A NETWORK OF NATIONS: WHY EFFECTIVE CYBERSECURITY REQUIRES INTERNATIONAL COLLABORATION

A Thesis
submitted to the Faculty of
The School of Continuing Studies
and of
The Graduate School of Arts and Sciences
in partial fulfillment of the requirements for the
degree of
Master of Arts
in Liberal Studies

By

Eric Hanson, B.A.

Georgetown University
Washington, D.C.
11/05/2009

A NETWORK OF NATIONS: WHY EFFECTIVE CYBERSECURITY REQUIRES INTERNATIONAL COLLABORATION

Eric Hanson, B.A.

Mentor: Ralph Nurnberger, Ph.D.

ABSTRACT

The Internet has revolutionized modern life across the globe, enabling dramatic advancements in technology and communications. Furthermore, the Internet has triggered a dramatic improvement in the efficiency and capabilities of people, organizations, and governments around the world. Regretfully, the Internet also exposes its users to increasing collection of new risks and vulnerabilities. These risks affect organizations and individuals across the planet, but they also pose unique threats to nations. Coupled with the architecture of the Internet itself, these risks demonstrate why international involvement is required for effective cybersecurity.

One examples of such a risk involves threats to the Domain Name System (DNS), a critical component employed in countless applications on the Internet that depend upon DNS reliability and integrity. Despite the serious consequences of disrupting these activities, vulnerabilities in the DNS that enable such disruptions have been known for over a decade. Only relatively recently has progress been made on the adoption of DNS Security Extensions (DNSSEC), a collection of security “fixes” that would close many

security holes within DNS, with a great deal more work needed before these issues can be considered fully addressed.

Botnets offer another example of a key challenge to international cybersecurity efforts and illustrate how the surge of power and productivity created by the Internet has also created opportunities for the world's criminal minds. Exploring the impact botnets have on cybersecurity and the Internet illustrates how basic aspects of network communication and everyday activity on the Internet have been leveraged to create the equivalent of a geographically-dispersed supercomputer. Botnets pose unique and complex challenges to a wide range of international relations issues and activities, most notably law enforcement and data protection.

Thankfully, increasingly many international bodies have begun to recognize the importance of cybersecurity and their efforts, though in many cases nascent and unproven, represent an important step. Through careful planning, appropriate involvement of the necessary stakeholders, and a proper respect for the global nature of these new threats, countries can achieve essential progress in cybersecurity.

TABLE OF CONTENTS

INTRODUCTION

The Internet is an integral part of the lives of millions of people around the world. Governments, businesses, and individuals across the globe have come to depend upon the capabilities and services that the Internet provides. Real-time communications, electronic financial transactions, data transfer, access to government services, and a myriad of other capabilities made possible by the Internet have truly revolutionized the modern age. Unfortunately, this revolution has not come without cost; while the Internet has ushered in a new era of prosperity and progress it has also brought with it dramatic new risks to organizations, individuals, and even nations. Increasingly, governments have begun to recognize the implications of these risks and taken measures to address them, resulting in a variety of efforts devoted to cybersecurity and its many related aspects. While many of these measures are conducted on a domestic basis, there also exists a growing category of activity devoted to international efforts. Recognizing the impetus behind these international efforts is important not only in understanding the current landscape, but also for appropriate planning for the future of international efforts on cybersecurity. This paper represents an effort to explain how effective cybersecurity both requires international collaboration and greatly benefits those nations involved.

In order to properly frame the text that follows, a few introductory points and clarifications are necessary. “Cybersecurity” is a very broad term which can be interpreted in a variety of different ways. For the purpose of this paper, the term will be

employed to indicate those efforts designed to ensure security of the interconnected system of networks known as the Internet. While this categorization is somewhat simplistic and neglects a wide range of other activities that may also be deemed cybersecurity, it aids comprehension of the material, particularly for the non-technical reader. Additionally, this paper is directed towards policy-makers who may be unfamiliar with the underlying concepts and background of the issues and as such is written in a style tailored to such an audience. While several aspects of the subsequent chapters will include technical explanations, these technical explanations are provided as an aid for understanding some of the underlying factors affecting international cybersecurity efforts. Finally, it is the hope of the author that this work will pique the interest of readers and encourage them to delve more deeply into cybersecurity studies. Each of the topics herein is touched upon briefly, however a wealth of additional material and analysis exists on all.

CHAPTER I

THE CYBERSECURITY CHALLENGE

The establishment and exponential growth of the Internet has triggered a dramatic improvement in the efficiency and capabilities of people, organizations, and governments around the world. Regretfully, this increased efficiency and capability has not come without costs. Today there are a wide range of threats and vulnerabilities that result from cyberspace and the utilization of the Internet. These threats and vulnerabilities, coupled with the architecture of the Internet itself, demonstrate why international involvement is required for effective cybersecurity.

The first half of this chapter examines the foundation of the Internet and demonstrates how its underlying structure and philosophy contributes to its international nature. The second half of this chapter explores several of the new threats and vulnerabilities that the proliferation of computer networks and the Internet has brought, illustrating why President Barack Obama declared cybersecurity a United States national security priority.[1]

[1] Joseph Weber, "Obama: Cybersecurity a 'national priority'," *Washington Times*, May 29, 2009.

What is the Internet?[2]

Many people who use the Internet may not understand its architecture or what actually makes it work. The emergence of the World Wide Web in the 1990's boosted the popularity of the Internet to such a degree that to this day many users consider it synonymous with the Internet itself, yet in reality it is only one of many different applications that make up the globally interconnected system of networks known as the Internet. If the Internet can be visualized as a system of roads, the World Wide Web would be one of many vehicles on those roads. Other vehicles include e-mail, file-transfer protocol, voice over internet protocol (VOIP), and countless other applications and utilities which rely upon the Internet. In order to truly understand why international cybersecurity efforts are needed and how they may benefit nations, we must first understand how the Internet actually works.

At its core, the Internet is a means of transferring information between different computer networks. The Internet enables the transfer of information from one computer to another regardless of physical or logical distance between the two machines. In many ways the process can be compared to the postal service. If one wishes to send a physical package to someone, the package must have both a return (i.e. originating) address and a destination address. In a similar manner, computers transfer information in discrete

[2] The description of the Internet contained within these next several pages is necessarily brief and does not give justice to the incredible complexity of Internet architecture. In several cases the explanation may strike more technically-informed individuals as overly simplified. This represents a deliberate decision on the part of the author to limit technical explanations in order to better focus on policy considerations.

quantities known as “packets.” Each device connected on the Internet must have a unique address so that its traffic may be routed accordingly. As such, let us imagine two computers, Computer A and Computer B, each of which is connected to the Internet through an Internet Service Provider (ISP) and is given a unique address (Internet Protocol Address or IP address).

After purchasing their connections to the Internet, the owners of Computer A and Computer B wish to communicate. Because of the immense number of devices connected to the Internet and the dynamic nature of those devices (devices are added and removed from networks every day), it is impossible for all computers to know the IP address for every device connected to the Internet. Instead, devices known as routers are used to ensure packets are delivered to the correct address. Routers, as one might assume, *route* packets between computers; each router contains a set of directions (a routing table) for delivering packets to their destinations. Due to a router’s limited capability to store information, these routing tables only contain the directions for a discrete number of addresses. If Computer A and Computer B are located on the same network (such as one you might have in your home or a small business), the router governing that network would recognize the destination IP address of Computer B and will immediately route the packets appropriately, completing the transfer. Routing becomes more complex when the two computers are not located on the same network.

Imagine an office environment in which you are a lowly desk clerk just beginning your employment. Suppose you have prepared a document that needs to go to the

company Chief Executive Officer (CEO). Being a simple desk clerk, you cannot send the document directly to the CEO; instead, the document must first go to your immediate supervisor. Unfortunately, your immediate supervisor is also too junior to send the information directly to the CEO and instead must send it to her supervisor for approval. This cycle repeats until the document is eventually given to someone who can deliver it directly to the CEO. Routers are organized in a similar hierarchical manner; each routing table has a finite number of addresses to which it may deliver information. If the destination IP address is not located in the routing table, the router will forward the packets to a higher-level router. This cycle repeats until the packets are forwarded to a router that recognizes the destination IP address. From there, the packets may travel "down" another set of routers until eventually reaching the final destination.

The Internet factors into this elaborate routing scheme when Computer A and Computer B are located on entirely different large networks known as Network Service Providers (NSPs). NSP networks typically cover entire countries or regions, and may lease Internet access for a wide variety of smaller ISPs. As such, NSPs are typically referred to as providing "backbone" service. Because even these large networks are not big enough to deliver packets to all computers across the world, all NSPs have agreements in place to transfer their packets through several information exchange points known as Network Access Points (NAPs) or Metropolitan Area Exchanges (MAEs). These agreements enable the global interconnection of different networks that we refer to as the Internet. Based on our earlier example, information will travel from Computer A

"up" through a series of routers until it reaches a NSP that transfers the information across the Internet backbone to another NSP serving Computer B's network. From there, the information travels "down" a similar set of routers until ultimately arriving at Computer B.

The truly international aspects of the Internet come with this interconnection of multiple regional networks across the globe. While large NSPs may control a significant portion of Internet traffic in their own region, they have limited power over the Internet as a whole due to the presence of other NSPs around the world. Furthermore, since the value of the Internet depends on reliable transmission of information to a destination regardless of what network that destination resides on, international cooperation is paramount. As later sections of this paper illustrate, the very same global interconnection and distributed management that make the Internet such a revolutionary tool of communication also make ensuring its security such a difficult task.

How We Got Here: The Origins of the Internet

The complete story of the birth and growth of the Internet is one which has been covered extensively and lies outside the scope of this work. Despite this, understanding the necessity for international cooperation on cybersecurity also requires understanding the basics of how the Internet was established. Understanding its origins reveals several fundamental characteristics that helped shape the Internet into what it is today and illustrate why effective cybersecurity cannot be achieved by a single nation.

ARPANET is Born

In the 1950's and 1960's computers were bulky, immense, and expensive electronics which often ran on specially formatted punch cards fed into the machine to generate actual computation. One of the many difficulties in using these early computer systems was that most of the computer's time was spent awaiting human instructions via the terminal; once computers received properly formatted instructions, they typically spent "very little time" processing that data.[3] As a result, researchers wishing to use these machines often encountered long waits and scheduling difficulties since each were forced to compete for access time with other researchers. In order to address this shortcoming, a technique known as "time sharing" was developed. Time sharing essentially split the computer's processing power into several different streams, each directed to a different project filled at different terminals (smaller computers connected to the larger processing system that performed the computations).[4] By 1966, employees of Advanced Research Project Agency (ARPA) began designing a computer network that could extend the practice of time sharing across geographically distant computer systems. This computer network would ultimately become known as ARPANET, and in many ways was the next logical evolution of time sharing.[5]

---

[3] Janet Abbate, *Inventing the Internet* (Cambridge, Massachusetts: The MIT Press, 1999), 25.

[4] Ibid., 24.

[5] James Gillies and Robert Cailliau, *How the Web Was Born: The Story of the World Wide Web* (Oxford: Oxford University Press, 2000), 17.

Philosophies underlying ARPANET

Beyond the architecture and physical framework of ARPANET, several of its underlying philosophies and design decisions have helped shape key issues in cybersecurity and the overall operation of the Internet. An early example of such a philosophy is the concept of open access. The initial plans for the development of ARPANET called for entry points on to the network (i.e. terminals where other computers could be accessed) only at specific sites where computers were connected to the time sharing network. By 1971, however, the design would change and the decision was made to grant certain non-host sites access to the network.[6] This seemingly minor decision was actually fundamental to building the Internet as we know it today. To this point, everyone involved in the ARPANET work had assumed that access would be restricted to those sites that could provide their own resources for the good of the network. The willingness of ARPANET administrators to allow for the possibility of open access in the absence of those resources was truly revolutionary. This policy of open access to information would become a foundation of the Internet and has repercussions even to this day, ensuring that all networks can connect to the Internet regardless of what contributions they may bring. Furthermore, this simple concept creates significant factors for consideration with regard to cybersecurity efforts.

This philosophy of openness could also be found in the development of many of the "protocols" that the early network required. The creation of ARPANET was not an

[6] Abbate, *Inventing the Internet*, 64.

easy task, particularly at the technical level; simply connecting the computers to one another was not enough as the computers at the different nodes were each unique and in many cases ran completely different operating software. These devices each spoke a different language and could not yet effectively communicate with each other. One potential solution to this problem was to force each of the computers to utilize the same language, rewriting their initial programming to be consistent across all of the systems. ARPANET's administrators quickly found, however, that the technical representatives from each of the nodes had little desire to engage in a wholesale revision of their operating languages to bring them in line with each of the other nodes.[7] This reluctance could have jeopardized one of the ARPANET's foremost goals: to integrate separately administrated entities into a common utility.[8] As a result, the founders of ARPANET were determined to develop common languages that would enable the dissimilar computers to communicate with each other while minimizing the additional burden on the computer administrators.[9] This practice would eventually be a source of controversy as internetworking continued; by the mid 1970's a battle of protocols erupted between ARPANET engineers and a group of telecommunications carriers. The carriers had devised their own protocol which they wished to see adopted universally to form a single

[7] Ibid., 67.

[8] David Clark, "The Design Philosophy of the DARPA Internet Protocols," *ACM SIGCOMM Computer Communication Review* 18, no. 4 (August 1998): 107.

[9] Abbate, *Inventing the Internet*, 67-68.

data network.[10] Ultimately, however, ARPA's attitudes would win over and their model of open access to the Internet would become the network standard most widely accepted across the United States and eventually the world.[11]

A final example of a foundational philosophy of ARPANET that continues to affect the Internet was the trust placed in collaborative and consensus-driven development. The protocols referenced above were in fact developed by the Network Working Group (NWG), a group of largely inexperienced researchers and grad students which had been informally established when an ARPANET administrator had called together programmers from the initial ARPANET nodes. In fact, many within the group expected a professional crew to take over their work, and only later began making official record of their conversations and decisions.[12] Even within this group, the desire for consensus and collaboration was apparent: rather than issue official statements or proclamations on decisions regarding protocols and other business, the group issued documents entitled Request for Comments (RFC).[13] These RFCs would eventually become a hallmark of ARPANET and later the Internet, harkening back to these early days and the desire for all involved in the functioning of the network to share their input. To this day, the collaborative model founded by ARPANET affects international

[10] Ibid., 162.

[11] Ibid., 178.

[12] Gillies and Cailliau, *How the Web Was Born*, 29.

[13] Ibid.

engagement on cybersecurity through encouraging involvement of a wide variety of pubic and private entities across the globe.[14]

The End of ARPANET

ARPANET continued to grow and evolve throughout the 1960's and 1970's. During this evolution, ARPANET retained its underlying philosophies of open access and collaboration and maintained its goal of achieving greater interconnection with distributed networks regardless of their design or orientation. Local networks, including proprietary commercialized systems, had sprung up in the years since ARPANET's creation, and through the use of the protocols developed by the NWG, these networks were capable of communicating with one another. This was put to the test in 1977, when computer scientists were able to send data across three of these independent networks.[15] This initial demonstration provided proof that the protocols could be extended beyond the actual ARPANET nodes themselves. Additionally, the demonstration showed that independent networks could maintain their individual systems and practices while having a connection to ARPANET and other networks. This retention of autonomy made it considerably easier for outside networks to participate in interconnection. As a result, following the demonstration a wide variety of public and private networks both domestic

[14] Today, RFCs are still utilized in the administration of the Internet. A full listing of current RFCs can be found on the website of the Internet Engineering Task Force at http://www.ietf.org/rfc.html.

[15] Abbate, *Inventing the Internet*, 131.

and international would join ARPA's interconnection system, establishing the first iteration of what would be known as the Internet.[16]

Ironically, the growing popularity of the Internet that ARPA had helped create through its protocols and design philosophies would eventually lead to ARPANET's decommission. During the 1980's, ARPANET would fall by the wayside while a variety of other organizations and entities would contribute to the continued development of the Internet. The collaborative and interconnected nature of the Internet meant that contributors came from many fields including the National Science Foundation (NSF) and other component of the U.S. government, university administrators, and private Internet service providers.[17] The creation of NSFNET in the mid 1980's would ultimately prove the end of ARPANET. NSFNET was developed by the NSF as a widespread national network in the United States that linked university computer centers to regional networks; these regional networks were then connected with a broader national network.[18] As NSFNET was established and popularity of the system grew, bolstered by the universities and removed from the military connections of ARPANET, ARPANET's administrators realized that their aging technology had run its course. As such, once NSFNET's backbone and system was in place, the remaining functions from ARPANET

[16] Ibid., 132-133.

[17] Ibid., 181.

[18] Ibid., 191.

were simply transferred to NSFNET; by 1990 the last ARPANET node had been transferred and the system itself was decommissioned.[19]

Privatization of the Internet

While the creation of NSFNET helped push the Internet further into the world of public interest, it continued to be administered by a government agency and the data transferred along the backbone (critical to interconnection) was limited to nonprofit research and education.[20] Privatization would ultimately be the step needed to propel the Internet from the minds of researchers and computer scientists and into the activities of common citizens and peoples across the planet. Ultimately, through a variety of efforts and negotiations involving government agencies, internal components of NSF, commercial network service providers, and NSFNET users, the NSFNET backbone would be replaced by a system of commercial backbones which would interconnect through a series of "exchanges" that enabled different proprietary networks to connect with each other.[21]

Once the NSFNET backbone was available for commercial use the computer industry was quick to create its own products, services, and applications that could be used on the Internet. The growth of these commercial offerings contributed greatly to the popularity and utility of the Internet. With privatization a whole host of new possibilities

[19] Ibid., 194.

[20] Ibid., 195.

[21] Ibid., 199.

arose; no longer restricted to applications that had immediate research or educational utility, developers created applications to cater to new users from the business community, services directed towards individual consumers, and even games.[22] However, one application which revolutionized the Internet and to this day remains one of the most powerful applications was the World Wide Web.

Birth of the World Wide Web

One of the primary factors behind the birth of the World Wide Web was visual. Despite the widespread growth of the Internet architecture and the increasing interconnection between private networks, most applications connecting to the Internet remained text-based. The two most popular: e-mail and file-transfer protocol, were revolutionary in terms of transferring information, but their drab appearances did not inspire excitement. Several commercial enterprises sought to fill this gap and created their own services which incorporated graphics and created a much more aesthetically pleasing experience for many users, yet these services were often proprietary and in many ways seemed counter to the fundamental characteristics of the Internet as an open and interconnected community. A solution would eventually be found due to the dedication and creativity of a group of researchers at the European Organization for Nuclear Research (CERN).

[22] Ibid., 200.

Though the technical details of the creation of the World Wide Web are fascinating and make for an interesting story, they are unnecessary for this study. Suffice to say, through ingenuity and vision the researchers at CERN were able to establish the foundations for the World Wide Web which directly led to the subsequent explosion of popularity of the Internet. The establishment of the World Wide Web and its commitment to open access allowing any group to create its own web page spurred creativity from countless areas. Through the World Wide Web, the Internet would eventually be transformed into the entity we know today, acting as a conduit for business, public relations, social activity, political forum, and countless other applications that one may now access through a simple address entered into a web browser.

The Case for National Interest in Cybersecurity

This brief explanation of how the Internet is designed and the philosophical underpinnings of its design have demonstrated that that the Internet is international in nature. However, even accepting all of this, nations may still ask the question, "Why should we care?" Though a valid question, a simple search of the news presents several answers:

- In August 2005 news reports described the systematic targeting of U.S. Department of Defense and defense contractor computer networks by computers located in China. [23] The exact motivations and identities of the attackers were

[23] Bradley Graham, "Hackers Attack Via Chinese Web Sites," *The Washington Post*, August 25, 2005.

never released, but many suspected the series of attacks, codenamed Titan Rain, were deliberate attempts by the Chinese military to steal information.[24]

- On April 27, 2007 the government of Estonia relocated a statue commemorating Russian soldiers that had fought against the Nazis.[25] Shortly thereafter, a series of attacks were aimed at several Estonian government, business, and media websites which ultimately forced many of the websites to shut down temporarily. The cyber attacks lasted several weeks, and were widely reported to originate from Russia.[26]

- In July 2009 US law enforcement officials arrested Sergey Aleynikov, a computer programmer who had recently resigned from a position with Goldman Sachs. Mr. Aleynikov had been accused of stealing "sensitive automated trading codes and uploading them to a [computer] server based in Germany."[27]

- On April 8, 2009, the *Wall Street Journal* reported that "cyberspies" had infiltrated the United States electrical grid and had left behind computer programs that would enable them to re-enter the system and cause disruptions to the national grid.[28]

- In early July 2009 a wave of cyber attacks simultaneously struck several websites in South Korea and the United States, including the White House and the Blue House (the South Korean executive office).[29] The attacks were initially attributed as originating from North Korea, but those findings were called into question

---

[24] Nathan Thornburgh, "Inside the Chinese Hack Attack," *Time*, August 25, 2005.

[25] Robert Vamosi, "Cyberattack in Estonia--what it really means," *CNET News*, May 29, 2007, http://news.cnet.com/Cyberattack-in-Estonia-what-it-really-means/2008-7349_3-6186751.html (accessed July 28, 2009).

[26] *BBC News*, "The cyber raiders hitting Estonia," May 17, 2007, http://news.bbc.co.uk/2/hi/europe/6665195.stm (accessed July 28, 2009).

[27] Greg Farrell, "Ex-Goldman employee accused of theft," *Financial Times*, July 6, 2009.

[28] Siobhan Gorman, "Electricity Grid in U.S. Penetrated by Spies," *Wall Street Journal*, April 8, 2009.

[29] Hyung-Jin Kim, "Report: NKorean army suspected over cyberattacks," *Associated Press*, July 11, 2009.

when later examinations indicated they may have come from the United Kingdom.[30]

These examples illustrate only a few of the more prominent reasons why nations should take an interest in cybersecurity. With the proliferation of computer systems and the increasing reliance upon the Internet for business and governance has come the proliferation of threats and challenges posed by these advances. Furthermore, the threats and challenges are so varied that several categories exist, including cybercrime, defense, critical infrastructure security, and others.

Cybercrime

One of the areas of significant challenge to international cybersecurity efforts is cybercrime.[31] Regretfully, the same technology that has enabled a revolution in communications and processing has also enabled a whole new world of criminal enterprise. Surveying the landscape of cybercrime today one finds a bewildering variety of acts with effects ranging from petty theft to multi-million dollar heists. One recent study of cybercrime identified eleven different categories including: theft of telecommunications services; communications or data storage in furtherance of criminal conspiracies; information piracy, forgery and counterfeiting; dissemination of offensive

[30] Jack Shofield, "British hacker claimed to be behind US and Korean attacks," *Guardian.co.uk*, July 15, 2009, http://www.guardian.co.uk/technology/2009/jul/15/hackers-internet-attack (accessed July 28, 2009).

[31] While the term "cybercrime" may ring of jargon and sensationalism (after all, in many cases cybercrime is merely crime that utilizes cyberspace or computers as a vehicle), it has become the term used by many in the field. It is relevant to note however that while many cybercrimes are similar to more "traditional" notions of criminality, the nature of cyberspace and the tactics of the criminals often make prosecuting and combating cybercrime a unique task.

materials; stalking; electronic money laundering and tax evasion; electronic vandalism and terrorism; sales and investment fraud; illegal interception of telecommunications; and electronic funds transfer fraud. Even this list, the study's author recognized, represented only a fraction of the possible cybercrimes.[32]

While some nations have taken initiative to develop their own laws and regulations regarding domestic law enforcement, cybercrime by its very nature is often multinational. A hacker breaking into a United States-based network to steal credit card information may live in Germany, perform his infiltration through a compromised system located in Brazil, and wire money from the stolen credit card accounts to a Swiss bank. Furthermore, difficulties in attribution may make confirmation of a thief's identity a monumental task requiring cooperation between law enforcement and network administrators in several countries. Given these and other challenges, it is not surprising to find that international law enforcement cooperation regarding cybercrime is an area of significant concern for many nations.

Defense

National defense offers another category where threats necessitate that states take cybersecurity measures. Similar to civilian populations, the militaries of the world also depend upon the Internet to communicate, organize, and execute their missions. While many militaries mitigate this through the development of proprietary military networks

[32] Peter Grabosky, "The Global Cyber-Crime Problem: The Socio-Economic Impact" in *Cyber-Crime: The Challenge in Asia*, ed. Roderic Broadhurst and Peter Grabosky (Hong Kong: Hong Kong University Press, 2005), 31.

that are not accessible via the public Internet, in many situations this separation is neither practical nor desirable. Cutting oneself off from the Internet may improve security, but it also removes the global interconnectedness and the ease and effectiveness of the communications tools that the Internet brings.

Attacking communications systems has been a tactic for as long as there has been war, and the Internet and military networks serve as merely the latest technology target. Whereas bombs may have once destroyed telegraph lines, today cyber attacks could potentially cripple a military network, disrupting or disabling key communication of critical data in a time of need. Furthermore, a nation's military may rely heavily upon certain aspects of the private sector as well, so even if a military is insulated from direct cyber attack the military and even the nation as a whole may suffer the effects of indirect attack upon supporting infrastructure or key dependencies.

Espionage presents another facet of the connection between cybersecurity and national defense. Just as the disruption of communications networks has evolved through the ages, so too has the art of spying on one's enemies. Whereas espionage at one point relied primarily on inserting covert operatives into the physical strongholds of one's adversary, the dramatic results of proficient cyber attacks can yield information far beyond what a single operative could physically obtain. Rather than stealing physical files from the archives of your enemy, in many cases it is much simpler and safer to infiltrate their computer systems and capture files residing on the hard drives of government computers connected to the Internet. This, too, is a tactic that has been

proven in the modern day and remains a significant source of concern for nations around the world.

Critical Infrastructure Security

The protection of a nation's critical infrastructure offers another area that warrants the concern of national governments. Critical infrastructure, as defined by the 2009 National Infrastructure Protection Plan (NIPP) issued by the United States Department of Homeland Security, consists of "systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters…."[33] The NIPP identifies 18 distinct critical infrastructure (also including several identified as "key resources") sectors, ranging from dams and nuclear power plants to communications and information technology.[34] While much of the document focuses on physical security, cybersecurity is specifically called out as an area where it is critical for government and private industry to collaborate, including the addition of an appendix devoted entirely to cybersecurity across each of the 18 sectors.[35] Furthermore, the United States clearly views critical infrastructure cybersecurity as a significant concern, as evidenced by a statement for the record by the Director of National Intelligence:

[33] U.S. Department of Homeland Security. *National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency*. Washington, DC: Government Printing Office, 2009, 109.

[34] Ibid., 3.

[35] Ibid., 113.

> "…the growing connectivity between information systems, the Internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, energy pipelines, refineries, financial networks, and other critical infrastructures… A successful cyber attack against a major financial service provider could severely impact the national economy, while cyber attacks against physical infrastructure computer systems such as those that control power grids or oil refineries have the potential to disrupt services for hours to weeks."[36]

Comments such as these demonstrate that ultimately, many of the reasons why critical infrastructure cybersecurity warrants the attention of nations are similar to why critical infrastructure physical security deserves national attention. Physical disruption or destruction of these infrastructures can result in loss of life or severe economic damage. While cyber attacks are not generally regarded as having significant potential of loss of life, their potential for causing economic damage and cascading effects is dramatic.

Conclusion

This chapter has illustrated that the foundations and basic architecture of the Internet, in addition to the unique threats and challenges it poses, clearly make a case for international involvement in cybersecurity. The categories of threats briefly described herein are only a few examples of why nations should concern themselves with cybersecurity. The next two chapters will build upon these points through an examination of two distinct case studies of international cybersecurity efforts. These case studies show

[36] Director of National Intelligence, "Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee, Statement for the Record, March 10, 2009," 39.

why international involvement is necessary, and further demonstrate some of the challenges such involvement brings.

CHAPTER II

WHAT'S IN A NAME?

The Internet has created a wealth of convenience as businesses everywhere have switched many services previously offered only in person to online options available from the nearest computer. Banks are among the many businesses engaging in these practices, giving their customers access to a wide variety of account management controls from the comfort of one's own home. Suppose that one afternoon you decide to take advantage of these services and sit down at your computer, open up your web browser, and type "www.mybank.com" into the address line. The familiar look of the bank's webpage greets you, along with two text input boxes where you enter in a username and password that you created when you first registered your account with the bank. After entering your username and password your account information is displayed along with the various options available to you, including the ability to transfer money, pay bills, file for a loan, and other options offered by your bank. You notice your most recent paycheck has been deposited in your account and everything is as it should be, close your web browser, and go about your day.

The next afternoon you drive to the bank and attempt to take money out of the ATM only to find that your bank account now shows zero funds. Subsequent investigation reveals that during the previous evening someone accessed your account and electronically transferred your entire balance, leaving your account empty. The

bank's network records show that your account was not broken into through a hole in their systems; instead, your account was accessed via the bank's webpage through the use of your username and password. Eventually, computer forensics experts discover that though you typed in "www.mybank.com" into your web browser and were directed to what you thought was the correct website, in fact you were the victim of an attack which affected the Domain Name System (DNS). The thief re-routed your navigation from the bank's webpage to a page cleverly designed to mimic the bank's homepage in every way, right down to the username and password input boxes. When you entered in your information it was quickly downloaded to a text file, while you were redirected to the actual bank's webpage to appear that nothing was wrong. Later that evening the thief consulted the text file, discovered your information, and used it to clean out your account.

The above scenario illustrates only one of a variety of ways in which users rely upon the Internet to manage sensitive affairs every day. The DNS, a critical component underlying the structure of the Internet itself, is employed in countless applications that depend upon its reliability and accuracy to carry out their functions. The above example could just as easily have consisted of the disruption of many other activities that utilize the DNS including the routing of emails or files, accessing confidential medical records online, using a Voice-Over-Internet-Protocol phone, electronic financial transactions between businesses, an antivirus software company delivering the newest signatures to defend against computer viruses, or others.

Despite the serious consequences of disrupting these activities, vulnerabilities in the DNS that enable such disruptions have been known for over a decade. Only relatively recently has progress been made on the adoption of DNS Security Extensions (DNSSEC), a collection of security "fixes" that would close many security holes within DNS, with a great deal more work needed before these issues can be considered addressed. Understanding DNSSEC and why it has yet to be widely implemented is a complicated affair that illustrates how international elements fit into the underlying structure of the Internet and, in turn, why robust cybersecurity requires the participation of many nations.

The Domain Name System

Before we can understand DNSSEC and the complex web of international involvement it requires, we must first understand how the DNS contributes to the everyday functioning of the Internet. Recall that the previous chapter discussed how computers on the Internet each have a unique identifier called an IP address; these unique identifiers are necessary in order to distinguish between computers on the Internet and ensure that traffic is delivered appropriately. ARPANET's early administrators realized the need for such a system when their burgeoning network encountered difficulties with similarly named users connecting to the same server. Smaller networks had no difficulty distinguishing computers or users because they would require each user to select a unique identifier, yet the distributed nature of even the early ARPANET (with its desire to

maintain local administrators' autonomy over the governance of their own networks) led to several computers and users on different networks selecting the same identifier.

Apparently "Frodo" was common enough across the technical community at the time that multiple sites across the country had users with the name, causing confusion on the network when e-mails were received.[1] As a result, researchers recognized that a naming scheme was necessary in order to establish some sense of organization and a way to differentiate between these users.

The result of these early researchers' efforts was the DNS, a hierarchical naming system that allowed for limited duplication of names while ensuring the names ultimately remained unique. At the top of this hierarchical structure lies the "root" or "root zone", while below reside several high level "domains" known as top-level domains or TLDs. ARPA originally established only six of these domains (edu, gov, mil, com, org, and net), however, several additional domains were added later and new domains continue to be added on a semi-regular basis.

The concept behind DNS was that each domain would have an internal naming system that ensured users could be uniquely identified, yet usernames could be safely duplicated across the domains without conflict. This was accomplished by naming computers with the use of the "@" symbol so that they would be listed as user@domain;

[1] Katie Hafner and Matthew Lyon, *Where Wizards Stay Up Late: The Origins of the Internet* (New York: Simon & Schuster, 1996), 252.

thus, frodo@edu would not be confused with frodo@gov.[2] Eventually the Internet would grow to include further subdivisions within the domains (subdomains) which can be readily seen in e-mail addresses to this day in the form user@subdomain.domain (e.g. john@yahoo.com).

With the advent of the World Wide Web in the 1990's, it became necessary to employ the DNS not only to identify individual users, but also to identify different hosts or servers that users would connect to in order to view a webpage. IP addresses, though sufficient for ensuring a unique identity for each computer connected to the Internet, were not easy to remember and did not allow users to navigate webpages easily. As a result, Tim Berners-Lee, a researcher at the European Organization for Nuclear Research, developed what would come to be known as the Uniform Resource Locator (URL).[3] URLs built upon the foundations of DNS by applying the hierarchical naming scheme to webpages to ensure that duplicates can be present across domains, but never within the same layer of the domain itself. Just as there could exist a "frodo" user on both the gov and edu domains, so too can there exist a www.frodo.com and a www.frodo.net because they exist on separate domains (.com and .net, respectively). Further divisions are indicated with a "/" and also retain the structure to prevents duplication, i.e. there can be a www.frodo.com/ring and a www.frodo.net/ring. As subsequent sections will illustrate, this fundamental system of dividing the Internet into domains, each with their own

[2] Abbate, *Inventing the Internet*, 189-190.

[3] Gillies and Cailliau, *How the Web Was Born*, 206.

organizational structure that follows a similar naming scheme yet remains autonomous, is key to understanding why the deployment of DNSSEC entails so many international elements.

One final technical detail necessary for this brief overview of DNS is how it actually works. The process is essentially the same as the process of how routers deliver traffic as presented in the previous chapter. Upon typing "www.mybank.com" into your web browser, your computer requests the location of the address from the nearest router that your ISP has configured to process DNS requests, known as a name server. After receiving the request, the name server translates "www.mybank.com" into a machine-recognizable form, the IP address. The name server then responds to the request with the IP address and your computer follows the directions to load the webpage of your bank. Similar to the example given in Chapter 1, if the name server does not know the address of the webpage it will forward the traffic on to a continuous chain of higher-level routers until the appropriate address can be found. Along the way, the various requests are given identification numbers (transaction IDs) to ensure that requests maintain proper routing back to your computer once the final address is located.[4]

Threats to the DNS

The DNS is an elegant system that enables the reliable, real-time routing of millions of addresses to millions of computers worldwide. Regretfully, DNS was not

[4] Microsoft TechNet, "How DNS query works," http://technet.microsoft.com/en-us/library/cc775637(WS.10).aspx (accessed August 26, 2009).

designed with security in mind. When the DNS was established, the Internet was a smaller place and many of the malicious techniques employed today had yet to be developed. However, it was not long until computer scientists began to recognize that the DNS was vulnerable and indeed work on addressing these vulnerabilities began as far back as 1993.[5]

Despite the severity of the vulnerabilities and the hard work of those involved in the early efforts to address them, it would be over a decade before an official catalog of the vulnerabilities was published. In the meantime, however, researchers in the field had begun work on a collection of security extensions that had been developed to address these vulnerabilities, calling the extensions DNSSEC. By August 2004, a Request for Comments entitled: "RFC 3833 Threat Analysis of the Domain Name System (DNS)" identified several different threats to the DNS which DNSSEC sought to resolve including such categories as "packet inspection", "ID guessing and query prediction", "name chaining", "betrayal by trusted server", "authenticated denial of domain names", and "wildcards."[6] Subsequent investigations have discovered additional vulnerabilities, including one in 2008 that was deemed so critical that it spurred an unprecedented

[5] D. Atkins and R. Austein, "Request for Comments: 3833: Threat Analysis of the Domain Name System," http://www.ietf.org/rfc/rfc3833.txt, (accessed August 26, 2009), 1.

[6] Ibid., 2-7.

gathering of DNS experts from around the globe to develop a solution before the vulnerability was discovered by hackers.[7]

The technical details of these and other vulnerabilities within the DNS are beyond the scope of this paper; instead it is sufficient to note that the core threats to DNS come from attacks that have the ability to corrupt the operation of DNS such that the requesting computer is given an incorrect response that directs the computer to an alternate address. Since so many services on the Internet employs DNS in one way or another, the consequences of corrupting DNS can be far-reaching. For instance, a successful attack could result in the example which opened this chapter: a user accessing a webpage based on a response from a DNS name server that has been corrupted to provide an incorrect response. Other possibilities range from preventing delivery of email to its intended destination to rerouting electronic payments to steal account information. As a result, the core of DNSSEC revolves around ensuring that DNS responses can be trusted as authentic.

The Development of DNSSEC

One of the founding principles of the Internet (as well as one of its greatest strengths) is its emphasis on maintaining an interoperable network across the globe while allowing for autonomous administration of individual networks. While a certain amount of uniformity across networks is needed to ensure that they are able to be interconnected,

[7] Joshua Davis, "Secret Geek A-Team Hacks Back, Defense Worldwide Web," *Wired*, December 2009.

the underlying principle of individual network autonomy remains strong. The need to balance interconnection with autonomy contributes to the international aspects of Internet governance, and presented a complicating requirement for the development of DNSSEC.

Functionally, this requirement necessitated that the solution offered by DNSSEC needed to be either compatible with existing software and hardware operated by the countless numbers of name servers and network administrators across the globe, or built as an optional added layer of protection on top of the existing DNS structure.[8] Otherwise, the implementation of DNSSEC risked destabilizing the interconnection of regional networks and, in the worst case scenario, spawning the creation of several separate networks that would be disconnected from the rest and unable to communicate with each other. Such a situation would create demarcation lines across the Internet where traffic could no longer be transferred, potentially shutting off access to entire domains. One need only imagine being unable to access all of the sites in the .com, .net, or other popular domains in order to recognize that such a situation would undermine the entire functionality of the Internet.

A further complication was presented by the need for seamless, uninterrupted transition to DNSSEC-capable systems.[9] Most of us, whether at work or at home, have encountered a time when our access to the Internet was unavailable; such times are at

[8] The Internet Corporation for Assigned Names and Numbers, *ICANN Proposal to DNSSEC-Sign the Root Zone*, http://www.ntia.doc.gov/DNS/ICANNDNSSECProposal.pdf (accessed August 26,2009), 2.

[9] Ibid., 4.

best inconvenient and at worst disastrous. Business networks in the present day account for this when performing regular maintenance or upgrades to their networks during off-hours or over the weekend in order to minimize this disruption. Regretfully, this approach, though suitable for smaller networks, was not deemed scalable to the larger construct of the Internet. The sheer amount of data and critical functions that rely upon always-active Internet access make such a task infeasible. Orchestrating a global shutdown of the Internet, even for the adoption of something as critical as DNSSEC, simply wasn't as option (after all, the off-hours on one side of the planet coincide with normal business hours on the opposite side). As such, DNSSEC had to be designed to be implemented with minimal interruption to Internet services.

The combination of the necessity to maintain existing DNS services and its continuous operation complicated the development of DNSSEC and prevented several possible solutions. Specifically, one early solution proposed that was invalidated by these factors was the encryption of the DNS traffic itself. Encryption of the DNS traffic would have solved the problem of DNS's vulnerability to tampering, but would have raised a whole host of other problems regarding the interoperability and open access of the Internet. Specifically, the introduction of encryption would have presented technical barriers that would necessitate that each of the name servers around the globe would need to be upgraded to be able to process the encrypted information. Such upgrades could be costly and time consuming and networks that, whether by choice or lack of funding, did not perform the upgrades could be cut off from the DNS. As a result, DNSSEC designers

would eventually adopt an alternative route to securing the DNS through the use of a technique known as public key cryptography.

Public Key Cryptography and DNSSEC

Public key cryptography is a means of encrypting a message in such a way that the recipient can verify that the message actually came from the sender and has not been tampered with in any way. Public key cryptography in the digital age involves the use of two electronic keys: a private key and a public key. Messages are encrypted by the sender with a private key that is kept secret and known only to the sender. Messages encrypted by a private key can then only be decrypted by the public key. Though the keys are mathematically related, they are generated in such a manner that it is extremely difficult to construct the private key using the public key.[10]

Public key cryptography ensures that a message can be trusted to come from the entity imagined, yet a key component that must be addressed is how to ensure that the public key can be trusted. This issue is resolved through the use of what is known as an authentication chain (also referred to as a chain of trust). Essentially, an authentication chain is a connection of trusted actors that ultimately leads to a final authority. While each of the actors involved in the chain may not interact directly with the others, each step occurs between two trusted actors who can attest to the validity of a public key. A physical analogue would be an instance in which I may give a trusted associate my public

[10] Geoff Huston, "DNSSEC – The Theory," *Internet Society*, August 2006, under "The ISP Column," http://isoc.org/wp/ispcolumn/?cat=44 (accessed August 26, 2009).

key, who in turn may distribute my public key to his trusted associates with whom I have no direct contact. Despite the lack of contact, because they trust my friend and my friend trusts me, each party can be assured that my public key is genuine.

With regard to DNSSEC, public key cryptography and the related authentication chain build upon the architecture of DNS itself. As described earlier, the DNS is set up hierarchically, with the root at the highest point, followed by several top-level domains, beneath which reside a series of subdomains. DNSSEC outlines an authentication chain that begins at the root and eventually flows all the way down to the subdomain through a chain of verification of public and private keys.

With a fully deployed DNSSEC, when someone typed in “www.mybank.com” into their web browser, their request would travel through the DNS to determine the IP address of “www.mybank.com”. At each stage of the request (locating the .com domain, locating the mybank subdomain) the public keys of the entities would be verified. As such, the root would verify that the “.com” TLD was valid, followed by the .com TLD verifying that the “mybank.com” subdomain was valid. With this example our authentication chain stops here, however, the process would continue in a similar manner for further subdomains, with the hierarchical authentication chain extended as far as needed. Even a cursory examination of this system reveals that a crucial component to deploying DNSSEC, enabling the authentication chain, and providing security and reliability to the DNS relies upon the participation of the root zone as the top of the authentication chain. As discussed earlier, this authentication process (known as

"signing") does not encrypt the DNS responses themselves, but rather employs public key cryptography to verify the reliability of the answers.

International Political Factors in the Signing of the Root Zone

The signing of the root zone has posed one of the greatest obstacles to the widespread adoption of DNSSEC and a factor that raises many international political and cybersecurity issues. The signing of the root zone involves a tangled web of international considerations, most related to the entity or entities that would be charged with generation, possession, and distribution of the public and private keys used in the root zone signature process. Because DNSSEC establishes the root zone as the final authority in the authentication chain, the control of the keys and the key generation process theoretically represents a level of control of the Internet itself. While the degree of this control can be questioned, there can be no doubt that it is a powerful factor both technically and politically given the reliance that countries around the world have on the Internet.

Fully understanding the implications of this control necessitates a greater understanding of how the root zone is managed under the existing framework, specifically in relation to the involvement of one organization in particular, the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN sits at the center of international controversy in large part due to its current arrangement with the United States Department of Commerce's National Telecommunications and Information

Administration (NTIA) and the private, United States-based Internet services company VeriSign. The management of the root zone by these three entities has generated considerable discontent amongst many international participants (both governmental and non-governmental) and has been a direct factor in the delay of signing the root and widespread deployment of DNSSEC.

ICANN

By July 1997 the Internet had expanded globally and a growing number of nations and international actors became involved in its operations as more regional networks connected. With the addition of these international elements, pressure to involve the international community in more of the management and governance of the Internet itself began to build. As much of the early development of the Internet had originated in the United States, many of the key elements of the continued maintenance and management of the Internet and related functions were performed by various organizations linked to or directly within the United States government. In an attempt to defuse much of this growing international pressure, President Bill Clinton directed the Secretary of Commerce to take steps to privatize the management of one of the most high profile of these elements: the DNS.[11] As a result, ICANN was established in 1998 as a not-for-profit public benefit corporation within the State of California. Under its agreement with the Department of Commerce's NTIA, ICANN would carry out several functions,

[11] U.S. Department of Commerce, "Memorandum of Understanding Between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers," November 25, 1998, http://www.ntia.doc.gov/ntiahome/domainname/icann-memorandum.htm (accessed August 26, 2009).

including the allocation of IP addresses, operation of the root zone server system, addition of new top level domains, and other coordination-related duties.[12]

The creation of ICANN represented an experiment in early Internet governance in that by granting a private organization the responsibility for such integral components of Internet operations, the United States was sending a deliberate message that Internet governance should be a "bottom-up" approach that limited the power of governments to influence the operation of the Internet. This message was reinforced by the fact that the International Telecommunication Union, an agency of the United Nations charged with responsibility for international communications, was never seriously considered for the role despite (or perhaps because of) the level of international government involvement in the group.[13] Instead, international involvement in the DNS would come from international private sector entities as established by the bylaws and organizational structure of ICANN. As a result, ICANN's bylaws included provisions for reconsideration of decisions, independent review of ICANN actions, periodic reviews of the structure of the organization itself, and a Board of Directors comprised of fifteen voting members of which no more than five may come from any one geographic

[12] Ibid.

[13] Geoff Huston, "Opinion, ICANN, the ITU, WSIS, and Internet Governance" *The Internet Protocol Journal* 8, no. 1 (March 2005), http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_8-1/internet_governance.html (accessed August 26, 2009).

region.[14]

Though the United States clearly wished to avoid undue government influence over the operation of the Internet, such wishes did not apply to *all* governments as evidenced by the fact that ICANN performed its functions, as it does to this day, under explicit agreement and contract with the U.S. government through the NTIA. Most relevant to the deployment of DNSSEC, ICANN is under contract with NTIA to perform the collection of functions known as the Internet Assigned Numbers Authority. Through this contract, when a TLD requests changes to the root zone ICANN must validate those changes and before the update can go live the NTIA must authorize the request. As such, while the responsibility for the DNS lies with ICANN, the NTIA (and hence, the United States government) must approve any and all changes to the system.

A final area of controversy surrounding ICANN and the management of the root zone involved the U.S.-based company VeriSign. Once a root zone update has been authorized by the NTIA, the update is distributed out to the broader Internet community through VeriSign.[15] That this function is handled by an U.S.-based company alone is enough to raise the eyebrows of many international observers, yet the issue is further complicated by the fact that VeriSign also operates the most popular TLD, .com. Many international and domestic elements view VeriSign's dual role in the management of the

[14] Internet Corporation for Assigned Names and Numbers, "Bylaws for Internet Corporation for Assigned Names and Numbers," http://www.icann.org/en/general/bylaws.htm (accessed August 26, 2009).

[15] Technically the update is transmitted to a group of high-level servers known as root servers prior to widespread distribution. For a detailed explanation of this structure consult the DNS Root Name Server FAQ provided by the Internet Society webpage at: http://www.isoc.org/briefings/020/.

root and their operation of the .com domain as posing a conflict of interest. Furthermore, many feel that VeriSign, as another U.S. entity at the center of root zone management, serves as proof that the United States maintains an unfair level of control over the Internet upon which all other countries depend.

DNSSEC at the Root Zone: A Call for Comments

The combination of VeriSign's business interests, NTIA's authorization role, and ICANN's structure and history lead many international observers to conclude that despite rhetoric to the contrary, the United States remains committed to control of the Internet. Furthermore, the role of these three organizations in the governance and management of the root zone has been a direct factor in the controversy and delay of signing the root and prolonging the existence of vulnerabilities to the DNS, contributing to the fact that it would be more than 15 years after the initial development of DNSSEC by the time the NTIA sought public comment on DNSSEC.

On October 9, 2008, the NTIA issued a press release calling for public comments on the deployment of DNSSEC, including deployment at the root zone. According to the press release, the NTIA was "committed to preserving the security and stability of the DNS" and that the organization deemed it "critical that [NTIA] get feedback from all

interested stakeholders."[16]

In addition to the request for general comments, NTIA released six potential proposals for deploying DNSSEC at the root and asked commenters to provide feedback on the proposals. The main differences between the six proposals had to do with the entities that would generate the public and private keys, distribute the public keys to the larger Internet community, and sign the root zone. The proposals for key generation and distribution included several options, with four of the six creating a new organization known as the Root Key Operator (including one of the four which made the Root Key Operator a shared duty of two or more operators), one proposal which assigned the responsibilities to ICANN through their existing IANA functions, and a final proposal which assigned the responsibilities to the Root Zone Maintainer (i.e. VeriSign). Each proposal maintained the authorization role of NTIA, while all of the proposals (with the exception of proposal 4 which assigned the responsibility to ICANN) assigned the signature of the root zone to the Root Zone Maintainer. Finally, NTIA also submitted two additional proposals it had received from ICANN and VeriSign for the deployment of DNSSEC at the root.

ICANN's proposal, predictably, recommended that the key management and signature functions be assigned to ICANN. The proposal cited ICANN's history of work

[16] U.S. Department of Commerce National Telecommunications and Information Administration, "Press Release: NTIA Seeks Public Comments for the Deployment of Security Technology Within the Internet Domain Name System," October 9, 2008, http://www.ntia.doc.gov/press/2008/DNSSEC_081009.html (accessed August 26, 2009).

with the management of the root zone, partnership with the U.S. Government, commitment to transparency, and status as a trusted actor amongst the international community as the primary reasons why it should be charged with the functions.[17] The ICANN submission, functionally identical to proposal 4 in the NTIA release, maintained the current arrangement with NTIA and VeriSign as the authorizer and distributor, respectively.[18]

In contrast, VeriSign's proposal hinged upon splitting the key generation functions among multiple organizations. VeriSign's proposal argued that by granting key generation function to multiple organizations it helped to address many of the concerns that actors (both international and domestic) have with control over this function, the implication being that granting ICANN's responsibility would merely perpetuate distrust and lack of transparency.[19] VeriSign's proposal, however, did not eliminate or in any way reduce its role in root zone management. Instead, coupled with the call for distributed key generation is a recommendation that "…certain key responsibilities would realistically need to be contracted by a third party. VeriSign has the necessary experience, facilities and processes and would be available to handle these responsibilities."[20] These "responsibilities" were such that VeriSign's proposal included the recommendation that

---

[17] The Internet Corporation for Assigned Names and Numbers, *ICANN Proposal to DNSSEC-Sign the Root Zone*, http://www.ntia.doc.gov/DNS/ICANNDNSSECProposal.pdf (accessed August 26,2009), 1.

[18] Ibid., 5.

[19] VeriSign, *Root Zone Signing Proposal*, September 22, 2008, http://www.ntia.doc.gov/DNS/VeriSignDNSSECProposal.pdf (accessed August 26, 2009), 1.

[20] Ibid., 2.

the actual key generation be held within a VeriSign facility in order to ensure proper security.[21] In fact, much of VeriSign's proposal hinged upon increased responsibility for VeriSign and frequently referenced work the company performed for their existing business operations as proof of their qualifications.

NTIA received fifty-six separate replies from a variety of individuals and organizations representing diverse business and international communities. The contents of their replies illustrate why the signing of the root generates such international political factors and why deployment of DNSSEC at the root has been so long delayed. With few exceptions, all of the comments strongly recommended that the root be signed and that DNSSEC provided the most appropriate choice at this time. Several comments noted that the lack of a signed root was a major contributor to the delay of DNSSEC implementation worldwide, and that signing the root should be considered a top priority. Additionally, several comments noted that while they recognized that the signature of the root was an issue with significant political considerations, the technical necessity was such that an interim solution (i.e. ICANN's proposal) should be put into place while the greater political battles over government involvement were fought. These comments illustrate that while DNSSEC and the signing of the root present significant international political issues, many members of the technical community feel that political negotiations have been an obstacle to the very necessary technical and operational requirements for improved cybersecurity.

---

[21] Ibid., 7.

None of the comments received wholeheartedly endorsed VeriSign's proposal for signing the root. Several comments expressed distrust of VeriSign, whom they viewed as possessing conflicting business interests and no international accountability. Specifically, those comments that directly addressed the VeriSign proposal expressed concerns that VeriSign sought to integrate itself into the root signing process to a degree that was not only inappropriate (given their status as a for-profit U.S. corporation), but would also put the company in such a position that replacing their role would be extremely difficult. However not all comments regarding VeriSign's proposal were negative; many comments agreed with a portion of the VeriSign proposal, specifically the concept of "key-splitting", which would divide the task of generating the keys used to sign the root among several different entities. Those in favor of key splitting felt that having one entity (whether VeriSign or ICANN) in control of the key generation function was inappropriate. In several cases key splitting was viewed as an appropriate way to break what was seen as United States domination of the process.

With regard to ICANN, the comments were generally in favor of the organization's proposal, though as mentioned above many were in favor of including the key splitting component of VeriSign's proposal. Overall, the comments approved of ICANN due to its legacy as a trusted actor that had consistently executed the IANA functions and contributed to the stability of the root. Several comments noted that due to the critical nature of DNSSEC and the necessity of deploying it at the root, the logistical and trust issues surrounding the development of an entirely new organization to execute

ICANN's function would further delay signing the root and should not be considered a near-term option.

One comment in particular is worth examining in detail; the comment was submitted by an anonymous individual who claimed no affiliation with any organization or country but mentioned that the comment was written from a "foreign, but not necessarily hostile, perspective." The comment essentially centered around the perspective that ICANN, VeriSign, the NTIA, and indeed even, strangely, the ITU would be inappropriate organizations for management of the root zone. The commenter noted that these organizations would further perpetuate United State's control of the root zone and did not address the realities of the international nature of the Internet. Instead, the comment called for "fully distributed ownership" that presumably involves representation from multiple nations, though the specifics of the alternate proposal are not entirely clear from the comment's content. While the comment itself lacks coherence in places and strikes this reader as overly vitriolic and reactionary, the criticisms it raises are points that need to be taken into consideration. Specifically, the comment gives voice to opinion that the management of the root zone is unfairly dominated by the United States, and that the current tripartite arrangement of NTIA, ICANN, and VeriSign is untenable for the long term. This desire for increased collaboration and involvement of international actors,

whether government or private companies, is a sentiment that is echoed in several other comments received.[22]

The Path Forward

ICANN issued a press release on June 3, 2009, announcing that it would work with NTIA, the National Institute of Standards and Technology, and VeriSign to sign the root zone "as early as feasible in 2009."[23] The release goes on to state that the necessity of DNSSEC is such that the organizations will develop an interim solution that will enable the signing of the root but does not impede the development of different long term proposals. Referencing the call for comments in October 2008, the release stated that "details of the process are still being worked", however, the interim process described in the release most closely approximates Proposal 2, with ICANN and VeriSign each managing portions of the signature process. As of August 2009, the root zone remained unsigned, with no additional announcements or information forthcoming from any of the involved parties. One assumes that negotiations and proposals for both the interim and long term solutions to signing the root have continued, but these discussions have clearly been held behind closed doors.

[22] Each of the comments received by NTIA can be found at their website hosted at: http://www.ntia.doc.gov/DNS/dnssec.html.

[23] Internet Corporation for Assigned Names and Numbers, "ICANN to Work with United States Government and VeriSign on Interim Solution to Core Internet Security Issue," June 3, 2009, http://icann.org/en/announcements/announcement-2-03jun09-en.htm (accessed August 26, 2009).

Conclusion

The vulnerabilities inherent in the DNS present a clear case for international involvement in cybersecurity, just as the trials and tribulations of DNSSEC deployment illustrate some of the challenges presented to any international cybersecurity efforts. Regretfully these challenges are not limited to efforts involving DNSSEC; such challenges can be found across the spectrum of cybersecurity issues. The next chapter examines another key example of a crucial cybersecurity issue that requires international efforts, yet presents its own similar challenges to those involved.

CHAPTER III

DISTRIBUTED ARMIES

Imagine that you turn on your computer one day to check your e-mail and upon opening your inbox discover several e-mails from friends and family responding to a message you don't recall sending. After examining the messages and checking your e-mail logs you discover that someone other than you sent out messages to your most frequently mailed contacts in your address book. The messages claimed that you were in financial trouble and requested money to be sent via wire transfer. Immediately recognizing that someone has hacked into your account, you change your password to your e-mail account. Subsequent investigation reveals that a program, running in the background on your computer, has been monitoring all of your web traffic and capturing every username and password you entered; periodically these logs were then uploaded to a web server. While you have antivirus software installed to prevent such events, once the program was surreptitiously installed on your computer it disabled your antivirus software as well as other security measures that may have alerted you to its presence.

The problem doesn't end there, however. After examining the logs of your recent Internet activity you discover that without your knowledge your computer has been engaged in a whole host of illicit activities over a period of weeks, including sending out thousands of unsolicited e-mail messages, hosting webpages that attempt to install similar monitoring programs on the computers of those who view the webpage, and bombarding

websites with repeated traffic. All of these activities were directed by an unknown individual who operated behind byzantine layers of complexity and security. Finally, you realize that your computer has not been alone in these efforts; your machine was one of hundreds, thousands, or even millions of other machines that were part of a new breed of threat to cybersecurity and the Internet, the "botnet."

While the thought of one's computer being a member of such a digital "army" may seem like science fiction, these shadow networks of infected computers known as botnets are very real and present a growing problem on the Internet. Botnets have the potential to unleash substantial destructive and disruptive power while maintaining a high degree of anonymity for those running them. Each of the activities described in the previous paragraphs happen to countless computers on a daily basis, all without the knowledge of the computer owner. Beyond the threat to the individual computer user, botnets can also be directly tied to several key issues of concern for international cybersecurity efforts. As such, their existence and the nature of the challenges they present offers an excellent example of how effective cybersecurity both requires and benefits the international community.

The Anatomy of a Botnet

Botnets offer a fascinating glimpse of how the surge of power and productivity created by the Internet has also created opportunities for the world's criminal minds. Exploring the impact botnets have on cybersecurity and the Internet illustrates how basic

aspects of network communication and everyday activity on the Internet have been leveraged to create the equivalent of a geographically-dispersed supercomputer. Yet in order to truly understand the botnet phenomenon we must first understand how they are developed and organized.

Botnets begin with specialized software that enables the botnet owner (also referred to as a "controller") to remotely control the infected computers (known as "bots"). This specialized software can take many forms including commercially available software known as a remote administration tool (RAT), specially designed programs written by the controller, or through the use of other software that can employ legitimate programs such as Internet Relay Chat (IRC) to issue and receive commands.[1] While the specially designed programs are created with malicious intent, many legitimate networks employ RATs to manage the activity and security of their networks, and millions of Internet users around the world employ IRC to communicate and exchange files. Regardless of which particular method is used, the ultimate goal is to enable the controller to direct the actions of the infected computer as if they were logged in as the administrator (a powerful user account that enables manipulation of a wide range of settings and programs).

Obtaining the proper software is only the first step in constructing a botnet. Next the controller must establish one or more computer servers necessary for the actual

[1] Moheeb Abu Rajab, Jay Zarfoss, Fabian Monrose, and Andreas Terzis, "A Multifaceted Approach to Understanding the Botnet Phenomenon," in *Internet Measurement Conference: Proceedings of the 6th ACM SIGCOMM conference on Internet measurement* (New York: ACM, 2006), 41.

operation of the botnet. These servers will enable the controller to issue commands through the channels identified above (RATs, specialized programs, IRC) or even over other well established protocols employed on the Internet.[2] Because these servers will enable the controller to manage and instruct the bots, they are often referred to as "command and control" servers.[3] Depending on the eventual size of the botnet and the security precautions of the controller, the command and control server or servers may exist on a single machine or several different machines. Furthermore, command and control servers are generally organized in such a way that they have a low public profile and cannot be easily discovered by any subsequent investigations that botnet activities may provoke. Some botnets employ designated servers that are built and designed for the specific purpose of issuing commands. However, such a setup can make it easier to connect the trail of traffic back to the botnet controller. As such, many controllers choose to use a public server or, increasingly, many botnet controllers postpone this step and employ a server hosted by one of the bots instead.[4]

The most recognizable components of a botnet are, of course, the bots themselves. Botnets have an extremely large range of size, but the general method of recruiting the bots is similar. Recruiting the bots is a matter of installing the software referenced earlier onto the target computers. Historically, installing such software may have been

[2] Ibid..,42.

[3] Evan Cooke, Farnam Jahanian, and Danny McPherson, "The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets," in *Proceedings of the Steps to Reducing Unwanted Traffic on the Internet Workshop* (Berkeley, CA: USENIX Association, 2005).

[4] Ibid.

accomplished through covert physical installation of the program through a CD, USB drive, or other removable media that has been loaded with the software. Direct physical installation comes with a variety of obvious problems, however, most notably the difficulty of gaining access to the computer and an increased chance of discovery. Instead, modern botnet controllers install the software remotely via security vulnerabilities present on the target computers. These vulnerabilities may stem from unpatched software programs, improperly configured operating systems, malicious websites, viruses, or a one of many other sources. The software is generally installed via the computer user visiting a website designed to exploit these vulnerabilities or through opening an infected file attached to an e-mail.[5] Often, the targeted users fall victim to social engineering or "phishing" attacks, wherein an e-mail has been crafted to appear to be from a legitimate source yet directs the user to download a file or visit a website that subsequently infects their computer.[6]

Once infected, the bot sends a series of communications to download appropriate instructions and any additional software that the controller requires to accomplish his goals. From here, the computer may take on a variety of roles depending upon the nature of the botnet. Some infected computers may be designated as "workers", i.e. bots that will actively execute the commands given by the controller. Other bots may be

[5] Organisation for Economic Co-Operation and Development, *Computer Viruses and Other Malicious Software: A Threat to the Internet Economy* (OECD Publishing, 2009), 23.

[6] Ibid., 23-24.

designated “proxy bots”, acting as a relay station between the command and control servers and the worker bots.[7] This arrangement of proxy bots and worker bots not only adds an additional layer of security should one attempt to connect the trail of bots, but also reduces the workload on the command and control servers, a factor which becomes key as the botnet grows in size.

What Makes Botnets a Threat?

While there are many variations on how to specifically organize a botnet, ultimately all consist of a network of bots under the command of the botnet controller who can issue commands with a reasonable degree of anonymity. Given such a structure, the next obvious question is “what can be done with it, and why should national governments be concerned?” As the below sections will illustrate, nations should be concerned about botnets because of their capability to engage in a range of behavior that, while not unique to botnets, is exponentially more destructive and disruptive than individual actions in large part due to the considerable computing power of a botnet.

Malware Distribution

One of the primary threats posed by botnets is their distribution of “malware”, which includes any of a wide variety of malicious computer programming designed to infiltrate, subvert, or disrupt computers or their services. Malware is a broad term that

[7] Chris Kanich, Christian Kreibich, Kirill Levchenko, Brandon Enright, Geoffrey M. Voelker, Vern Paxson, and Stefan Savage, “Spamalytics: An Empirical Analysis of Spam Marketing Conversion,” in *Conference on Computer and Communications Security: Proceedings of the 15th ACM Conference on Computer and Communications Security* (New York: ACM, 2008).

includes any number of insidious programs including viruses, worms, "keyloggers", "Trojan Horses", and others. Because the term malware is so broad, the results of the distribution vary depending upon the specific type involved. Malware may be designed to physically disable or disrupt computers, collect sensitive information, clog Internet bandwidth with relentless traffic, send unsolicited e-mail, recruit additional bots, or any number of other activities selected by the malware author.[8] Some of the most egregious and prevalent malware activities are explored in further detail below, yet countless varieties exist and new malware designed to exploit and subvert computer systems is released daily.

Botnets are not the sole distributors of malware; viruses, worms, and other such malicious programs have been around since the early days of the Internet. The key difference between more traditional methods of malware distribution and the rise of malware distributed by botnets is volume. Whereas previously malware distribution was limited primarily by the availability of resources (a single computer is only capable of distributing as much malware as it has system resources to do so), the rise of botnets have enabled malware developers to exponentially increase their distribution capability. Each bot computer added to a botnet adds its computing power, as well as its bandwidth capability, to the power of the botnet as a whole. In turn, not only can the additional bot be used for other malicious activities, but they can also immediately begin the

[8] Nicholas Weaver, Vern Paxson, Stuart Stanifold, and Robert Cunningham, "A Taxonomy of Computer Worms," in *Workshop on Rapid Malcode: Proceedings of the 2003 ACM Workshop on Rapid Malcode* (New York: ACM, 2003), 14-16.

distribution of malware to recruit additional members, creating a continuous chain of bot additions.

The large scale distribution of malware should concern nations for economic reasons as well. Beyond its use in recruiting bots for botnets and the threats posed by such botnets (as subsequent sections will illustrate), malware is also responsible for considerable financial costs. In 2009 the Organization for Economic Co-Operation and Development (OECD) found that while the financial figures were difficult to collect and inconsistent in measurement, several surveys indicated dramatic costs. Included among OECD's analysis was £33.5 million incurred for a member organizations of a British banking association. On a larger scale, OECD also referenced a survey of 52 information technology officials who estimated a cost of €9.3 billion directly attributed to malware in 2006.[9] The impact was not limited to Europe either, as the same study cited an estimate by the U.S. Government Accountability Office of $67.2 billion incurred by U.S. businesses in 2007.[10]

Spam

Everyone knows the special pleasure of receiving junk mail in their mailbox at home. Unsolicited mail typically involves advertisements for services and businesses that you never knew existed or at the very least deemed irrelevant to your interests. In the

[9] Organisation for Economic Co-Operation and Development, *Computer Viruses and Other Malicious Software*, 68.

[10] Ibid., 69.

same manner, the Internet and the rise of e-mail as a primary means of communication have given rise to junk e-mail, collectively known as “spam”, which clogs up virtual mailboxes just as readily as their physical counterparts. While most users may regard spam as merely an annoyance, spam carries a potential for harm that defies its seemingly benign appearance. Botnets, with their host of infected computers, have exponentially increased the amount of spam that can be distributed on a daily basis. Through a variety of technical means that need not be elaborated for the purposes of this paper, large botnets can distribute astronomical amount of spam over a very short period of time. As recently as July 2009 one of the largest active botnets sent more than 10 billion spam messages in a single day.[11]

The distribution of spam may stem from a variety of motivations, monetary gain being one of the most prevalent. One of the most innocuous methods of generating money from spam involves e-mails which direct users to webpages that have been configured to have little content but a wealth of ads. As advertising revenue on the Internet is often based upon unique “page views” (meaning that the owner of a website is paid a small sum for every unique IP address that visits the webpage hosting the ad), each of the spam recipients represents a potential page view and thus a potential source of revenue.

[11] Symantec, “MessageLabs Intelligence: August 2009: Cutwail Damaged by ISP Shutdown Whilst Donbot Offers Medical Assistance to Billions,” http://www.messagelabs.com/mlireport/MLIReport_2009.08_Aug_FINAL.pdf (accessed September 14, 2009), 3.

Another method of generating money from spam involves encouraging spam recipients to purchase a range of products. Spam messages such as these focus on directing recipients towards webpages where items (pharmaceutical products are common in recent trends, but any products could be substituted) can be purchased. In many of these cases there may even be legitimate businesses at the other end of the line selling the pharmaceutical or other products. McAfee, a leading antivirus and anti-spam vendor, recently conducted an investigation of these types of spam messages and discovered that the botnets used in the actual distribution of the spam were merely the final executor of a series of contracts and subcontracts that began with a legitimate corporation. The corporation contracted out services from various companies to drive traffic to their site, and through ignorance, willful ignorance, or indifference the corporations ended up employing illegal botnets to increase traffic to the site via the distribution of millions of spam messages over several months.[12]

While the cybersecurity implications of such spam are relatively minor, the level of network congestion it can create, particularly when botnets are involved, presents an issue of concern. In August 2009, Symantec (a leading antivirus and anti-spam technology developer) noted that spam accounted for 88.5% of all e-mail sent across the globe; put in other terms, spam constituted 1 out of every 1.13 emails.[13] Additionally, in

[12] McAfee, "September 2009 Spam Report," www.mcafee.com/us/local_content/reports/7056rpt_spam_0909.pdf (accessed September 14, 2009), 5-6.

[13] Symantec, "MessageLabs Intelligence," 8.

September 2009 McAfee noted that pharmaceutical spam alone constituted "between 60 percent and 65 percent of today's global email volume."[14]

ISPs, e-mail hosting providers, and administrators across the world that are responsible for the timely flow of information across their networks are understandably impacted by such an incredible rate of traffic generated by these unwanted messages. Botnets contribute to this congestion through drastically increasing the number of messages that may be sent. Prior to the rise of botnets, spam was generally sent via dedicated machines using e-mails obtained through automated programs searching the web for publicly posted addresses (such as an e-mail address posted on a webpage), or a list of valid e-mail addresses purchased or obtained through other means. As ISPs and mail server administrators became more concerned about the problem of spam, this traditional method of spam distribution encountered diminishing returns as they found their IP addresses blacklisted, essentially preventing any e-mail message sent from their computer from reaching its intended destination. Botnets offered an attractive solution to the blacklisting problem primarily because fresh infected computers could be added at such a rate that blacklisting efforts could not keep pace.

Finally, not all spam is designed solely to generate money. Spam may also be employed as a means to distribute malware and recruit new bots for the botnet. Recruiting more bots not only fuels future spam activity, but also contributes to another threat posed by botnets: collection of sensitive information.

[14] McAfee, "September 2009 Spam Report," 3.

Information Mining and Identity Theft

Botnets can also be used to attain a wide range of information, which in turn can be leveraged for financial or other gains. Remember that each of the bots in a botnet represents a system that has been compromised. Depending upon the specific software or RAT employed, a botnet controller may be able to search through the files on the computer and upload them to a server for retrieval. The controller may also be able to monitor and log e-mail traffic, usernames and passwords, or any other information entered into the infected computer. Additionally, if the infected computer is located on a personal or business network a controller may be able to gain access to other computers or files located on that network, expanding their access to information even further.

Depending upon the nature of the infected computer, the botnet controller has access to a wide variety of information and opportunities. Similar to the example presented early in the previous chapter, if the compromised computer is a personal computer he could use his log of usernames and passwords to clean out the user's bank accounts. If his data collection activities turned up sensitive or proprietary information from a computer located on a corporate network, he may choose to ransom that information back to the company. Finally, and most relevant to national interests, if the infected computer is a government machine or located on a government network, the controller may have access to a wide range of sensitive or classified information that

could be used for political ends. Indeed, while official reports are understandably absent, there have been countless news reports of electronic espionage activities undertaken by nation states to obtain such sensitive information.[15] While one would expect that state-sponsored espionage activities may not grow to the mammoth proportions of some of the largest botnets, the same vulnerabilities and techniques used to build these larger botnets could be employed in a smaller, more targeted campaign focused on government networks.

Enhanced Computing Power

While the techniques described above can and have been employed without the use of a botnet, botnets enable these activities on a massive scale. Because botnets can consist of millions of infected computers the damage that the controller could cause outweighs the damage from similar attacks carried out by smaller groups. A report issued in April 2009 noted the discovery of a botnet with nearly 2 million infected computers, with indications that this may not even be the largest botnet on record.[16] This concentration of computing power makes botnets such a threat, a threat best illustrated by

[15] One need only conduct a simple Internet search to discover a wealth of articles on the subject. For specific examples, see "Cyberspies penetrate electrical grid: report" (Reuters: http://www.reuters.com/article/topNews/idUSTRE53729120090408), "Cyber-spies tracking terror on Web" (CNN: http://www.cnn.com/2007/TECH/05/29/internet.spying/), or "Chinese hackers using ghost network to control embassy computers" (TimesOnline: http://www.timesonline.co.uk/tol/news/uk/crime/article5996253.ece).

[16] Siobhan Chapman, "Massive 2 million PCs botnet uncovered," *Computerworld*, April 24, 2009, http://www.computerworld.com.au/article/300537/massive_2_million_pcs_botnet_uncovered?fp=4194304&fpid=1 (accessed September 15, 2009).

one of the most concerning capabilities of botnets: the Distributed Denial of Service attack, or DDOS.

Each time a user on the Internet visits a website, information must be exchanged between the computer and the server hosting the website (web server). Just as the previous chapter described the request and response mechanism for DNS, a computer and a web server must exchange information for the user to load the website. Images, text, and any other information present on the website must be transmitted to the requesting computer. Furthermore, because of the global nature of the Internet, the web server must handle requests coming in from all around the world simultaneously. Given that some of the most popular sites on the web may serve millions of requests per day, such a task demands capable and reliable equipment.

Despite incredible advances in web server technology, even the most advanced web servers can only handle a finite amount of traffic before their response rates begin to be affected. A web server under a heavy load may find its responses to be significantly slower than average while it accommodates the huge queue of pending requests. Eventually the web server may encounter such tremendous traffic that it cannot handle all of the requests and simply shuts down, incapable of responding to any requests at all. Examples of such behavior happen all the time during the normal course of business on the Internet, even with the most reliable and powerful of websites. In September 2009, Google, the premier search engine and e-mail provider, encountered such a problem when an oversight during routine maintenance resulted in one of their web servers

processing so much traffic that it failed, leading to a cascade of server failures that would eventually bring down their popular e-mail service for a period of hours.[17] The impact of such downtime, whether in lost revenue, functionality, or popular opinion (after all, if a company offers a service for a fee yet their web servers routinely fail customers will not be inclined to purchase their service) can be profound.

A Denial of Service (DOS) attack occurs when an attacker organizes such a incident which results in a disruption to the webpage or online service. The concept behind DOS attacks, namely preventing users from accessing a network resource, is one that has been known since the early 1980's.[18] With the rise of botnets, however, traditional DOS attacks have been augmented to employ multiple computers in geographically distinct locations. As a result, DOS attacks have largely given way to Distributed Denial of Service Attacks (DDOS). Furthermore, botnet capabilities are such that the controller can execute a DDOS attack at will and sustain it indefinitely, causing great difficulty for web server administrators attempting to revive their web servers and bring their websites back online.

DDOS attacks have increasingly been a problem since the 1990's, with several high-profile cases targeting not only commercial businesses, but governments as well. A Canadian hacker launched a series of attacks on major websites including Yahoo, eBay,

[17] Ben Treynor, "More on today's Gmail issue," posted on *The Official Gmail Blog*, September 1, 2009, http://gmailblog.blogspot.com/2009/09/more-on-todays-gmail-issue.html (accessed September 15, 2009)

[18] Georgios Loukas and Gülay Öke, "Protection Against Denial of Service Attacks: A Survey," *The Computer Journal Advance Access* (Oxford: Oxford University Press, 2009), 1.

Amazon, CNN, and others in February 2000. The hacker would eventually be sentenced for causing an estimated $1.7 billion in damages.[19] In 2007 several websites run by the government of Estonia came under a sustained DDOS attack that lasted weeks following the removal of a statue commemorating Soviet soldiers killed in World War II.[20] The United States government was attacked on July 4, 2009 in a DDOS that brought down the websites of several government agencies including the Secret Service, Department of Treasury, Federal Trade Commission, and the Department of Transportation.[21] These and other examples are widespread in the media, however the full extent of DDOS attacks may be greater than initially suspected as security researchers suspect that many threatened or actual attacks may never be reported because of the potential damage to victims' reputation.[22]

Botnets for Hire

Finally, the threat of DDOS attacks from botnets is enhanced through the actions of enterprising botnet controllers leasing out their botnets to those willing to pay for their capabilities. Cyber criminals, hackers, and even disgruntled rivals or corporate competitors can now pay controllers to conduct spam, DDOS, or malware distribution

[19] Ibid., 3.

[20] Jeremy Kirk "Estonia recovers from massive DDoS attack," *Computer World*, May 17, 2007 http://www.computerworld.com/s/article/9019725/Estonia_recovers_from_massive_DDoS_attack (accessed September 14, 2009).

[21] Lolita C. Baldor, "Federal Web sites knocked out by cyber attack," *Associated Press*, July 7, 2009.

[22] Loukas and Öke, "Protection Against Denial of Service Attacks," 4.

campaigns on their behalf. This digital arms trade effectively removes the technical barrier to operating a botnet and offers another reason why botnets and the threats they pose warrant international attention.

Challenges to International Efforts

Given the extent of the threat posed by botnets, it should come as no surprise that individuals, organizations, and nations concerned about cybersecurity increasingly recognize the importance of taking steps to address them. Indeed, as the next chapter will illustrate, there are several different international efforts and agreements that have been established or are ongoing that address components of the botnet threat. However, botnets present several challenges to international efforts to combat them, stemming from difficulties in volume, prevention, attribution, and the complexities of international law enforcement.

Volume

Part of the challenge of addressing botnets comes from the fact that the malware used to propagate them evolves on a daily basis. While there is an entire industry devoted to developing antivirus software and other malware countermeasures, there is also a very devoted hacker and cyber criminal community devoted to improving malware's ability to bypass those countermeasures. One vendor noted that despite having 50 engineers working fulltime on malware analysis and prevention, the rate of 200 new malware

samples per day was simply overwhelming.[23] Compounding this evolution rate is the wide variety of software and operating systems that must be tested against, as the multiple versions of software and hardware employed on the Internet often prevents universal fixes. Finally, while there are exceptions, malware protection vendors typically issue updates only after vulnerabilities have already been discovered and exploited, rather than patching new vulnerabilities before malware developers discover them. The end result is that protection against malware becomes a very reactive, rather than proactive, endeavor where defense techniques constantly try to keep up with advances in offense.

Prevention

The vulnerabilities that allow controllers to infect computer systems may stem from a variety of reasons, but one of the most prolific is due to unpatched software or operating systems. While software vendors routinely issue updates to patch identified vulnerabilities these patches may only arrive after malware exploiting it is loose on the Internet. Alternately, patches may not be applied by the end users; they may not fully appreciate the need to apply such patches, instead viewing the patches and the associated reminders to install the patches as a nuisance. Furthermore, many software vendors are hesitant to offer patches to people whom they know did not purchase the software legally, presenting additional complications to addressing vulnerable computer systems. While leaving these systems unpatched and vulnerable to infection may offer a certain form of

[23] Organisation for Economic Co-Operation and Development, *Computer Viruses and Other Malicious Software*, 75.

justice, it also contributes to the pool of potential bots, as users are unlikely to stop using their systems despite the lack of security.

As referenced above, while antivirus software exists to help prevent malware from infecting a system, most antivirus software is only capable of stopping malware once it has been identified and a preventative measure is developed. This reactive approach means that new malware often has a significant period of time during which to operate before antivirus and other software products will prevent it from taking hold. A recent report by a cybersecurity firm noted that of the "hundreds to thousands" of new malware attacks it discovers on a daily basis, the average detection rates of thirteen leading antivirus programs over the period of a month ranged from 16% to only 44% detection rates.[24] The number of vulnerable systems created by these conditions ensures that botnet controllers always have a wealth of potential bots to recruit.

Unfortunately, the problem of vulnerable systems is not one that can be easily solved and may be beyond even the most committed efforts. Requiring software to maintain up-to-date patches to retain functionality seems untenable, as it minimizes the sense of ownership and would also cause the program to stop functioning should the user be unable to obtain the patch, a prospect unpalatable to vendors and consumers alike. Furthermore, such a policy would not deal with the key issue of piracy, as many pirated software products contain modifications designed to bypass such security features. New

[24] Cyveillance, "Cyber Intelligence Report: A Cyveillance Report, August 2009," www.cyveillance.com/web/docs/WP_CyberIntel_H1_2009.pdf (accessed September 14, 2009), 3.

technology and advances offer hopes for improved malware detection, prediction, and protection efforts, but even these have not yet kept pace with malware's evolution.

Attribution

If prevention offers significant challenges, response does not make for an easier task, as botnets present complicated and difficult problems with regard to the attribution of activity. If the botnet has been set up with advanced security precautions, the botnet controller can be reasonably assured of his anonymity for several reasons. One of the reasons involves the use of a multi-layered botnet architecture described in the previous sections. By creating multiple layers between the controller and the bots through the use of control servers and proxy servers, the controller ensures that any investigators seeking to get to the root of the botnet will have a very complicated web to untangle. Contributing to this problem is a phenomenon known as "spoofing", wherein the botnet operator disguises the IP addresses of the bots and servers. Spoofing is accomplished through exploiting the underlying protocols of the Internet to create the appearance that e-mail and other Internet traffic originated from an alternate source. As such, botnet investigators seeking to discover the source of a spam e-mail message not only have to deal with the complex layers of control servers, proxy servers, and worker bots, but must also deal with spoofing attempts to disguise the originator of the e-mail and other traffic, potentially at several different steps in the process. While there are methods for

determining the true originating address of the traffic, the investigation and necessary steps further complicate an already complex problem.[25]

Spoofing leads to other problems as well when it comes to active response to botnet activity. One of the most obvious ways to stop botnet activity is to block traffic emanating from the bots. Blocking traffic can be accomplished in a variety of ways, yet the most common is a technique where individual or entire ranges of IP addresses are put on a list or "blacklist." Subsequently, ISPs block all traffic from the addresses located on these lists, rendering the bots incapable of sending additional spam or conducting DDOS attacks. If the IP addresses of the bots are properly spoofed, however, ISPs run the risk of blocking legitimate IP addresses through the blacklist. Additionally, because botnets can often switch their IP addresses very quickly, ISPs may choose to blacklist an entire range rather than individual addresses, which heightens the risk that valid IP addresses not engaged in botnet activity may be affected.

Law enforcement

Finally, perhaps the greatest challenge to international efforts to combat botnets has to do with the inherent complexity of prosecuting international cybercrime. Beyond the difficulties in attribution (a key part of any law enforcement action being proof that the accused committed an offense), there is the problem of where and how to prosecute the botnet controller. Botnet controllers may exploit the gaps in international law by

[25] Farha Ali, "IP Spoofing," *The Internet Protocol Journal* 10 no. 4, http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-4/104_ip-spoofing.html (accessed September 15, 2009)

routing traffic to countries where laws for electronic crimes may not be sufficiently advanced (or sufficiently strict) to allow for prosecution. Even in countries where applicable laws are in place, prosecution may require cooperation between international law enforcement entities that may be unprepared to address the incident due to high cost, poor relationships between the countries, or simply the logistics of conducting an investigation dependent upon electronic records located on geographically distant computers.[26] Given the complexities of how a botnet operates it is virtually guaranteed that some or all of elements involved (including the controller, bots, proxy servers, malicious website, and target) in an attack will be located in different countries.

Conclusion

Botnets and the complex array of issues surrounding them present a clear case for international involvement in mitigation and prevention efforts. The distributed computing power at the hands of a botnet controller can range to well over a million computer systems which, when activated, can unleash network congesting spam, engage in information harvesting activities, or conduct debilitating DDOS campaigns. Unfortunately, the steps necessary to curb the botnet threat are not always apparent and the challenges to developing a long-term solution are many. The final chapter of this work catalogues many of the international efforts that are underway to address these and other critical cybersecurity issues and explores recommendations for the path forward.

[26] Grabosky, "The Global Cyber-Crime Problem," 52.

CHAPTER IV

TOWARD INTERNATIONAL CYBERSECURITY EFFORTS

The explosive growth of the Internet since the 1990's has spurred nations to recognize that while the Internet does create extraordinary potential for efficiency and new opportunity it also holds the potential for considerable risks. As global networks have become more interconnected and individuals and organizations around the world have come to rely upon the Internet for more and more of their daily activities, governments have become more concerned about cybersecurity. These concerns have motivated a variety of activities designed to address several political and technical aspects of cybersecurity. While many countries have engaged in a variety of activities within their own borders, increasingly several international and regional bodies have designated groups devoted to the critical issue of cybersecurity. Regretfully, there are also significant challenges to successful international cybersecurity efforts. Only with careful planning and preparation can nations make the most efficient use of their resources and ensure productive international efforts to secure cyberspace.

Current International Efforts

Just as the Internet and reliance upon cyberspace has become pervasive across the world, so too has the issue spread through the various international organizations and bodies across the globe. Cybersecurity by its very nature transcends national borders, and the growing recognition of this can be seen in many prominent international

organizations. A brief survey of these organizations yields a wealth of initiatives, working groups, and international agreements designed to address one or more facets of cybersecurity.

United Nations

As the most broadly representative international body, with 192 countries on its membership roster, the United Nations (UN) offers a forum for a wide variety of issues of international concern, including cybersecurity. The U.N.-affiliated group most involved in cybersecurity efforts is the International Telecommunication Union (ITU). The ITU was established in 1865 as the International Telegraph Union due to the growing need for a comprehensive framework for international interconnection of telegraph lines. The ITU evolved throughout the rest of the 19th and 20th centuries, changing its name to the International Telecommunication Union in 1934 as communications technology matured and the telegraph declined into obsolescence. Following World War II, the ITU became an agency of the United Nations, where it remains to this day; by 2009 ITU membership had grown to include 191 member states and more than 700 additional organizations.[1]

The ITU conducts a wide variety of cybersecurity activities, many of which gained significant impetus after the World Summit on the Information Society, a UN initiative which included "Building confidence and security in the use of ICTs

[1] International Telecommunication Union (ITU), "ITU History," http://www.itu.int/net/about/history.aspx (accessed October 1, 2009).

(Information and Communication Technologies)" among its principles.[2] Based on this principle, in 2007 the ITU launched the Global Cybersecurity Agenda (GCA) as an "international framework for cooperation and response focus[ing] on building partnership and collaboration between all relevant parties in the fight against cyber threats."[3] The GCA contains five separate "pillars", each of which addresses a discrete area of cybersecurity efforts, including Legal Measures, Technical and Procedural Measures, Organizational Structures, Capacity Building, and International Cooperation.

The Legal Measures pillar has developed two main products: the publication *Understanding Cybercrime: A Guide for Developing Countries* and the ITU Toolkit for Cybercrime Legislation. Both items are designed to assist countries in developing and implementing appropriate legislative measures to deal with cybercrime both on a national and international basis, and were developed by experts representing many different countries as well as policy and technical disciplines.[4]

The Technical and Procedural Measures pillar encompasses the work of the ITU Standardization Sector (ITU-T) and the ITU Radiocommunications Sector (ITU-R). ITU-T focuses on the development of international cybersecurity standards, while ITU-R

---

[2] International Telecommunication Union, "WSIS Declaration of Principles: Building the Information Society: a global challenge in the new Millenium," http://www.itu.int/wsis/docs/geneva/official/dop.html (accessed October 1, 2009).

[3] International Telecommunication Union, "GCA Brochure," http://www.itu.int/wsis/implementation/2009/forum/geneva/new-gca-brochure.pdf (accessed October 1, 2009) 4.

[4] Ibid.,14-16.

engages in activities designed to secure the radio-frequency spectrum. Additionally, Technical and Procedural Measures includes the "International Multilateral Partnership Against Cyber Threat (IMPACT) Global Response Centre (GRC)", a cyber threat resource center that can provide real-time warnings to ITU member states.[5]

The Organizational Structures pillar focuses on harmonizing the various national and regional structures devoted to cybersecurity in order to "facilitate communication, information exchange and the recognition of digital credentials across different jurisdiction."[6] Meanwhile, the Capacity Building pillar has produced several tools and initiatives designed to improve the implementation and deployment of cybersecurity capabilities, including a cybersecurity self-assessment tool and a cybersecurity outreach and awareness toolkit. Additionally, the ITU is developing a toolkit to assist developing countries to address the threat of botnets.[7]

Finally, the International Cooperation pillar involves several ongoing initiatives including an expert group charged with analyzing and continuing development of the GCA itself, an international public-private partnership devoted to addressing cyber threats, and a policy and international cooperation centre. The ITU also established a

[5] Ibid., 26.

[6] Ibid., 28.

[7] Ibid., 34.

"Cybersecurity Gateway" as a repository for national, regional, and international cybersecurity initiatives worldwide.[8]

Organisation of Economic Co-operation and Development

The Organisation for Economic Co-operation and Development (OECD) was established in 1961 to contribute to the overall economic growth and cooperation of its member nations, a list that presently includes thirty countries. The OECD provides a forum for governments to "compare policy experiences, seek answers to common problems, identify good practice and coordinate domestic and international policies."[9] Given the profound economic considerations involved in cybersecurity (or a lack thereof), it should come as little surprise that OECD has sponsored several initiatives and reports focused on the subject.

Most of OECD's cybersecurity efforts fall under the rubric of its Working Party on Information Security and Privacy (WPISP), an intergovernmental forum that addresses policy matters related to information security and privacy on an international and intercultural basis. The WPISP has several historical and ongoing initiatives designed to promote increased cybersecurity, including the issuance of the report "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security",

[8] International Telecommunication Union, "Cybersecurity Gateway Overview," http://www.cybersecurity-gateway.org/overview.html (accessed October 1, 2009).

[9] Organisation for Economic Co-operation and Development (OECD), "About OECD," http://www.oecd.org/pages/0,3417,en_36734052_36734103_1_1_1_1_1,00.html (accessed October 1, 2009).

conducting two surveys of national information security policies, sponsoring several international workshops including a partnership with Asia Pacific Economic Cooperation (APEC) on the topic of information systems and network security, and development of a report on identity theft.[10]

As referenced in the previous chapter, the OECD has recognized the growth of malware as a significant threat to the economic productivity of nations and has engaged in many activities devoted to the issue. OECD collaborated with APEC to host a joint workshop on malware in 2007 which brought together "government, industry, Computer Security Incident Response Teams (CSIRTs), civil society, consumers, and others who play a role in combating malware."[11] Additionally, in 2009 the OECD released a report on the economic consequences of malware that included suggestions for increased international cooperation to address the threat that malware poses to economic security. Finally, with regard to the malware-related issue of spam, the OECD sponsors an initiative which developed an anti-spam toolkit in 2007; however, the initiative may have lapsed as the website devoted to it has not been updated since that time.

[10] Organisation for Economic Co-operation and Development, "What is the Working Party on Information Security and Privacy (WPISP)," http://www.oecd.org/document/46/0,3343,en_2649_34255_36862382_1_1_1_1,00.html (accessed October 1, 2009).

[11] Organisation for Economic Co-operation and Development, "APEC-OECD Malware Workshop," http://www.oecd.org/document/34/0,3343,en_2649_34255_38293474_1_1_1_1,00.html (accessed October 1, 2009).

North Atlantic Treaty Organization

The North Atlantic Treaty Organization (NATO) was established in 1949 as a defense coalition involving countries in the North Atlantic area including Europe and North America. Throughout the Cold War NATO largely represented the forces of the capitalist Western Europe and North America against the communist forces of the Soviet Union. Though the Cold War has since ended, the organization remains a key mechanism for cooperation and development of the defense capabilities of its 28 member nations. Just as cyberspace has changed the landscape of the civilian sector, so too has it changed the landscape of defense. Recognizing this, NATO sustains several ongoing initiatives that address defense aspects of cybersecurity.

In 2002, NATO leaders directed the establishment of a technical Cyber Defense Programme to enhance the alliance's cyber defense posture and operating capability. By 2006, NATO leadership decided that additional work was needed to protect critical systems over the long term. Despite this commitment, the cyber attack on the government systems of Estonia in 2007 motivated the organization to reassess their efforts in cyber defense. The subsequent policy on cyber defense was approved in 2008 and is currently being implemented. One of the recent outcomes of the policy was the 2008 establishment of the Cooperative Cyber Defense Centre of Excellence in Tallinn, Estonia. The Centre is

charged with providing NATO with a wide variety of cyber products and services including research and development, training, analysis, and subject matter expertise.[12]

Finally, NATO continues to promote cyber defense as a key issue for the alliance, sponsoring numerous workshops, conferences, and seminars devoted to the issue. NATO co-sponsored a seminar in Armenia in 2008 that focused on developing a common understanding of cyber attacks as well as sharing best practices and opportunities for cooperation in preventing and responding to them.[13] Another NATO-sponsored workshop in February 2009 was designed to "rethink present strategies and identify urgent measures to be taken in order to minimize the strategic and economic impacts of cyber attacks."[14] Finally, NATO sponsored a recent conference at the Centre of Excellence in Estonia which invited prominent members of academia, government, business and the military to discuss cyber warfare including "theory and practice from both strategic and tactical perspectives."[15]

---

[12] North Atlantic Treaty Organization (NATO), "TRANSNET: Cooperative Cyber Defense (CCD) COE (Estonia)," https://transnet.act.nato.int/WISE/TNCC/CentresofE/CCD (accessed October 1, 2009).

[13]North Atlantic Treaty Organization (NATO), "Armenia hosts cyber defense seminar," http://www.nato.int/cps/en/natolive/news_50197.htm?selectedLocale=en (accessed October 1, 2009).

[14] North Atlantic Treaty Organization (NATO), "SPS workshop rethinks approaches to cyber security," http://www.nato.int/cps/en/natolive/news_50624.htm?selectedLocale=en (accessed October 1, 2009).

[15] North Atlantic Treaty Organization (NATO), "Cyber warfare conference," http://www.nato.int/cps/en/natolive/news_55801.htm?selectedLocale=en (accessed October 1, 2009).

Council of Europe

The Council of Europe was established in 1949 to promote democracy, protect human rights, and maintain the rule of law in Europe. This mission translates into several initiatives, one of which would ultimately lead to the development of a crucial international agreement known as the Convention on Cybercrime, which entered into force in July 2004.

The Council of Europe's Convention on Cybercrime is the only binding international treaty on cybercrime that nations have ratified to date, and covers a range of specific issues that fall under the broad category of cybercrime.[16] Specifically, the Convention defines certain criminal offenses to harmonize international legislations, identifies investigation techniques and powers that are more aligned with the nature of cybercrime, and determines traditional and new opportunities for international cooperation in investigation and prosecution of cybercrimes.[17] While the definitions and investigatory powers established by the Convention are important steps in addressing cybercrime, it is the international cooperation piece of the Convention which offers the most unique and influential results. The Convention requires international cooperation among the signees "to the widest extent possible" and furthermore creates a legal basis

[16] Council of Europe, "Cybercrime: a threat to democracy, human rights and the rule of law," http://www.coe.int/t/dc/files/themes/cybercrime/default_en.asp? (accessed October 1, 2009).

[17] Peter Csonka, "The Council of Europe Convention on Cyber-Crime," in *Cyber-Crime: The Challenge in Asia*, ed. Roderic Broadhurst and Peter Grabosky (Hong Kong: Hong Kong University Press, 2005), 311.

for a 24/7 network of national contact points for cybercrime-related assistance.[18] Since prosecuting cybercrimes depends upon electronic evidence which, if not collected in a timely manner, can be easily lost, the Convention's emphasis on quick and efficient international assistance is one of its greatest strengths.

Other International Efforts

The above selection of international efforts merely scrapes the surface of the extent of international, regional, and bilateral organizations and initiatives devoted to cybersecurity. A study released in 2009 devoted nearly a hundred pages to approximately seventy different international and regional organizations and their cybersecurity efforts, yet the authors recognized that even their extensive list was far from comprehensive.[19] As such, this paper makes no attempt to catalog all or even the most influential international cybersecurity efforts conducted across the globe. Furthermore, it is important to note that the initiatives described above are heavily weighted towards policy issues and do not do justice to the many groups devoted to the more technical and Internet engineering aspects of cybersecurity. Suffice to say, cybersecurity has increasingly become an issue that international organizations, regardless of size or mission, have recognized as an important issue facing nations in the present age.

[18] Ibid., 324.

[19] Michael Portnoy and Seymour Goodman, eds. *Global Initiatives to Secure Cyberspace* (New York: Springer Science+Business Media, LLC, 2009) 97.

Challenges to International Cybersecurity Efforts

Given the plethora of initiatives and opportunities for international cybersecurity engagement, one of the foremost challenges facing national governments is not whether to engage at all, but which of the many groups would afford the best use of government time and resources. As anyone who has ever spoken with a government employee knows, there are always too many meetings and coordinating groups to attend given the limited resources at hand. Unfortunately, deciding which group to support is only the first of several challenges facing international cybersecurity efforts. Each of the many cybersecurity issues that face nations today entail their own unique challenges, however, two particular categories extend across all cybersecurity efforts: balancing government influence, and managing the ratio of technical and policy solutions.

Balancing Government Influence

While it may seem odd to state that one of the foremost challenges to effective international cybersecurity efforts stems from international governments themselves, in fact the careful balancing of national interests and influences is critical to the success of international cybersecurity initiatives. As with other aspects of international relations, cybersecurity is an area that can illustrate profound differences in international political, economic, or social values and priorities. Unless carefully managed, these differences can seriously impede or even derail efforts designed to improve international cybersecurity.

One of the examples of a case in which international tension has affected cybersecurity efforts was briefly described in Chapter 2, namely the case of DNSSEC and the organization and oversight of ICANN. A key obstacle to signing the root (and consequently widespread adoption of DNSSEC) is the entity responsible for holding the keys and the potential for government or governments to influence the activities of that agency. Despite a track record of responsible and appropriate oversight of ICANN by the United States Department of Commerce, the appearance of United States government dominance and influence over the organization is enough to prompt many in the international community to distrust the organization and its role. A recent report to the European Union noted that many nations should pay careful attention to their government's role in Internet governance and matters of cybersecurity because their citizens will "inevitably turn to their governments if there is any major national disruption to their Internet service, and not to the various Internet governance bodies responsible for coordinating resources."[20]

Another example of how government priorities may impede cybersecurity efforts can be seen through differing views on how the Internet should be regulated, particularly with regard to content. The predominant view held in much of the Western world is that the Internet should be a forum for free and open discussion of ideas regardless of content (except in certain situations where the content is distinctly criminal, such as child

[20] Commission of the European Communities, "Communication From the Commission to the European Parliament and the Council: Internet governance: the next steps," http://ec.europa.eu/information_society/policy/internet_gov/docs/communication/comm2009_277_fin_en.pdf (accessed October 2, 2009) 2.

pornography). In contrast, several governments across the world have much broader categories of information that they feel should not be available on the Internet. The massive firewall and content-blocking activities that the Chinese government engages in on a daily basis, blocking access to information and even altering content to align it with the overall vision of what the government deems appropriate, serves as a ready example. Regardless of whether one views content filtering and blocking as appropriate or not, these issues touch upon key factors in international cybersecurity efforts. Beyond the overall potential for such issues to create disagreements between governments that may ultimately derail the entire international process, they can also lead to direct cybersecurity concerns. For instance, in 2009 security researchers revealed vulnerabilities in content-filtering software that the Chinese government sought to have installed on every computer in the country.[21] While the Chinese government later patched the software vulnerabilities and removed some of the mandated install requirements, the example demonstrates how social and political measures can seriously impact cybersecurity. Though the program was mandated only within Chinese borders, such political views on restricting access to content could very easily have the potential to affect larger international cybersecurity efforts.

Unfortunately, the challenge of balancing government influence while at the same time satisfying government desires is not an easy one to address. Despite the differences

[21] Scott Wolchok, Randy Yao, and J. Alex Halderman, "Analysis of the Green Dam Censorware System," University of Michigan, Computer Science and Engineering Division, http://www.cse.umich.edu/~jhalderm/pub/gd/ (accessed October 9, 2009).

in priorities and opinions that nations will have, allowing each nation to define its own rules in order to allow for the most national sovereignty is not necessarily a viable solution. While such an arrangement respects national sovereignty it can also compound the problems for those seeking to address cybersecurity. The global nature of the Internet and the fact that each of the national networks are interconnected means that cyber criminals and others seeking to use the Internet to meet malicious ends will seek to exploit differences between the laws and policies governing networks in various nation states. Should one government decide that allowing the free operation of botnets is in their national interest, cyber criminals will no doubt use the country as a launching pad for their future activities. Similar examples could be inadequate or nonexistent cybercrime laws, improper manipulation of traffic passing through regional networks, or other practices that could affect the integrity and reliability of Internet operation and cybersecurity efforts.

Finally, it is important to note that international cybersecurity efforts may also be hindered by the hidden motives of some of the countries involved. Countries that may be engaged in cyber espionage activities against others may be disinclined to work closely together on efforts to address the very vulnerabilities they exploit to obtain their information. In this manner, international cybersecurity efforts are similar to other international efforts as they can involve internal and external political factors as well as all of the other complications that come with any sort of bilateral or multilateral activity.

Managing Technical and Policy Solutions

Managing the balance of technical and policy solutions to cybersecurity problems presents another challenge to international cybersecurity efforts. This challenge can manifest in several different ways, one being that cybersecurity is a very technical field in which many traditional policy individuals lack expertise. Similarly, the realm of politics and international relations often requires a level of nuance and relationship management which technical cybersecurity experts may not possess. This situation presents challenges because many cybersecurity issues facing the globe have both technical and policy components, necessitating the involvement of individuals with both skill sets to ensure an appropriate solution. For instance, addressing the threat of botnets may require technical measures to prevent a DDOS attack or disrupt the routing of malicious traffic, but successful mitigation of the threat may also require substantial policy measures to ensure cooperation and communication among different nations.

Another key manner in which the technical/policy balance presents challenges involves the rapid advance of technology. In the past few decades the pace of technology innovation and evolution has been exponential, with technology advancing rapidly each year. Unfortunately, with each advance in technology comes similar advances from those who seek to exploit the technology for malicious ends; a fact demonstrated by the dramatic growth of viruses, malware, botnets, and other attacks and vulnerabilities encountered on the Internet today. Unfortunately, the speed of technology often outpaces the speed of government. Nations are rarely viewed as quickly adaptable entities; they are

typically very slow to address new matters for a variety of reasons, not the least of which is the amount of coordination necessary in an organization as large as a national government. Legislation and legal authorities all too often lag behind the pace of technology, presenting difficulties in determining national policy and law enforcement activities. As a result, governments often find themselves confronted by a dilemma with regard to cybersecurity issues: should they employ existing laws which were not originally developed to address these issues or, alternately, should new laws be developed to specifically address new threats? This dilemma is magnified at the international level, where new laws and agreements are typically even more difficult to pass and enforce and have a much longer lead time to develop.

The Path Forward

Given the wide range of cybersecurity threats and issues facing nations in the present age, the multitude of existing cybersecurity initiatives, the rapid pace of technology development, and the challenges posed to international cybersecurity initiatives, cybersecurity seems poised to be an increasingly prominent component of present and future national and international activities. When pursuing these activities, there are several key measures that nations should employ, including judicious use of public-private partnerships, crafting genuinely international solutions, and a clear national and international strategy.

Public-Private Partnerships

One important factor that nations need to consider when developing their international cybersecurity engagements is the involvement of an appropriate mix of public and private entities. As demonstrated in previous chapters, the very foundation and operation of much of the Internet's architecture involves a complex partnership among several public and private entities. Particularly with issues such as DNSSEC or botnets, key players from both the public and private sectors need to be involved if any lasting solution is to be developed. While governments are the only entities that can jointly develop policy to govern national cooperation, private sector companies and organizations around the world have key responsibility and skills that make their involvement in international cybersecurity efforts a benefit as well as a necessity.

On a purely practical level, technical cybersecurity expertise often resides in the private sector to a degree that may not be easily matched by public entities. Market-driven private sector companies are often more able to hire and retain cutting-edge technical experts from a variety of areas, including cybersecurity. As the Internet and cyberspace has grown and become more entrenched in both business and personal activities so too has the desire for cybersecurity. This has in turn created an entire industry devoted to offering cybersecurity products and solutions to government, business, and individuals. This industry represents a wealth of resources, technical expertise, and experience that governments should leverage in collaborative efforts to address some of the most pressing cybersecurity issues around the world today.

On a more strategic level, cyberspace is too vast for any government or coalition of governments to adequately protect. The interconnected, geographically dispersed, and semi-autonomous organizational structure of the Internet is such that private sector entities around the world possess not only cybersecurity expertise, but in many cases a considerable degree of operational control over portions of the Internet. Whether dealing with botnets and the millions of computers owned by organizations and individuals they entail or attempting to deploy DNSSEC across the root servers and regional networks, national governments face limitations in dealing with the problem alone simply due to resources and access to information. As a result, national governments must strongly consider those situations in which even international efforts cannot hope to achieve cybersecurity objectives without appropriate input from the private sector.

Crafting Genuinely International Solutions

The architecture and underlying philosophies of the Internet, with its acceptance of a multitude of networks with minimal connection requirements, emphasis on interconnection and open access, and essentially leaderless organizational structure serve as its foundational elements and greatest strengths. The Internet works as well as it does primarily because, beyond a basic set of requirements and minimally invasive procedures, it allows for open access to businesses, governments, and individuals across the globe. As such, it is important that governments do not neglect this key characteristic when developing cybersecurity policy solutions. While governments may feel the need to assert control over portions of the Internet or attempt to impose their national viewpoints

upon others, one need only imagine a world in which cyberspace was Balkanized into rival networks with no means of interconnection to recognize what is at stake.

While conjuring up visions of being unable to access a webpage because it is not located on your national network may seem overly dramatic, it is not outside the realm of possibility. Already some countries are particularly stringent regarding the content they filter out or block from their citizens view, restricting web pages containing content they deem objectionable. On a more technical level, at points the contention and delay regarding the deployment of DNSSEC at the root zone threatened to create rival root zones that would contribute to a degradation of the Internet architecture. With these situations as examples, governments and international bodies must ensure that they maintain the core principles behind the Internet while developing solutions to the very real and pressing problems of cybersecurity; otherwise they risk destroying the very thing that they are trying to protect.

Clear Strategy

Finally, while it may seem to go without saying, it is absolutely critical that nations hoping to achieve progress on cybersecurity develop a clear and comprehensive strategy for international involvement. Particularly with so many different international venues and opportunities for cybersecurity initiatives, a clear strategy tailored to national and international priorities is a key component to ensuring successful cybersecurity

efforts. These priorities, in turn, should be the product of a careful analysis of the most critical threats and vulnerabilities facing nations and cyberspace in general.

One of the primary needs for a clear and coordinated strategy to cybersecurity is that cybersecurity is such a vast area of activity. As the previous chapters have illustrated, cybersecurity impacts all manner of national and international concerns, ranging from spam, malware, law enforcement cooperation, defense and espionage activities, trade and economic relations, and even social and political interactions. Further complicating these matters is the fact that each of these areas in turn may be broken out into several components, each of which may in turn be the responsibility of different government agencies. Any effective national strategy will need organize the efforts of each government agency and ensure that their missions and authorities are firmly established and understood by all parties. If a government cannot get its own house in order, it will be unlikely to achieve meaningful progress on the international stage.

Conclusion

The opportunities and challenges posed to international cybersecurity efforts are clear, as are many of the measures necessary to ensure their effectiveness. The increasing international reliance upon the Internet makes cybersecurity an issue with which all nations should be concerned. As this chapter has illustrated, already there exist a wide range of international organizations that have recognized cybersecurity as an important topic and have taken steps to involve nations in addressing it. These activities run the

gamut of cybersecurity issues, ranging from anti-spam working groups, botnet mitigation activities, outreach and awareness on cybersecurity topics, assisting nations in developing their cybersecurity laws and legislation, and other critical concerns and initiatives. One hopes that the wealth of activities and the shared national interest in cybersecurity will continue to serve as motivation for increased international efforts to address these critical issues.

CONCLUSION

The preceding chapters have made the case for why effective cybersecurity both requires international collaboration and greatly benefits those nations involved in such efforts. The Internet has enabled an exponential growth of productivity and possibility for the developed world, and presents incredible opportunity for the developing world. Innovation and the rapid pace of technological advancement almost guarantee that the full set of possibilities generated by the Internet has yet to be seen. However, if we as a global community are to continue to achieve this rapid evolution of capability we must develop international solutions for some of the most pressing cybersecurity issues.

Thankfully, it does appear that some progress is being made as many governments have stepped up their involvement in cybersecurity activities both domestically and internationally. Some challenges have been overcome as well even since this paper was originally developed. Since completing Chapter II, ICANN announced a replacement for its Joint Project Agreement with the United States Department of Commerce and replaced it with a new "Affirmation of Commitments." The Affirmation contains provisions which not only ensure the continual existence of ICANN as a non-government not-for-profit organization, but also substantially increased the organization's level of transparency with regard to international oversight.[22] Many

[22] Internet Corporation for Assigned Names and Numbers, "The Affirmation of Commitments – What it Means," http://www.icann.org/en/announcements/announcement-30sep09-en.htm (accessed October 29, 2009).

people and organizations within the international community have hailed the Affirmation as a firm step forward for Internet governance and the security of the DNS.

Despite significant progress, however, serious challenges and threats to cybersecurity remain, while new challenges and issues arise regularly. Among the most concerning of these topics is the future of warfare and the implications that widespread use of the Internet bring. The cybersecurity vulnerabilities and consequences outlined in this paper may very well offer a glimpse of the future of warfare, a future where nations send malware to coincide with their bombs. Already the world has seen accusations of state-sponsored cyber “attacks”, undoubtedly a concept that will continue to affect international discourse. Furthermore, the issue of cybersecurity is a broad one with components involving not only organizations and individuals but complicated problems involving user behavior, software, infrastructure, and even the threat of vulnerabilities built-in to manufactured hardware. Just as the Internet continues to expand and evolve, so too will new threats and issues in cybersecurity.

Throughout the progress made and the challenges yet ahead, one thing remains certain: domestic actions to ensure effective cybersecurity can only go so far, and indeed may threaten the very international fabric of the Internet they seek to protect. Only through careful international collaboration can nations hope to ensure that the Internet remains a powerful and reliable tool for continued progress.

BIBLIOGRAPHY

Abbate, Janet. *Inventing the Internet.* Cambridge, Massachusetts: The MIT Press, 1999.

Abu Rajab, Moheeb, Jay Zarfoss, Fabian Monrose, and Andreas Terzis. "A Multifaceted Approach to Understanding the Botnet Phenomenon." in *Internet Measurement Conference: Proceedings of the 6th ACM SIGCOMM conference on Internet measurement*. New York: ACM, 2006.

Ali, Farha. "IP Spoofing." *The Internet Protocol Journal* 10 no. 4. http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-4/104_ip-spoofing.html (accessed September 15, 2009).

Atkins, D., and R. Austein. "Request for Comments: 3833: Threat Analysis of the Domain Name System." http://www.ietf.org/rfc/rfc3833.txt (accessed August 26, 2009).

Baldor, Lolita C. "Federal Web sites knocked out by cyber attack." *Associated Press*. July 7, 2009.

BBC News. "The cyber raiders hitting Estonia." May 17, 2007. http://news.bbc.co.uk/2/hi/europe/6665195.stm (accessed July 28, 2009).

Chapman, Siobhan. "Massive 2 million PCs botnet uncovered." *Computerworld*. April 24, 2009. http://www.computerworld.com.au/article/300537/massive_2_million_pcs_botnet_uncovered?fp=4194304&fpid=1 (accessed September 15, 2009).

Clark, David. "The Design Philosophy of the DARPA Internet Protocols." *ACM SIGCOMM Computer Communication Review* 18, no. 4 (August 1998): 107.

Commission of the European Communities. "Communication From the Commission to the European Parliament and the Council: Internet governance: the next steps." http://ec.europa.eu/information_society/policy/internet_gov/docs/communication/comm2009_277_fin_en.pdf (accessed October 2, 2009).

Cooke, Evan, Farnam Jahanian, and Danny McPherson. "The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets." in *Proceedings of the Steps to Reducing Unwanted Traffic on the Internet Workshop*. Berkeley, CA: USENIX Association, 2005.

Council of Europe. “Cybercrime: a threat to democracy, human rights and the rule of law.” http://www.coe.int/t/dc/files/themes/cybercrime/default_en.asp? (accessed October 1, 2009).

Csonka, Peter. “The Council of Europe Convention on Cyber-Crime.” in *Cyber-Crime: The Challenge in Asia*, ed. Roderic Broadhurst and Peter Grabosky. Hong Kong: Hong Kong University Press, 2005.

Cyveillance. “Cyber Intelligence Report: A Cyveillance Report, August 2009.” www.cyveillance.com/web/docs/WP_CyberIntel_H1_2009.pdf (accessed September 14, 2009).

Davis, Joshua. “Secret Geek A-Team Hacks Back, Defense Worldwide Web.” *Wired.* December 2009.

Director of National Intelligence. “Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee, Statement for the Record, March 10, 2009.”

Farrell, Greg. “Ex-Goldman employee accused of theft.” *Financial Times*. July 6, 2009.

Gillies, James, and Robert Cailliau. *How the Web Was Born: The Story of the World Wide Web.* Oxford: Oxford University Press, 2000.

Gorman, Siobhan. “Electricity Grid in U.S. Penetrated by Spies.” *Wall Street Journal*. April 8, 2009.

Grabosky, Peter. “The Global Cyber-Crime Problem: The Socio-Economic Impact” in *Cyber-Crime: The Challenge in Asia*, ed. Roderic Broadhurst and Peter Grabosky. Hong Kong: Hong Kong University Press, 2005.

Graham, Bradley. “Hackers Attack Via Chinese Web Sites.” *The Washington Post*. August 25, 2005.

Hafner, Katie, and Matthew Lyon. *Where Wizards Stay Up Late: The Origins of the Internet.* New York: Simon & Schuster, 1996.

Huston, Geoff. “DNSSEC – The Theory.” *Internet Society*. August 2006, under “The ISP Column.” http://isoc.org/wp/ispcolumn/?cat=44 (accessed August 26, 2009).

Huston, Geoff. “Opinion, ICANN, the ITU, WSIS, and Internet Governance.” *The Internet Protocol Journal* 8, no. 1 (March 2005).

http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_8-1/internet_governance.html (accessed August 26, 2009).

International Telecommunication Union (ITU). "ITU History." http://www.itu.int/net/about/history.aspx (accessed October 1, 2009).

International Telecommunication Union. "Cybersecurity Gateway Overview." http://www.cybersecurity-gateway.org/overview.html (accessed October 1, 2009).

International Telecommunication Union. "GCA Brochure." http://www.itu.int/wsis/implementation/2009/forum/geneva/new-gca-brochure.pdf (accessed October 1, 2009).

International Telecommunication Union. "WSIS Declaration of Principles: Building the Information Society: a global challenge in the new Millenium." http://www.itu.int/wsis/docs/geneva/official/dop.html (accessed October 1, 2009).

Internet Corporation for Assigned Names and Numbers, "The Affirmation of Commitments – What it Means," http://www.icann.org/en/announcements/announcement-30sep09-en.htm (accessed October 29, 2009).

Internet Corporation for Assigned Names and Numbers. "Bylaws for Internet Corporation for Assigned Names and Numbers." http://www.icann.org/en/general/bylaws.htm (accessed August 26, 2009).

Internet Corporation for Assigned Names and Numbers. "ICANN to Work with United States Government and VeriSign on Interim Solution to Core Internet Security Issue." June 3, 2009. http://icann.org/en/announcements/announcement-2-03jun09-en.htm (accessed August 26, 2009).

Kanich, Chris, Christian Kreibich, Kirill Levchenko, Brandon Enright, Geoffrey M. Voelker, Vern Paxson, and Stefan Savage. "Spamalytics: An Empirical Analysis of Spam Marketing Conversion." in *Conference on Computer and Communications Security: Proceedings of the 15th ACM Conference on Computer and Communications Security.* New York: ACM, 2008.

Kim, Hyung-Jin. "Report: NKorean army suspected over cyberattacks." *Associated Press.* July 11, 2009.

Kirk, Jeremy. “Estonia recovers from massive DDoS attack.” *Computer World*. May 17, 2007. http://www.computerworld.com/s/article/9019725/Estonia_recovers_from_massive_DDoS_attack (accessed September 14, 2009).

Loukas, Georgios and Gülay Öke. “Protection Against Denial of Service Attacks: A Survey.” *The Computer Journal Advance Access.* Oxford: Oxford University Press, 2009.

McAfee. “September 2009 Spam Report.” www.mcafee.com/us/local_content/reports/7056rpt_spam_0909.pdf (accessed September 14, 2009).

Microsoft TechNet. “How DNS query works.” http://technet.microsoft.com/en-us/library/cc775637(WS.10).aspx (accessed August 26, 2009).

North Atlantic Treaty Organization (NATO). “Armenia hosts cyber defense seminar.” http://www.nato.int/cps/en/natolive/news_50197.htm?selectedLocale=en (accessed October 1, 2009).

North Atlantic Treaty Organization (NATO). “Cyber warfare conference.” http://www.nato.int/cps/en/natolive/news_55801.htm?selectedLocale=en (accessed October 1, 2009).

North Atlantic Treaty Organization (NATO). “SPS workshop rethinks approaches to cyber security.” http://www.nato.int/cps/en/natolive/news_50624.htm?selectedLocale=en (accessed October 1, 2009).

North Atlantic Treaty Organization (NATO). “TRANSNET: Cooperative Cyber Defense (CCD) COE (Estonia).” https://transnet.act.nato.int/WISE/TNCC/CentresofE/CCD (accessed October 1, 2009).

Organisation for Economic Co-operation and Development (OECD). “About OECD.” http://www.oecd.org/pages/0,3417,en_36734052_36734103_1_1_1_1_1,00.html (accessed October 1, 2009).

Organisation for Economic Co-operation and Development. “APEC-OECD Malware Workshop.” http://www.oecd.org/document/34/0,3343,en_2649_34255_38293474_1_1_1_1,00.html (accessed October 1, 2009).

Organisation for Economic Co-operation and Development. "What is the Working Party on Information Security and Privacy (WPISP)." http://www.oecd.org/document/46/0,3343,en_2649_34255_36862382_1_1_1_1,00.html (accessed October 1, 2009).

Organisation for Economic Co-Operation and Development. *Computer Viruses and Other Malicious Software: A Threat to the Internet Economy.* OECD Publishing, 2009.

Portnoy, Michael. and Seymour Goodman, eds. *Global Initiatives to Secure Cyberspace*. New York: Springer Science+Business Media, LLC, 2009.

Shofield, Jack. "British hacker claimed to be behind US and Korean attacks." *Guardian.co.uk*, July 15, 2009. http://www.guardian.co.uk/technology/2009/jul/15/hackers-internet-attack (accessed July 28, 2009).

Symantec. "MessageLabs Intelligence: August 2009: Cutwail Damaged by ISP Shutdown Whilst Donbot Offers Medical Assistance to Billions." http://www.messagelabs.com/mlireport/MLIReport_2009.08_Aug_FINAL.pdf (accessed September 14, 2009).

The Internet Corporation for Assigned Names and Numbers. *ICANN Proposal to DNSSEC-Sign the Root Zone*. http://www.ntia.doc.gov/DNS/ICANNDNSSECProposal.pdf (accessed August 26,2009).

The Internet Corporation for Assigned Names and Numbers. *ICANN Proposal to DNSSEC-Sign the Root Zone*. http://www.ntia.doc.gov/DNS/ICANNDNSSECProposal.pdf (accessed August 26,2009).

Thornburgh, Nathan. "Inside the Chinese Hack Attack." *Time.* August 25, 2005.

Treynor, Ben. "More on today's Gmail issue." posted on *The Official Gmail Blog*. September 1, 2009. http://gmailblog.blogspot.com/2009/09/more-on-todays-gmail-issue.html (accessed September 15, 2009).

U.S. Department of Commerce National Telecommunications and Information Administration. "Press Release: NTIA Seeks Public Comments for the Deployment of Security Technology Within the Internet Domain Name System."

October 9, 2008. http://www.ntia.doc.gov/press/2008/DNSSEC_081009.html (accessed August 26, 2009).

U.S. Department of Commerce. "Memorandum of Understanding Between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers." November 25, 1998. http://www.ntia.doc.gov/ntiahome/domainname/icann-memorandum.htm (accessed August 26, 2009).

U.S. Department of Homeland Security. *National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency*. Washington, DC: Government Printing Office, 2009.

Vamosi, Robert. "Cyberattack in Estonia--what it really means." *CNET News*. May 29, 2007. http://news.cnet.com/Cyberattack-in-Estonia-what-it-really-means/2008-7349_3-6186751.html (accessed July 28, 2009).

VeriSign. *Root Zone Signing Proposal*. September 22, 2008. http://www.ntia.doc.gov/DNS/VeriSignDNSSECProposal.pdf (accessed August 26, 2009).

Weaver, Nicholas, Vern Paxson, Stuart Stanifold, and Robert Cunningham. "A Taxonomy of Computer Worms." in *Workshop on Rapid Malcode: Proceedings of the 2003 ACM Workshop on Rapid Malcode.* New York: ACM, 2003.

Weber, Joseph. "Obama: Cybersecurity a 'national priority', *Washington Times*, May 29, 2009.

Wolchok, Scott, Randy Yao, and J. Alex Halderman. "Analysis of the Green Dam Censorware System." University of Michigan, Computer Science and Engineering Division. http://www.cse.umich.edu/~jhalderm/pub/gd/ (accessed October 9, 2009).