to inspect on the Internet whether it is reasonable or otherwise. It will be up to Congress and the Executive branch to ultimately consider detailed proposals and balance the protection roles of government. The Judicial branch

will ensure that proper authority is not being overstepped. And it will ultimately be up to the citizenry to see and support a proper balance of privacy and protection. There is some reasonable government role in protection of the borders on the Internet, and even privacy advocates can be part of a reasonable solution. This issue can hopefully be dealt with through reasonable dialog rather than polarizing arguments. One of the important ways advocates for increased protection at the border can approach the issue is by clearly articulating the reasonable and legitimate interests of the government and the people in protecting the border, and by emphasizing the narrow nature of the inspections. Reasonable people are likely to find the argument for some narrow protection at the borders on the Internet to be legitimate.

Freedom of speech advocates are also likely to be concerned about the ability to block legitimate Internet traffic. It is good and appropriate that there are people who pay attention to such issues. It is precisely the handling of this issue and ensuring that protected speech is handled properly that will separate this implementation from the methods taken by authoritarian regimes. This issue can be addressed by taking due consideration of the issue and again finding the proper balance of protecting free speech and security, and explaining this to both citizens and decision makers. Neither privacy nor free speech issues should prevent a reasonable implementation of Internet border inspection.

B. NEED FOR PROPER OVERSIGHT

Internet border inspection could be abused to gather improper information or interfere with free speech. Proper oversight is key to preventing abuse. Congress and the Executive branch should consider, along with other implementation measures, the proper methods to ensure sufficient oversight is conducted without being overly burdensome. Privacy Officers are one approach that some government agencies and even business sector organizations are using to ensure privacy protection. Congressional oversight also could be used, especially during the stages of early implementation, to ensure that the institution of Internet border inspections starts off with the right precedents, and maintained as appropriate.

Oversight can include more than just external oversight. It can include training. A properly implemented and rigorous training program would teach all employees the proper uses and limits of information gathered during the course of inspections. Rigorous initial training, plus regular refresher training, can help prevent abuses in the first place and reduce the need for other oversight bodies to take corrective action. An example of a similar training program is the intelligence community's Intelligence Oversight training. The training program includes rigorous initial training and then annual refresher training. With this program personnel routinely police themselves and co-workers to ensure no improper intelligence is collected. A similarly rigorous program would go far in helping to build confidence that Internet border inspection would be used for only legitimate and reasonable purposes.

In addition to proper oversight, appropriate consideration should be given to dealing with complaints. A foreign host computer might have been blocked due to its being the source of criminal activity crossing the border into the United States. If the operator of the host computer had taken appropriate corrective action they might be interested in having the block removed. For example a foreign web site might be blocked because is contained child pornography, or had been compromised and used by hackers as an intermediate launching platform for subsequent hacking activity. If the operators of the host computer had taken the contraband material off of the host, or taking security measures to prevent it being used by hackers a means should be considered for requesting a block to be removed. Also if someone in the United States had been denied access to a foreign host computer they also might be interested in inquiring about the block. For example a researcher might routinely go to hacker web sites to gain insights into hacker methods and intentions. A means should be considered to allow for appropriate inquiries about the nature of the block, and a means established for petitioning removal of such a block in appropriate circumstances.

C. CONCERNS OF OTHER INTERNATIONAL ACTORS

The United States has an overwhelmingly dominant position on the Internet. Other nations that have a prominent interest in the Internet already recognize this fact. In

many ways they may see the largely unrestricted nature of the Internet as a way in which they can participate without undue US influence. Even the hint of the US putting up significant border controls would represent one more way that the US could influence the Internet at large. The idea of merely being able to monitor traffic at the borders, or implement information embargos, could easily send even some allies into quick opposition. Because the United States holds such a large lead in the physical infrastructure capacity of the Internet, there is a very significant portion of the traffic passing between other countries that passes at some point through the US. If the United States blocked even a single IP address from crossing the border, a large portion of the Internet both in and outside the US would be potentially unable to reach that address. Traffic within a given region, such as Europe, may be unaffected, but a significant amount of traffic passing between points in Asia and Europe could be affected; exchanges that pass from one region to another could be similarly impacted. This would give the United States significant potential power that it does not currently possess. In a world where other powers both great and small already see the US as overwhelmingly dominant, any significant increase in its power could be seen as a threat. The United States would have to show that this power would be handled responsibly, to gain the support of allies, and that properly implemented it could deter crime and increase security for all nations that seek to conduct legitimate activity on the Internet.

D. CONCERNS ABOUT OTHER NATIONAL SYSTEMS

Some people are likely at first, to consider Internet border inspection as being too similar to the illiberal structures that authoritarian regimes have established within their borders to restrict access to the Internet. A reasonable and careful consideration of the proposed inspections will show that the proposed controls have a fundamentally different nature and purpose than the controls put in place by authoritarian regimes. Several countries have established controls for the purpose of limiting access by their people to political or religious speech. Among these countries are China, Cuba, Singapore, Vietnam, Burma, the United Arab Emirates, Saudi Arabia, and Egypt.[47] China has

[47] S. Kalathil and T.C. Boas, *Open networks, closed regimes: the impact of the Internet on authoritarian rule*. 2003, Washington, D.C.: Carnegie Endowment for International Peace. p. 9.

implemented a system that has garnered perhaps the most attention, and it has been referred to by some as the "Great Firewall of China". Internet border inspection as described in this thesis is not equivalent to the "Great Firewall of China". China arrests individuals for expressing antigovernment views online, and members of groups like the Falun Gong are sent to reeducation camps for sharing information over the Internet.[48] While the United States might use inspection to block access to child pornography, which is considered contraband by most of the developed world, China uses its system to block access to Falun Gong websites outside their borders.[49] Legitimate free speech is protected in the United States, but the same type of speech is not protected in China. There may be a few technical similarities between the systems, but the purposes are fundamentally different, and to equate them as the same misses this vital point. If this difference is properly highlighted, reasonable people will be able to understand and accept Internet border inspection, while still opposing improper use by authoritarian regimes.

E. COST AND NECESSITY

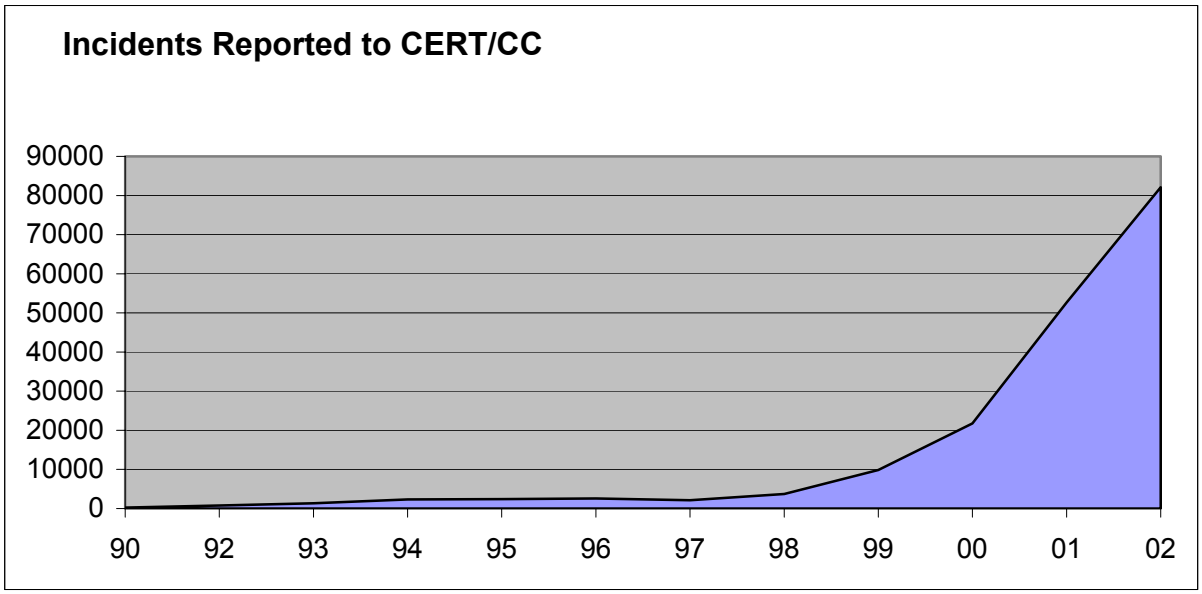
Some people will be concerned about the cost and necessity of such a project. Understanding the threat on the Internet is key to understanding why border inspection is a reasonable measure and potentially worth the costs involved. The Carnegie Mellon Computer Emergency Response Team (CERT) was originally set up to coordinate computer emergency incident information on the Internet for DARPA. According to CERT statistics, computer incidents have shown a steadily increasing trend since 1990, with a dramatic increase every year since 1998. (See Figure 7).[50]

[48] Ibid. p. 13.

[49] Ibid. p. 13.

[50] CERT Statistics. www.cert.org. June 3, 2003.

Figure 7. Computer Incidents



With such a rise in computer incidents, computer security has taken on a new importance for anyone connected to the Internet. Internet border inspection will not be a panacea for correcting all of these ills. There are a many other measures that should be taken which organizations like CERT recommend. The US Government has also developed in partnership with the private sector and academia a National Strategy to Secure Cyberspace. This strategy recommends measures that should be taken at all levels to enhance security. "Securing cyberspace is a difficult strategic challenge that requires coordinated and focused effort from our entire society, the federal government, state and local governments, the private sector, and the American people."[51] These efforts cannot be replaced by Internet inspection, but such inspection could complement them, and close a gap that is currently wide open at the border. Only the Federal government could implement such measures, and the Federal government has a reasonable and legitimate interest in providing some additional level of security at the borders on the Internet.

As an example, we can compare security on the Internet with other physical homeland security measures established to prevent crime and terrorism. Adequate homeland security must be a partnership between the private sector and government.

[51] National Strategy to Secure Cyberspace. http://www.whitehouse.gov/pcipb/. June 3, 2003.

Individuals and each organization must implement appropriate physical security measures, based on a reasonable evaluation of the threat of crime or terrorism. Likewise adequate cyber-security calls upon individuals and businesses to deploy appropriate computer security measures based on the daily threat. The US government, however, does not leave physical security up to the individual or business alone. It also takes reasonable measures at a national level including physical border searches, looking for guns or bombs, to reduce the threat coming into the country in the first place. It is reasonable to conclude that there is some appropriate role that the government could play at the national borders on the Internet as well.

It was mentioned earlier that some political issues are best addressed when events open a political window of opportunity, and there are other issues that are shaped by larger historical forces making them almost inevitable. Internet border security may fit both categories. There is currently a heightened sense of awareness of security throughout the United States in the aftermath of the terrorist attacks of September 11, 2001. This heightened security awareness may allow both government leaders and the common citizen to understand the logic of Internet border inspection more easily. Thus there is a current window of opportunity to take such action.

However there are larger historical forces at work as well. The trends toward more people connecting to the Internet every year (see Figure 8), and the dramatic increases in computer incidents, show that it may be just a matter of time before some security measures have to be taken at the border on the Internet.

Figure 8. Estimate of total population on-line as of September 2002

World Total	605.60 million
Africa	6.31 million
Asia/Pacific	187.24 million
Europe	190.91 million
Middle East	5.12 million
Canada & USA	182.67 million
Latin America	33.35 million

The Internet was developed and grew as a largely borderless small and specialized communications medium. It has developed, since its early years, into a major communications medium, and now represents a very large and growing financial interest. The need for increased security for such a large and important collection of information and financial interests has made it a legitimate interest of government. There is no reason to expect this trend to reverse, and little reason to believe it will slow down any time soon. If one of the fundamental functions of government is to provide security, then it is not unreasonable to describe increasing assertion of national sovereignty on the Internet as inevitable. If nations will increasingly assert their sovereignty, then border inspection is a reasonable area of discussion. As was pointed out earlier, authoritarian regimes have already asserted similar prerogatives on the Internet. It seems that instead of letting their abuse of the authority be an argument for not asserting reasonable measures, the United States should set a positive example of how such measures can be narrowly applied for legitimate purposes. The United States has used its dominant power for good in many ways. For example, the dominant naval power of the United States keeps the oceans of the world more secure for everyone, except pirates and criminals. Even if the United States has a dominant role on the Internet, this can also be for the benefit of everyone except criminals.

F. CONCLUSION

There are several important political considerations that must be adequately addressed if Internet border inspection is to be considered feasible. Some of the most prominent have been mentioned here; others may surface as the concept is explored further. Internet border inspection represents a significant if not dramatic increase in potential US government authority and power on the Internet. It is vital that any concrete proposal be designed to appropriately address political concerns before implementation. The proposal needs to be adequately explained to the public, and all interested parties given the opportunity to express their views. There needs to be an understanding of the threats on the Internet, and the legitimate interests of government to take measures, like border inspection, which could provide enhanced security for many even outside US borders. If the proposal is well designed and adequately understood, a majority of interested parties may conclude the approach is reasonable

THIS PAGE INTENTIONALLY LEFT BLANK

VII. CONCLUSION

This thesis has introduced and explored the concept of Internet border inspections. This final chapter will describe some findings and policy implications that have not been fully examined elsewhere in this thesis, and will also describe some recommendations for further study.

A. FINDINGS AND POLICY IMPLICATIONS

Implementing Internet border inspections would have important implications. There would be significant impacts on the Internet itself, and there would be political and diplomatic impacts inside and outside the United States. One impact would be a fundamental shift away from thinking of the Internet as borderless. Some nations have already installed controls within their own countries, but they are generally considered authoritarian and not a major presence for content on the Internet. Inspection could change that perception. However, in other ways the United States could set a strong and positive precedent on the Internet. The US may be able to bring some order out of the common chaos and lawlessness that is currently a fact of life in cyberspace. If the Internet were better policed, it could potentially enhance growth and stability on the Internet, in a fashion similar to the way that the US providing security in international waters enhances and stabilizes world trade. Hackers and virus writers can be likened to the pirates of cyberspace. In the current environment, it is taken for granted that they cannot be tracked or significantly hindered except through laborious and often dead end law enforcement actions, but new tools like Internet border protection and inspection could provide a way of isolating them and bringing order to the Internet. Software and media pirates, who also operate with very little inhibition on the Internet currently, could also find their means of distribution blocked to major markets for gaining and distributing their illegal goods.

The United States government had been successful in tracking down and almost eliminating child pornography from crossing the border when the primary means was physical print media. This success reached its apex at about the same time the Internet was becoming accessible to the general public. The Internet became the new media of

choice to engage in child pornography distribution. The borderless nature of the current Internet is exactly the environment that distributors of such contraband prefer. Internet border inspection and blocking could provide new investigative tools that could help stem the tide of child pornography that crosses the borders of the United States daily.

Once there is a means of performing reasonable inspections and protections at the border of the Internet, additional measures could be taken to make the Internet a safer environment. The idea of border inspections should not be dismissed out of hand based on the fear of potential abuse. In the future, Internet border inspection may be considered as natural, routine, and harmless as physical border inspections, which are assumed to be a basic part of protecting people and business inside countries, around the world.

B. AREAS FOR FURTHER CONSIDERATION

There are several issues that should be given additional consideration in future analysis and discussion of Internet border inspection.

Routers can be used to parse traffic based on almost any of the normal header information. This includes protocols, ports, and services. One idea, briefly mentioned in Chapter III, was the idea that certain traffic could be taken out of the normal stream based on the service rather than the IP address alone. This may be valuable to Customs authorities if they identify services used to traffic in information goods such as software, movies, and music. The practical ways for implementing this in the context of Internet border inspection should be explored.

Another issue which was briefly touched on in the discussions of legal jurisdiction was the potential role and authority of the Department of Defense to defend the United States against an information warfare attack launched during a time of war or hostilities. Whether this role is minor or significant has yet to be determined. However, it would have been unthinkable when the United States was young to not have military fortifications to protect the major routes of commerce along the borders from potential invasion or attack from armies and navies in their day. The idea of the cyber-fortifications at the border may make more sense as cyber warfare is developed outside

US borders. This should also be considered further in the context of Internet border protection.

Chapter III described Internet services comparable to people crossing the border unchecked. These services, which include Telnet and Secure Shell, represent a relatively small portion of the total Internet traffic. However, because they are one of the major ways that hackers gain access to victim computers to conduct their crimes, additional consideration could be given to the idea of requiring individuals using these services to hold a cyber equivalent of a passport or visa when crossing the border into the United States. Routers are able to block based on a service and not just an IP address. This might mean that a new IP service, like Telnet, would be created requiring additional authentication to conduct system administration across borders, and the normal Telnet and Secure Shell services might not be allowed to cross the border. Significant additional thought would be needed to fully develop such a concept.

There is one additional area deserving further consideration. More thought should be given to how the proposal for Internet border inspections should be discussed and developed. Additional discussion and development could be done in conjunction with allies or even in an international forum, or it could be conducted entirely within the United States. Once it was developed it could be offered to other countries, or efforts could be made to keep it within the United States. Each approach would have short-term ramifications and potentially long term impacts as well. If it were implemented in a balanced and narrow way in conjunction with other nations that respected individual rights, it could enhance security for all nations including the United States, but there are many other aspects to consider in this discussion. This issue warrants additional exploration.

C. CONCLUSION

The idea of Internet border inspection and protection is multifaceted. It includes technical, legal, and political aspects that could be areas for significant exploration in themselves. With proper consideration, this idea may prove a fertile source for further discussion, research, and eventually even policy proposals.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A – TITLES OF UNITED STATES CODE

Title 1, General Provisions
Title 2, The Congress
Title 3, The President
Title 4, Flag and Seal, Seat of Government, and the States
Title 5, Government Organization and Employees; and Appendix
Title 6, Surety Bonds (Repealed)
Title 7, Agriculture
Title 8, Aliens and Nationality
Title 9, Arbitration
Title 10, Armed Forces; and Appendix
Title 11, Bankruptcy; and Appendix
Title 12, Banks and Banking
Title 13, Census
Title 14, Coast Guard
Title 15, Commerce and Trade
Title 16, Conservation
Title 17, Copyrights
Title 18, Crimes and Criminal Procedure; and Appendix
Title 19, Customs Duties
Title 20, Education
Title 21, Food and Drugs
Title 22, Foreign Relations and Intercourse
Title 23, Highways
Title 24, Hospitals and Asylums
Title 25, Indians
Title 26, Internal Revenue Code; and Appendix
Title 27, Intoxicating Liquors
Title 28, Judiciary and Judicial Procedure; and Appendix
Title 29, Labor

Title 30, Mineral Lands and Mining

Title 31, Money and Finance

Title 32, National Guard

Title 33, Navigation and Navigable Waters

Title 34, Navy (Repealed)

Title 35, Patents

Title 36, Patriotic Societies and Observances

Title 37, Pay and Allowances of the Uniformed Services

Title 38, Veterans' Benefits; and Appendix

Title 39, Postal Service

Title 40, Public Buildings, Property, and Works; and Appendix

Title 41, Public Contracts

Title 42, The Public Health and Welfare

Title 43, Public Lands

Title 44, Public Printing and Documents

Title 45, Railroads

Title 46, Shipping; and Appendix

Title 47, Telegraphs, Telephones, and Radiotelegraphs

Title 48, Territories and Insular Possessions

Title 49, Transportation

Title 50, War and National Defense; and Appendix

Source: www.uscode.house.gov

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dr. Linton Wells
   Principal Deputy Assistant Secretary of Defense (NII), Dept. of Defense
   Washing ton DC

4. Martha Stansell-Gamm
   Chief, Computer Crime and Intellectual Property Section, Dept of Justice
   Washington DC

5. Robert Liscouski
   Assistant Secretary of Homeland Security for Infrastructure Protection
   National Cyber Security Division (NCSD), Dept of Homeland Security
   Washington DC

6. National Infrastructure Protection Center
   Washington DC

7. HQ Air Force Office of Special Investigations
   Andrews AFB, MD

8. Kevin Farrell
   Naval Information Warfare Activity
   Washington, DC

9. Air Force Computer Emergency Response Team
   Lackland AFB, TX

10. Joint Task Force –Computer Network Operations
    Washington DC

11. Joint Information Warfare Center
    Lackland AFB, TX

12. Russell Jokinen
    Customs and Border Protection
    Washington, DC