IN THE INTERNET WE TRUST?
SECURITY ISSUES IN INTERNET GOVERNANCE

by
Adrienne Marlena Allen

A thesis submitted to Johns Hopkins University in conformity with the requirements for
the degree of Master of Arts in Global Security Studies

Baltimore, Maryland
August 2014

© 2014 Adrienne Marlena Allen
All Rights Reserved
ABSTRACT

Underlying all military, political, and individual use of the Internet is trust. The ability of the Internet to live up to that trust is weakening, in part due to increasing demands for ever-expanding applications, and in part due to the increasing diversity of malicious actors, including states, seeking to control or conform the Internet to their purposes. This thesis argues that a systemic, global loss of trust is just starting to broadly occur in the Internet’s ability to transmit data securely and in the current multistakeholder model of Internet governance to govern fairly. This ebbing of trust in both the technical and the policy levels creates a need to apply a new generation of accountability mechanisms that extend beyond market dynamics.

Each of the three chapters in this thesis focuses on an aspect of waning trust due to global vulnerabilities in the Internet’s infrastructure and governance. The first chapter posits that certificate authorities possess a degree of immunity to traditional reputational pressures, and suggests drawing from lessons learned in the private military contractor industry to make reputation more important and increase accountability. The second chapter evaluates whether security solutions to Border Gateway Protocol (BGP) vulnerabilities are adequate to address deliberate, state-sponsored attacks. The third chapter analyzes schools of thought on Internet governance models and asks whether U.S. policy positions regarding surveillance and historic legislation regarding access position the country for continued leadership in the current model.

All three chapters used case studies primarily of cyber incidents, as well as trust-based frameworks, to examine evidence. The paper concludes that trust-based mechanisms, including reputational levers, trust frameworks, and national accountability structures, are available for use by individual companies, networks of networks, and at
the state level, respectively, but current policy prescriptions are not widely taking
advantage of them. Most significantly, the U.S. government’s ability to push for trust-
based solutions in the Internet’s technical infrastructure may weaken if the U.S. cannot
inspire trust in its own leadership.

Thesis Advisors and Readers: Dr. Benjamin Ginsberg, Dr. Kathryn Wagner Hill, Dr.
Sarah O’Byrne, Mr. Thomas Stanton, and Dr. Jacob Straus
ACKNOWLEDGEMENTS

I am tremendously grateful for the selfless support, patience, and love of my husband Matt, without whom this thesis would not be possible.

I would also like to thank the members of the Johns Hopkins faculty that guided me through this process and imparted truly inspiring paradigms for evaluating national security, especially Dr. Sarah O’Byrne, Dr. Jacob Straus, Dr. Benjamin Ginsberg, and Dr. James Lewis.
# Table of Contents

INTRODUCTION .................................................................................................................. 1  

CHAPTER 1: EXPOSING A GLOBAL WEAKNESS: REPUTATION OF CERTIFICATE AUTHORITIES .......................................................................................................................... 14  
  Industry Overview and Literature .................................................................................. 16  
  The Market for Certificate Authorities ......................................................................... 20  
    Definitions of Reputation and Reputational Loss ....................................................... 21  
    Current Frameworks for Measuring Reputational Loss ............................................. 23  
    Gaining Market Share ............................................................................................... 25  
  Recent Attacks: RSA, DigiNotar, and Comodo ............................................................ 27  
    RSA Breach ............................................................................................................... 28  
    DigiNotar Breach ..................................................................................................... 30  
    Comodo Breach ...................................................................................................... 32  
    Conclusion ................................................................................................................ 33  
  Analyzing Transnational Shadow Industries ................................................................. 36  
    Private Security Companies ....................................................................................... 36  
    Possible Lessons from Private Security Companies ............................................... 39  
    A Path Forward ......................................................................................................... 42  
    Conclusion ................................................................................................................ 43  

CHAPTER 2: ROUTING SECURITY AND TRUST IN THE INTERNET ................................... 46  
  Background: Overview of Internet Routing .................................................................... 48  
  Literature Review .......................................................................................................... 52  
    Routing Vulnerabilities ............................................................................................... 52  
    Solutions ..................................................................................................................... 55  
  Case Studies .................................................................................................................. 62  
    Belarus and Iceland .................................................................................................... 63  
    Applying Social Trust Theory to BGP Security ......................................................... 67  
    Conclusion .................................................................................................................. 75  

CHAPTER 3: STAKEHOLDER MODELS FOR INTERNET GOVERNANCE .............................. 77  
  Background .................................................................................................................... 79
Literature Review .................................................................................................................. 84
First View: Multistakeholder Model is Still Unstudied, but the Best Alternative .......... 85
Second View: Advocacy for the Unregulated, U.S.-Sponsored Model ..................... 88
Third View: State Regulation is Inevitable ....................................................................... 91
International Behaviors .................................................................................................... 96
Internet Access ..................................................................................................................... 96
Surveillance .......................................................................................................................... 101
Analysis ............................................................................................................................... 104
Conclusion ........................................................................................................................... 106
CONCLUSION ..................................................................................................................... 107
BIBLIOGRAPHY ................................................................................................................. 114
BIOGRAPHY ....................................................................................................................... 125

List of Figures

Figure 1: Public Trust Framework ...................................................................................... 70
INTRODUCTION

“The Internet is the coolest thing mankind has done since Gutenberg, the wheel, and fire.”¹ Since its earliest days, the Internet has enabled revolutionary access to information around the world. Disruptive innovation to human interactions and commerce has skyrocketed in the decades since United States (U.S.) engineers developed the Advanced Research Projects Agency Network (ARPANET) in 1969. One of the most important elements of the Internet’s architecture, unchanged since its ARPANET days, is that it is fundamentally dependent on trust. Consumers trust their devices with their personal information in order to facilitate faster connections and identify products they like. Internet providers and hardware producers trust each other to follow common protocols and assume each has a rational, market-driven motive in mind. Nations trust that the organizations charged with Internet governance will not undermine their concepts of national sovereignty in cyberspace.²

However, the assumption that the Internet is trustworthy is not accurate anymore. In 1998, hacker collective L0pht testified before the U.S. Senate that the Internet did not deserve unfettered trust, claiming they could take down the Internet in less than 30 minutes.³ The hackers’ discussion about cyber vulnerabilities in U.S. critical infrastructure prompted an uptick in security spending and research by the U.S.

¹ Healey, Jason. 2014. “Cyber Conflict.” Discussion at the RSA Conference, San Francisco, California, February 27.
² Though sometimes used interchangeably, the terms “Internet” and “web” are not synonymous. The Internet is the layer of routers, switches, and other hardware that enable exchanges of information across networks. The World Wide Web (web), developed in 1989, lies on top of the Internet’s physical infrastructure and translates the exchanges of data into usable information and transactions.
government. As of 2014, however, demands on the Internet have continued to outpace security measures. The Internet is currently used for military applications, espionage, and social networking in addition to commerce. Increasing numbers of Internet users and uses provide new targets for malicious actors looking to steal, spy on, modify, or disrupt data. State and non-state actors are developing technologies to exploit Internet vulnerabilities to achieve economic or political outcomes. While the dangers have been of long-term interest to hackers, many web users are still unaware of how tenuous their everyday trust in the Internet is, and Internet security is a relatively recent newcomer to high foreign policy debates.

Originally engineered to enhance communications, the Internet was designed more for survivability, workability, and connectivity through load and cost balancing than for protecting personal and economic security.\(^4\) Traffic was directed based on where load was lightest. Today, the Internet supports wide-ranging forms of communication, including satellite communications, cellular technologies, and the numerous applications and transactions one can use and conduct through the web. The “network effect” also pulls additional users into the web. Individuals, enterprises, and networks are all incentivized to use the Internet in order to increase their visibility, customers, and experience.\(^5\) As the user base of the Internet continues to expand exponentially, countries around the world are investing research and development resources into cyber technologies that can be used as instruments of power in espionage and military contexts.

This thesis seeks to explore some of the basic risks to the Internet through the lens of trust. The common theme throughout is that trust in the Internet is beginning to erode

---


on many levels, not just because of exploits of coding flaws, but due to the inherent design of the Internet itself. At the same time, state behavior in cyberspace is changing as more countries develop information and communications technology (ICT) and use it to increase their power. Technical and policy solutions must evolve in order to address the growth of this complex development.

Trust is prevalent in and essential to the operation and political support of the Internet. Trust broadly defined in this thesis is the “psychological state comparing the intention to accept vulnerability based upon positive expectation of the intentions or behavior of another.” In the tactical context of the Internet, trust is manifested by individuals, companies, and states entering into a variety of relationships in order to provide or consume services. Chapter 2 of this paper employs a functional representation of trust, positioning forms of trust along vertical and horizontal axes. Horizontal trust is trust among peers, with few hierarchical enforcement mechanisms to compel good behavior. Vertical trust is trust facilitated by a hierarchy, where enforcement and compliance are central. Influencing the trust among peers or in a hierarchy will as a result influence trust in the Internet itself where these relationships operate. Trust in the Internet is the common thread throughout this thesis.

This thesis is made up of three chapters. Each chapter focuses on a particular aspect of Internet security, discusses weaknesses in the system of trust, and analyzes where behaviors should change in response to cyber incidents. The first chapter focuses

---

on authentication issues in the Internet’s application layer.7 The second chapter focuses on vulnerabilities in routing, which is part of the Internet’s physical infrastructure. The third chapter evaluates weaknesses in the current and proposed Internet governance models. All three chapters reveal an increasing appetite among bad actors to exploit vulnerabilities as well as a changing narrative about how governing the Internet’s technical functions should occur.

The conclusion across all of the chapters is that the Internet’s trust framework has fatal flaws on a global scale, and while technical solutions are underway, international social and political governance mechanisms are necessary to improve accountability in Internet infrastructure, protocols, and governance. In addition, the increased recognition of the Internet’s global vulnerabilities is coming at a time when trust in the U.S. government is near a significant low.8 9 As a result, incorporating U.S.-sponsored solutions into architectural changes may depend on outside support including large-scale private sector adoption, and likely future attacks, before other nations are willing to ally with U.S. policy prescriptions.

The first chapter examines certificate authorities because they provide a glimpse at end user interactions with the web. Certificate authorities are fundamental to discussions of trust because they enable everyday reliance on the web for a multitude of transactions. This chapter asks whether accountability mechanisms can spur better behavior and transparency among certificate authorities. This paper is divided into three

---

7 The application layer includes the exchange of data among users on the web. It is generally referred to as the “top” layer of the Internet and protocol suites because of its proximity to the end user and reliance on architecture below it for functions including addressing, routing, and communications. Source: http://technet.microsoft.com/en-us/library/cc958821.aspx


sections. The first section outlines some of the views and models of how reputation is gained and lost, and examines whether variables that influence reputation can be applied to certificate authorities. The second section examines three case studies of breaches to certificate authorities, where damage was greatest, and why. A third section compares certificate authorities to another poorly understood industry, private security companies, to draw lessons learned about where applying reputational costs in obscure industries can be most effective and where future work should be done.

To provide context for certificate authorities, the chapter begins with an overview of the flaws endemic to individual certificate authorities as well as how they function as a network. The flaws highlight the insufficiency of the current structure of accountability measures to motivate certificate authorities to operate responsibly and without government interference. In some cases, certificate authorities are sponsored or operated directly by governments, which opens the door to placing political pressures on these authorities to validate or revoke certain websites. The first part of the chapter also provides an overview of the current literature, including academic studies, economic modeling on reputational loss and gain, news stories of recent breaches, and security journals documenting the creation and evolution of certificate authorities. The literature overwhelmingly agrees that the structure of certificate authorization has significant vulnerabilities. Furthermore, much of the literature affirms that because certificate authorities manage trust in online transactions, attacks on the authorities are likely to have a compounding effect on loss of trust in Internet security.

The chapter includes three case studies of recent breaches to demonstrate that a certificate authority can successfully avoid severe reputational damage if it has a
demonstrated commitment to security before and after an attack occurs. Case studies include RSA, DigiNotar, and Comodo, which are three of the largest entities in the authentication space. Each one of these case studies was chosen from the available literature because the companies in question had experienced a significant attack that compromised their authentication capability. Furthermore, all three companies possess significant market share in their respective markets, so the attacks demonstrated repercussions on Internet infrastructure in general. Lastly, all three responded differently to the attacks, providing an opportunity to contrast how differing crisis communications and other incident management efforts may result in varying degrees of reputational loss.

The case studies lead to two main conclusions. First, the largest certificate authorities’ command of the market may shield them from some of the more destabilizing effects that would force others out of the market after a breach. Second, certificate authorities that can demonstrate reasonable efforts to protect from and respond to attacks are less likely to suffer reputational loss. Customers transfer their lost confidence into the trust system as a whole, instead of the specific certificate authority. Both of these aspects have implications for Internet security. If the market does not currently hold certificate authorities accountable enough to incentivize good practices, then state attempts to operate or compel certificate authorities is not likely to stop. It should be noted that the conclusions from the case studies will need further exploration, since cascading effects from the breaches will continue to unfold. Chapter One was completed in August 2013, so further study is recommended as longer-term economic effects of breaches on company valuations and pricing can be documented. Furthermore, the Heartbleed
vulnerability discovered in April 2014 can cast additional light on the context of SSL vulnerabilities.

The last section in Chapter One contrasts certificate authorities with private security companies, as both are transnational industries that can blur lines of state sovereignty. States can sponsor or explicitly own certificate authorities or contract with private security companies, according to which amount of liability the state is willing to accept. As a result, certificate authorities and private security companies can take actions on behalf of a state that has international implications, without attributing legal responsibility to the state. In both industries, auditing and evaluation are voluntary. U.S. certificate authorities will commonly pay for validation from auditing firms, which increases their legitimacy. However, there is no international standard that all authorities or companies must subscribe to in order to earn the reputation of a trusted entity. Both industries also suffer from lack of long-term incentives to promote good behavior because of insufficient customer demand for good behavior. This paper argues that some of the same mechanisms used to insert accountability mechanisms into private security companies should also be applied to certificate authorities, but the evidence suggests that a stronger international community is a prerequisite to enforcing good behavior among the certificate authorities. To date, this community still does not exist.

Chapter Two analyzes vulnerabilities in Internet routing, which sends data to their proper destinations. This chapter asks whether applying a trust framework to proposed security solutions can also strengthen relationships among the entities involved. Chapter Two focuses on Internet routing because of its critical role in enabling the Internet’s physical infrastructure to properly function. Trust issues in Internet routing and routing
protocols illustrate how the physical aspects of the Internet are vulnerable to cyber incidents. The paper is divided into three sections. The first section conducts a review of the literature on commonly identified vulnerabilities in Border Gateway Protocol (BGP), which is the standard of communication that routers use to send information to and from different networks. BGP is commonly referred to as the “glue” that binds the Internet together. The second section provides a case study on seemingly deliberate attacks on BGP to demonstrate how threats mostly consisting of numerous, unintentional route hijacks are expanding to rare, deliberate attempts to monitor and potentially modify data around the world. The third section uses a trust framework referred to in social theory to frame current solutions to BGP vulnerabilities. Current technical security proposals rarely address undesired political exploitation by countries asserting greater authority in cyberspace. They also do not account for how inserting hierarchical authority might affect trusted relationships among peers. Examining solutions through the trust framework identifies where technical and policy solutions may need to account for cause and effect dynamics in changing trust structures and how those dynamics can affect success of the proposed solutions.

Chapter Two begins with a brief overview of how routing works on a basic level in order to provide context on the various relationships and steps involved in routing data on the Internet. Routing relies on a deep bench of Internet Service Providers (ISP), routers, and network operators to send data to its intended destinations. The literature review draws from technical working group reports from public-private partnerships, scientific experiments, modeling in academic journals, and multiple security articles to produce a holistic picture of the ongoing discussions around Internet routing security.
The review uncovers broad agreement in the literature that there are many unintentional threats to routing, but a smaller amount of the literature discusses and highlights concerns with deliberate threats. Route hijacking is widely recognized as a basic threat to Internet infrastructure, but generally the literature does not treat it as a significant impairment to Internet functionality. The exception to this is when it occurs on a large scale, such as in the cases of China and Pakistan, which both accidentally rerouted global traffic in attempts to block domestic access to certain websites. These incidents illustrated how states that can accidentally reroute global traffic likely have the capability to deliberate reroute it as well.

The literature features two different camps of scholars and technical experts who recommend changes to BGP: those who advocate central roots of trust to exert more control over providers and routers in order to increase accountability and authenticate routing announcements, and those that decry use of central roots because of their propensity to open the way for a regulatory regime or for abuses of power. Most proposals in favor suggest that regional Internet address registries, or RIRs, should serve as central roots of trust. Technical experts and academics in favor of a central root of trust propose a system whereby any network operator could then look up a signed certificate of a routing announcement and use the authentication to identify the originating authority. If an unknown or incorrect ISP appeared as the origin of the announcement, the operator could then deter other routers from passing the traffic to the indicated destination. Each RIR would also have a degree of authority over which paths it chooses to authorize. Lastly, trust roots would be able to mediate conflicts between networks and aggregate resources across the Internet to combat common problems.
Those opposed to central trust roots fear that RIRs, or whichever entity was designated as a trust root, would be vulnerable to political persuasion, ultimately decreasing trust in the system as a whole. Providing RIRs with power to revoke or issue certificates would increase the risk that they could abuse that ability in favor of political allies or due to pressure. At the same time, a trust root would divest ISPs of a degree of their power to adjudicate service. A more hierarchical structure could conceivably find an ISP noncompliant and take steps to disconnect some of its services.

To illustrate a scenario where these solutions are relevant, the chapter features a case study on Belarus and Iceland. These countries are featured simply because to date, they represent the only open source example of deliberate, systematic attacks on Internet routing. Available intelligence includes time, traceroutes, and geographical locations of the attacks, and demonstrates a significant investment of time and resources into attacks on routing, as well as a lack of insight into motive. The case study also briefly examines Belarus’ role as a dialogue partner in the Shanghai Cooperation Organization (SCO). China’s leadership in the SCO and some of its activities with other dialogue partners reveal an interest in helping partners develop route filtering and other Internet control capabilities. The paper makes no effort to connect any nation to the attacks, but further study should examine variables that could provide context on possible motives.

Lastly, the chapter draws on ideas of horizontal and vertical trust to evaluate current technical solutions to BGP vulnerabilities. Horizontal trust refers to trust among peers in distributed or social networks, whereas vertical trust refers to an entity’s trust in hierarchical authority. Aspects of the Internet often align closely to horizontal trust, especially since popular use of the web includes social networking. In contrast, Internet
routing relies on a hierarchy of address allocation authorities, backbone providers, and smaller ISPs to propagate information and validate trustworthiness down their respective chains, which exemplifies vertical enforcement mechanisms to compel good behavior.

However, social experiments have highlighted a potential causality between horizontal and vertical trust that has not yet been translated to Internet routing. Social dynamics indicate that a change in vertical trust causes more of a change in horizontal trust than the other way around. So an increase or decrease in trust in an authority is more likely to result in a corresponding gain or loss in trust in one’s peers. Increased or decreased trust in one’s peers, conversely, is less likely to have a significant corresponding gain or loss of trust in authority. As a result, solutions to BGP vulnerabilities should be reexamined in this context. Using cryptography and central trust roots may result in increased vertical trust, but if those central trust roots abuse their power then trust in the everyday transactional relationships among peers are more likely to suffer as well.

The proposed solutions all recognize that BGP vulnerabilities are significant enough to require ongoing study. Most of the solutions require large amounts of time and resources to implement, and so far there is not enough customer demand or awareness to make these solutions market viable. However, if attacks like those seen in Belarus and Iceland continue to occur, trust in the Internet will likely plummet. States may also become more likely to take advantage of BGP vulnerabilities to eavesdrop on national or international traffic. In response, solutions must evolve to incorporate deliberate state actions as a category of threat, and do so with an eye to how changing horizontal or vertical trust will have follow-on effects throughout the routing ecosystem.
Chapter Three hypothesizes that U.S. political actions since 9/11 have provided other nations with ammunition to accuse the U.S. of untrustworthiness in shepherding the multistakeholder model of Internet governance. The weakening U.S. role in international governance of the Internet is particularly significant because it signals a possible change to how the Internet as a whole will function in the coming era. The chapter organizes the primary views on the future of Internet governance into three camps based on how each recommends the U.S. role should evolve. The literature review drew from international scholars, political leaders, open source press materials, international forum publications, and academic papers to form a multi-faceted look at governance. These various sources also provided a holistic look at technical and policy concerns of great and emerging powers as well as history of competing governance models.

The second section describes two examples of Internet controls spreading globally that pose risks to successfully implementing U.S.-preferred models of governance. Blocking web access and surveillance are two forms of Internet controls that many countries are widely using to ensure their “information security,” which includes control of speech and expression. The U.S. also has engaged in surveillance and has toyed with legislation on blocking Internet access in times of emergency. Despite the U.S. Congress’s long-term insistence on an open, free Internet, it has allowed intelligence agencies to develop sophisticated surveillance capabilities that seemingly emasculate the government’s claims to espouse an Internet free of state control. These two case studies were selected because of their prominence in national security debates at the time this paper was written and their likelihood of shaping future governance and technical debates.
The third section analyzes the implications of state behavior in governance forums, including the behavior of the U.S. The chapter concludes that U.S. influence in multistakeholder forums is likely to decrease as a result of U.S. actions, which may in turn decrease the strength of the multistakeholder model. Of note, this chapter was completed in December 2013 before United Nations and national meetings occurred to discuss these issues, as well as announcements by governance organization ICANN (Internet Corporation for Assigned Names and Numbers) to transfer some of its U.S.-shepherded address allocation functions to the international community. Further study is critical to updating the context in this chapter as well as evaluating longer-term implications of U.S. behavior in 2012-2013.

All together, the three chapters constitute a look at cracks in the building: the virtual application, physical infrastructure, and political aspects of the Internet. While the Internet has been remarkably resilient to attacks thus far, erosion in reliability is occurring in many places. This has implications for consumer and operator activity on the Internet, as well as how the U.S. asserts its role and scopes future priorities in the international community. If the U.S. is to influence development of technical controls and threat awareness, then it must improve its reputation in governance forums and convince other nations that it is still a trustworthy advocate of the multistakeholder model.
CHAPTER 1: EXPOSING A GLOBAL WEAKNESS: REPUTATION OF CERTIFICATE AUTHORITIES

In today’s “new economy,” which has become service-based instead of manufacturing-based, the U.S. relies heavily on Internet services to conduct commerce, including online banking and numerous other daily transactions. These transactions can include various types of activities such as correspondence including e-mails, electronic data interchange, electronic funds transfers, marketing, and supply chain management. The funds and information flowing across virtual networks makes the data a prime target for malicious actors seeking financial or political gain. Specifically, the industry of certificate authorities presents a unique problem. Certificate authorities operate almost as a shadow industry to most consumers; not many end users know of or understand how their daily e-commerce transactions are secured. Recent attacks on certificate authorities around the world have brought the industry more into the public eye, but have also demonstrated severe weaknesses in the overall system of trust that the certificate authorities support. This paper focuses specifically on why issues of reputation should be considered when proposing policy solutions to change to the certificate authority system of trust.

Weaknesses in certificate authorities portend severe danger for the Internet and networked communications in the 21st century if the system does not undergo fundamental changes. Efficient and secure information technology (IT) and communications architecture is necessary to support the basic ability of two parties to exchange information in a trusted connection. This underpins the national security and financial health of the U.S. and nations around the world, which will increasingly have data intercepted and manipulated unless regulatory, policy, and technical changes occur.
I maintain that security companies, specifically trust certificate authorities, are relatively resistant to reputational damage from cyber attacks for two reasons, and that any policy prescription needs to take this unique economic reality into consideration. The first reason why certificate authorities are resistant to reputational damage is because their services are essential enough to global communications that demand is inelastic, proofing them against fallout from security problems. The second reason is because when a certificate authority is breached, victims often transfer their lost confidence and lack of trust into the trust system as a whole instead of the specific certificate authority. In this way, the system absorbs some of the consequences that might usually plague an individual company in other industries. The consequence of this anomaly is that the market does not currently hold certificate authorities accountable enough for reputational damage to incentivize good practices. This presents a global security problem, since transactions around the world are becoming more vulnerable to increasingly sophisticated malicious actors and the nebulous role of states in operating certificate authorities means regulation would be complex.

To provide background on this problem, I first discuss weaknesses identified in individual certificate authorities and the underlying system as described in the literature. Second, I discuss common ideas about how reputation is gained or lost and how damage can be measured to indicate that certificate authorities are uniquely immune to common reputational requirements for companies. This paper will use a series of three case studies to examine recent attacks on major certificate authorities in the Netherlands and in the U.S. and identify how the market responded. In these case studies, I examine and compare first-order economic consequences including direct and indirect costs where
available, as well as the security community’s reaction to each incident. Based on these case studies, I propose that similar to other shadow industries like private security companies, certificate authorities must be brought into a more transparent system of accountability where reputation is emphasized.

**Industry Overview and Literature**

Before discussing current problems with certificate authorities, first I will define what these companies are and the niche market they occupy. Certificate authorities are third party organizations that use public key infrastructure (PKI) technology to validate the identities of two transacting parties, most commonly an end user’s Web browser and the website it has been commanded to retrieve.\(^{10}\) For example, a bank will own a pair of keys. The public key asserts the bank’s identity; when a user logs on, his or her browser receives the public key along with a digital certificate signed by a certificate authority verifying that the bank is who it says it is. The browser’s website also verifies the identity of the certificate authority against its database of legitimate authorities. As the user logs on and submits information to the bank, the bank server’s private key deciphers the information so only the bank can read it. This exchange of credentials occurs through a Transport Layer Security (TLS)/ Secure Sockets Layer (SSL) technology that encrypts the information, thereby preventing successful interception during the communications exchange. By validating websites, certificate authorities indicate to Web browsers whether or not a website is trustworthy. Because demonstrating trustworthiness is crucial for online e-commerce transactions, the activity of certificate authorities underwrites the security of networked communications across the globe. However, “the degree of

---

security provided by SSL rises and falls with the authentication system upon which it rests.”\textsuperscript{11} This means that even if a legitimate website is certified by an untrustworthy certificate authority, then the system is still at risk because of the degree of doubt.

Certificate authorities in the U.S. most frequently pay for evaluation against private standards by accounting firms. After having received approval by the accounting firm, the authority can then request that Internet browser sponsors include its certificate in its list of trusted certificate authorities. This enables the certificate authority to then sell its certificate to websites or other subscribers seeking to execute the authentication procedure. When a user makes a request for his or her browser to retrieve a particular website, the browser then compares the signing certificate authority to the list of approved authorities in its database.\textsuperscript{12}

Across the security community, there is widespread agreement that the certificate authority framework has severe vulnerabilities and must be changed. First, the system of certificate authorities is unstructured and unregulated. There is little brand recognition around certificate authorities, so they can operate without much public scrutiny. Certificate authorities are too poorly understood and too numerous, and that fewer, more regulated certificate authorities would mean a safer market that is better understood. The current “wild west” environment makes the whole certificate authority-based system of trust fundamentally flawed. Each individual certificate authority has the autonomy to validate any website, which arguably creates the potential to become “a single point of failure” for the whole system because each one can certify any domain name including


\textsuperscript{12} Roosa and Schultze 2010, 4
those that should not be certified.\textsuperscript{13} Current legal frameworks for authentication
disadvantage the end user, who is often unaware of the certificate authority’s existence in
their transactions or the certificate authority terms they are implicitly accepting by
conducting online activity.\textsuperscript{14}

Another emerging problem is that certificate authorities can also issue additional
subordinate certificates through a “hybrid” model of “sharing trust.”\textsuperscript{15} With each new
subordinate certificate, the level of accountability and security of the whole system
decreases, since each one has the ability to vouch for any domain name. This means that
illegitimate domain names or those hosted by malicious actors have a better chance of
obtaining third party certification and successfully intercepting communications between
an end user and the malicious website. It also decreases control that both browser
companies and end users have over the list of certificate authorities they trust. Currently
there are just beyond 650 operational certificate authorities around the world.\textsuperscript{16}
Additional research on certificate authorities by the Electronic Frontier Foundation SSL
Observatory on its website shows that certificate authorities operate in more than 54
jurisdictions, and there are no overarching regulations or codes of conduct that extend to
all certificate authorities in operation. In addition, 46 certificate authorities were
government-owned as of 2010 and many more countries owned subordinate certificate
authorities.\textsuperscript{17} The accounting industry in the U.S. has sponsored several sets of standards,

\textsuperscript{13}Van Eijk, Nico and Axel Arnbak. 2012. “Certificate Authority Collapse: Regulating Systemic
Vulnerabilities in the HTTPS Value Chain.” TRPC.
http://cyber.law.harvard.edu/events/2012/09/vaneijk_arnbak
\textsuperscript{14}Roosa and Schultze 2010, 3
\textsuperscript{15}Roosa and Schultze 2010, 6
\textsuperscript{16}Van Eijk and Arnbak 2012
\textsuperscript{17}Electronic Frontier Foundation. 2010. EFF SSL Observatory. https://www.eff.org/observatory
but they do not uniformly apply to global certificate authorities and no minimum security standard exists for SSL certificates.

Because no consistent jurisdictional authority regulates or holds certificate authorities accountable, this enables untrustworthy certificate authorities to operate. Current literature emphasizes the realized potential for disruptive man-in-the-middle attacks due to intimate levels of access that malicious actors can acquire through use of the certificate authority trust system. Man-in-the-middle attacks are not discussed in depth in this paper, but the definition used here includes when a malicious actor intercepts and decrypts the connection to an SSL-secure server, enabling him or her to manipulate, change, or view data. Several security researchers have been able to exploit single flaws in the trust system to create these types of attacks and potentially impact numerous websites.

Attacks on certificate authorities present even more difficulties. Not only do they impact the individual companies, but they affect the Internet at large; if the trust providers that are supposed to guarantee secure networked communications become unreliable, then trust in national and individual capabilities to safeguard sensitive military and commercial information on the Internet is severely impacted. This means that attacks on certificate authorities, of which only a handful have been reported in the media each year since 2010, can “severely [undermine] confidence in the system.”\textsuperscript{18} Financial consequences from a hack vary more widely. At the enterprise level, organizations most often have to manually replace compromised certificates, which can be a lengthy process.

This means that organizations may have to operate “in a compromised condition”—possibly for many months—while the thousands of compromised certificates are manually replaced,” leaving them even more vulnerable to exploits.¹⁹ The review of existing literature agrees that the global trust system is vulnerable because of the poor structure and regulation of certificate authorities, but damage is often discussed in hypotheticals and assumptions. The most common argument is that the explicit purpose of these certificate authorities is to increase “trust” in secure transactions, so their weakening from an attack weakens trust in Internet security by extension. Most scholars have identified this structural problem with the system of trust, but researchers have acquired information on only a few attacks enough to be able to study them in depth. This paper will supplement the current literature by showing that post-attack damage to these companies rarely includes reputational damage if the company demonstrates a commitment to security and customer communications before and in the wake of the attack.

**The Market for Certificate Authorities**

After reviewing operations of and problems with certificate authorities, this section will discuss the role of reputation in certificate authority security. First, the section will describe common definitions of reputation and reputational costs and second, will examine results from current models of measuring costs to discuss implications for certificate authorities. Third, the section will expand on how certificate authorities gain market share, including possible building blocks for how one develops its reputation.

Definitions of Reputation and Reputational Loss

Existing definitions of reputation and reputational loss provide an understanding of the current environment. Concepts of company reputation include the idea that reputation is a measure of confidence of shareholders, customers, and investors in the company.\(^{20}\) This paper will use Cannon and Schwaiger’s two-fold construct to define components of company reputation: 1) the sympathy the company inspires in its stakeholders and 2) the company’s perceived competence.\(^{21}\) Depending on the industry, stakeholder sympathy can be more important to maintaining the good reputation of the company than the perception of being the most competent. As a result, when a company’s reputation suffers damage, it is usually because either its stakeholder sympathy or perceived competence (whichever is more vital to company image) has weakened.

Several variables can then damage reputation to varying extents. Reputational loss is most frequently measured in economic terms, so potential losses from breaches can be quantified in terms of abnormal churn. Within the past ten years, studies have identified that type of attack (attack vector and consequence in terms of confidentiality, integrity, and availability) and type of firm affected can cause reputational damage to wax or wane. A study of stock market reactions to data breaches from 1995-2000 found that stock market reactions vary according to the type of breach. If the breach included “unauthorized access to confidential data,” then market reactions were likely to be significantly negative.\(^{22}\) Other types of breaches did not cause any notable market reaction. Confidential data is almost always accessed and compromised when certificate


\(^{21}\) Cannon and Schwaiger 2005, 193

authorities are breached, but the market has not reacted dramatically to recent breaches, as discussed below. Significantly, publically reported data breaches in one industry through information transfer can also result in an increase in market value for firms specializing in IT security services.\textsuperscript{23} \textsuperscript{24} As a result, certificate authorities may have a degree of immunity to market sensitivity, and attacks in other industries can actually boost the reputation of IT security companies like certificate authorities by increasing demand for their competence.

Recent literature on U.S. disclosure rules for companies to report breaches discusses the topic of reputation, pointing to industry fear that reputation will be the main collateral damage from public disclosure.\textsuperscript{25} Young lists “a company’s brand strength, its market position, its ability to raise capital, its future growth capacity, its customer and supplier bargaining power, its position vis-à-vis its competition, and its customer, supplier, and investor dealings” as what every company seeks to protect from reputational damage.\textsuperscript{26} Many of these elements apply less to certificate authorities, however. Some certificate authorities are privately held, others owned by governments, and the authentication process that certificate authorities conduct is among the less visible products of the larger firms.

Reputational costs to certificate authorities can be more difficult to identify because consumers do not know much about the industry in general. To tease out Cannon


\textsuperscript{26} Young 2013
and Schwaiger’s construct for reputation with respect to certificate authorities, this paper posits that sympathy is often irrelevant or unimportant because consumers are unaware of or uninterested in certificate authorities in the first place.\textsuperscript{27} As a result, consumers do not expect certificate authorities to inspire or connect with them personally or maintain an image. Competence, however, is theoretically more important, but an attack on a certificate authority does not immediately decrease consumer confidence in certificate authority competence. Often, consumers do not have enough information about certificate authorities to become upset. This is significant because consumers are not pushing for a reshaping of the global Internet architecture or for certificate authorities to abide by international standards of order and conduct. When consumer or market accountability mechanisms do not exist, the industry does not necessarily exercise good judgment. This is especially dangerous in the case of certificate authorities since not only does the product suffer as a result of the lack of good practices, but the global Internet is put at risk.

**Current Frameworks for Measuring Reputational Loss**

Reputational damage from cyber attacks is still not completely understood, or exhaustively explained in the literature. However, a few studies create models from qualitative information to provide at least a notional idea of how attack damage can be scaled. One discussion of reputation loss to Dutch banks posits that subjectivity across most models is too high. The model uses fuzzy logic common in artificial intelligence to develop “fuzzy variables,” which are then translated through a sequence of steps into

\textsuperscript{27} Roosa and Schultz 2010, 3
This methodology uses anecdotal evidence from surveys of company respondents to create a slightly more flexible framework for measuring indirect losses. A regularly conducted Ponemon study also uses an interview structure to collect information on damage from data breaches across a wide selection of industries. The 2011 report found that indicators of reputational damage in the technology industry were consistently low at a 2.7% “abnormal churn rate,” where the churn rate represents customers that left the company only because of the breach who otherwise would have stayed. Similar results appeared across data breaches in the United Kingdom; abnormal churn rates in technology companies were at 3.4%. Both Ponemon studies noted that according to interviews, direct and indirect costs significantly decreased if the company had proactively taken steps to address their security posture before the breach occurred, notably through hiring a chief information security officer. The studies suggest that the security industry is relatively resistant to costs from a breach given the low churn rates and the significant mitigation measures that can be achieved through hiring information security-focused personnel.

Overall, the current models used to analyze data breaches all suggest that type of attack has an impact on the scale of reputational damage. As discussed above, attacks that compromise confidential data consistently result in greater reputational damage to organizations as well as a more negative market reaction than attacks that might render a website unavailable. And significantly, attacks that certificate authorities are most likely to experience, or man-in-the-middle attacks that enable “unauthorized access to

---

confidential data” such as banking credentials or personally identifiable information of end users, are supposed to cause the most severe reputational damage. However, current churn rates across the industry do not reflect reputational costs one might expect given the industry’s propensity to attacks on confidentiality.

Gaining Market Share

In 2011, Symantec publicized results from a Netcraft Secure Server Survey, which found that market share per unit of Symantec’s SSL certificates grew by more than 2 percent year-over-year.30 Symantec’s press release attributed the findings to the company’s ability to provide more “value-added services” to customers such as daily malware scans and “seal-in search,” referring to the Verisign logo that appears in search results to attract customer clicks. Symantec also notes that its Verisign seal is “the most popular and recognized security mark in the world.”

A 2004 economic study of the certificate authority market summarizes how certificate authorities work. The certificate authorities are “suppliers” selling digital certificates, or the “product,” to interested individuals and companies that are the buyers, representing the “demand.”31 This study posited that Lemons theory, first articulated by George Akerlof in 1970, should be applied to the market for certificate authorities, since sellers know more about the product they are selling than the buyers. This situation results in information asymmetry and on occasion bad product driving out the good.32

The application to the digital certificate market is that disparity in certificate quality, due to technical security, procedural, or legal differences, may not be readily apparent to all buyers, especially individuals.

Customers of certificate authorities are diverse. Large companies and state government agencies drive business to the largest certificate authorities because of their bigger reputation for customer service and trust “out of the box.” However, individuals and smaller companies also rely on digital certificates and may not understand what distinguishes a good certificate authority from an untrustworthy one. The economic literature on this topic indicates that because of this lack of information, “the market offers no incentive for the production of high quality digital certificates.”

Certificate authorities may also vary based on each market. Trust in an online retail context “is the basic element upon which trading parties develop long-term relationships.” Transaction trust, or when a customer interacts with an online retailer and completes a purchase, has been deconstructed into two key components: party trust, or the trust each party has in the other to adhere to business norms, and control mechanisms, the external third-party mechanism that increases trust in the transaction. Digital certificates serve as a control mechanism in retail transactions by allegedly providing an additional guarantee of security. However, evidence from recent studies show that digital certificates, as a third party control mechanism, have not had a demonstrable impact “on either consumer trust or purchase intention.” Notably, the trust in question is in the retailer website, not in the certificate authority itself. Yet again, certificate authorities and their digital certificates are difficult to isolate as a variable.

---

34 Backhouse, Baptista, and Hsu 2004, 1373
35 Chien, Chen, and Wu 2013, 8
36 Chien, Chen, and Wu 2013, 7
Studies of retail relationships among customers and sellers also identified that previous online shopping experiences of customers are more likely to influence their purchase intent from a particular website than control mechanisms. Initial sampling validity tests used three variations to analyze digital certificate trustworthiness: websites certified by the U.S. government, websites certified by other websites, and lastly websites that have more than one certification.\textsuperscript{37} Findings concluded that together, previous experience and digital certificates “may not directly trigger purchase intention, but do influence purchase intention via the consensus public opinion regarding the trustworthiness of the e-tailer.”\textsuperscript{38} In sum, the presence of a digital certificate in a transaction affects the reputation of the retailer, which could also shield the authority itself from reputational damage in the event of a breach.

As recent market studies demonstrate, certificate authorities do compete with each other for the best brand. However, their reputations are less at stake than those of the websites they certify. Based on retailer studies, the online retailer is more likely to suffer loss of customers than the certificate authority.

**Recent Attacks: RSA, DigiNotar, and Comodo**

This section will discuss three case studies of breaches of certificate authorities, including steps that firm leadership took to address and communicate the attacks, to demonstrate how the reputation was impacted by the breach. The case studies cover attacks in 2011 on security firm RSA and certificate authorities DigiNotar and Comodo. Damage varies across the cases, with the most unsettling consequences tied to the “unknown” loss of confidentiality and intellectual property.

\textsuperscript{37} Chien, Chen, and Wu 2013, 14
\textsuperscript{38} Chien, Chen, and Wu 2013, 8
RSA Breach

In 2011, an attack on security firm RSA used phishing and backdoor Trojans to mine data on the security company’s SecurID authentication software.\textsuperscript{39} SecurID Marketing experts contend that RSA’s brand was damaged since its very purpose in the market was undermined by the attack on its security services. RSA did not publically report the damage, but the company’s executive chairman published an online letter to customers on the company website, advising them to take a layered approach to securing their data.\textsuperscript{40} The letter also referred to the threat as an advanced persistent threat (APT), a type of attack that usually implies nation-state backing or sponsoring because of its long-term, persistent, and often expensive attacks. Other security professionals have commented that RSA may have imprecisely used this term in an effort to make the attack seem more sophisticated than it was in reality.\textsuperscript{41}

In RSA’s case, the security firm disclosed the breach to its consumers within a week of the attack, but omitted breach details, including time, length of attack, and that the company’s SecurID token technology was specifically targeted. Follow-on analysis has indicated that the unknown extent of the damage and possibility for stolen intellectual property might result in longer-term losses. Analysis of the breach in 2011 initially concluded that the key technology behind SecurID is likely safe and mitigation measures are not time-intensive or expensive.\textsuperscript{42} However, ensuing analysis revealed much more severe damage, and later in 2011, major defense contractor Lockheed Martin experienced an unsuccessful attack on its networks via stolen SecurID credentials.\textsuperscript{43} RSA had to

\textsuperscript{40} Rashid, Fahmida. 2011. “RSA SecurID Breach is a Lesson in APTs.” \textit{eWeek} 28 (7): 30-30.
\textsuperscript{41} Webb 2012, 21
\textsuperscript{42} Rashid 2011
\textsuperscript{43} Webb 2012, 21
reissue more than 40 million SecurID tokens and security experts noted that the breach may have caused permanent, significant damage to RSA’s certificate authority technology in general, which has much greater implications for the U.S. technologies that rely on it as well as consumer trust in the security industry.\textsuperscript{44}

By some accounts the RSA hack is the fourth worst attack in the current century, primarily because of the implications of lack of trust in the global Internet.\textsuperscript{45} Discussions a year later noted three main consequences from the breach: the direct loss and replacement costs to RSA for the 40 million stolen tokens, the poor judgment in delaying details about risks to SecurID, and hidden costs from reputation and other unknown losses.\textsuperscript{46} Financial losses due to reputational damage are minimal, however, even by the toughest standards of measurement and especially considering that loss of confidential data should incur the greatest degree of damage according to contemporary models of reputational loss. Three days after the breach was announced, share prices of RSA parent company EMC increased, suggesting that concern about the attack among shareholders, investors, or consumers did not directly correlate to market activity.\textsuperscript{47} By June 2011, a few months after the March attack, EMC shares had fallen about 5%, and competitors were offering incentives for RSA customers to switch to their services instead.\textsuperscript{48} Media reports emphasize the chatter over RSA’s debatable managerial response to the attack as well as the undermining of its core business, but considering the scale of the attack, the

\textsuperscript{47} Armerding 2012
ensuing incident at Lockheed Martin, and the fact that its core business was put in jeopardy, RSA showed a remarkable resilience. Executive Chairman Art Coviello increased his role in the media and the firm began strategic investments with other IT security companies. RSA also announced a change in its approach to a “defense doctrine.”

This allows a few possibilities. First, that reliance on RSA as a key underwriter of Internet security makes demand inelastic. The second possibility is that the perception of RSA’s competence only suffered in relative terms as a result of the breach, not in absolute terms. RSA’s role as an industry leader in creating essential services may have built up enough of a “competence” model for itself that even a severe attack was not enough to undo its place in the market. Fallout from the RSA breach did include “psychological damage” among chief information officers that lost faith in the security of their enterprise authentication model. However, this threat to the security model may not necessarily signal incompetence; rather, it confirms that a paradigm shift must occur across the whole industry.

**DigiNotar Breach**

Dutch company DigiNotar was another victim in the high-profile attacks that occurred in 2011. DigiNotar, a root certificate authority, issued SSL certificates to websites to guarantee their ability to complete transactions and to indicate legitimacy to users. During “Operation Black Tulip,” hackers breached DigiNotar and executed man-

---

50 Webb 2012, 22
51 Armerding 2012
in-the-middle attacks to acquire information from users and block others.  Ensuing investigations suspected a state-sponsored effort by Iran to quell dissident communications on the Internet. Hundreds of bad certificates appeared during the forensic investigation, pointing to a significant breach far beyond what the company had indicated. In fact, DigiNotar did not report the breach until 90 days after the attack and only after the integrity of the certificates was called into question by a German company. DigiNotar also allegedly negotiated with Microsoft to delay patching updates that would have revoked DigiNotar’s ability to vouch for websites, and succeeded based on the Dutch Government’s heavy reliance on DigiNotar. These delays resulted in use of these fraudulent certificates by Iranian citizens up to six weeks after the breach. By September 2011, DigiNotar’s parent company Vesco announced that DigiNotar had initiated voluntary bankruptcy.

DigiNotar was forced into voluntary bankruptcy, but the Black Tulip report revealed that basic cybersecurity practices were lacking, including poor passwords and protection from malware. Notably, the reputational loss was arguably from the poor practices the breach revealed, not necessarily the fact that the company was breached; this variable is almost impossible to isolate. The report does note that public confidence in the system was severely affected as a result of the breach, yet provides no quantitative

55 Ashford 2011, 6
56 Computer Fraud and Security 2011
57 ENISA 2011, 1
or qualitative evidence that this occurred. DigiNotar’s collection of actions confirms
that a company’s post-incident behavior can also shape how its reputation fares in the
aftermath. Worse than the RSA attack, DigiNotar’s delay in disclosing the breach
significantly affected how the media characterized the competence of the company.

**Comodo Breach**

The third breach discussed here also occurred in 2011 to a certificate authority
called Comodo that uses PKI technology to issue certificates. In the first of several
attacks on Comodo in 2011, an individual with an Iranian Internet Protocol (IP) address
who self-identified as “Comodo Hacker” acquired access from a Comodo partner account
in Southern Europe and issued nine fake SSL certificates, impacting huge sections of the
Internet. This happened because the partner account inadvertently provided Comodo
Hacker with legitimate certificates, which illustrates the problem with delegation of
certificates in the hybrid model of trust discussed earlier. Comodo Hacker supplied nine
bogus SSL certificates to websites across seven domains, including Google and Yahoo,
and also gained control of an SSL certificate for a Mozilla Firefox update server that
could have allowed Comodo Hacker to inject malicious code into an end user’s Web
browser. Comodo posted quickly about the compromise on a company blog, noting the
attack and revocation of certificates, which may have saved it reputational damage.

Presentations on the first Comodo attack at the 2011 Black Hat Conference
focused less on problems with the company itself and more on the central problem with

---

60 Mimoso 2012
the system of trust, the fact that there is no alternative to the current certificate authority system. This is further corroborated by a joint report on economic espionage by McAfee and the Center for Strategic and International Studies that compares financial loss from cyber attacks to “tolerated costs” of business; users and subscribers to certificate authorities have no choice but to rely on the system in order to conduct their transactions so tolerate the associated costs of attack. The European Network and Information Security Agency (ENISA) even stated that certificate authorities as large as Comodo are “too large to fail.” Comodo countersigns up to roughly 25% of the SSL certificates on the Internet, so boycotting Comodo would remove access to a significant portion of the Web and force a “tradeoff between connectivity and security.” Each customer trying to boycott Comodo would then have to accept permanently broken links for several websites. This suggests that even severe reputational damage, which Comodo did not suffer, might not be sufficient to turn customers away because of the market command Comodo has across the Internet. Examining the reputational consequences to Comodo after the breach confirms certain immunity to damage of this kind. At the same time, the security community widely recognized the risk even a single hacker could pose to a certificate authority with a powerful presence like Comodo.

**Conclusion**

In each of the case studies, the media reaction was that the general public’s confidence in the PKI or other trust-related service eroded, while only industry experts

---

61 Mimoso 2012
63 ENISA 2011, 2
64 Van Eijk and Arnbak 2012, 15
lost trust in the specific organizations.\textsuperscript{65} 66 Accounts in all three of these cases indicate that immediate, timely, and thorough customer communications play a significant role in minimizing indirect costs, including reputational damage. Recent analysis by industry pollsters SafeNet and the Ponemon Institute have indicated, respectively, that customers are likely to avoid a retailer that has suffered a breach and that it can take up to six months for sales to stabilize and for customers to regain confidence in company networks.\textsuperscript{67}68 However, there is insufficient evidence to suggest that attacks have a significant, long-term effect on reputation of certificate authorities specifically.\textsuperscript{69} Customers may be more likely to change their behavior in relation to the breached retailer than they are with respect to the certificate authority that issued a compromised certificate. RSA’s breach, while the most significant in terms of long-term damage and downstream impact to the U.S. economy, received relatively low levels of customer antagonism. Comodo also experienced relatively low levels of reputational damage. Even DigiNotar, which went bankrupt, was lambasted more for its lax security procedures and poor handling of its security requirements instead of the attack itself, a key distinction. This resilience of reputation signals to state and non-state actors that the public still does not understand the danger of certificate authority structure enough to proactively push for


\textsuperscript{67} “Global Survey reveals impact of data breaches on customer loyalty.” 2014. SafeNet. \url{http://www2.safenet-inc.com/email/2014/dp/GlobalCustomerSentiment/index.html#631}


\textsuperscript{69} Consumer response to Internet trust in general shows most Americans are not as informed about the risks as other national security issues. “Heartbleed’s Impact.” 30 April 2014. Pew Research Center. \url{http://www.pewinternet.org/2014/04/30/heartbleeds-impact/}
it to change. It also reinstates that the security industry in general is vulnerable, making the global communications available for exploits. Attacks may be new and threatening enough to cause surprise more than censure.

Studies of reputation across certificate authorities indicate that authorities are more likely to attract customers because of price, browser compatibility, and ease of use, not based on their reputation for security, at least with smaller customers. The current free market structure for certificate authorities is problematic, and customers of certificate authorities often do not have as sophisticated of an understanding. Therefore, customers do not have accurate means to determine or demand reputational standards from the certificate authorities, which prevents the market from self-correcting. Trust has been defined as a positional economic good; consumers are willing to pay more for more trust, which enables them to conduct more and better transactions. Trust is also “a function… of the norms of a civil society.” However, though certificate authorities engage in and support a “system of trust,” they are also the only service providers, so consumers have no choice but to trust them. Van Eijk and Arnbak contend that the Comodo and DigiNotar breaches, among others, demonstrate this in practice by leading to a “collapse of trust in HTTPS communications.” And for the time being there is no immediate alternative system available.

---

73 Van Eijk and Arnbak 2012
Analyzing Transnational Shadow Industries

Because the media describes the current market for certificate authorities as a shadow industry, where the power of reputation is not fully utilized, it is worthwhile to compare it to other industries with similar problems to identify similar solutions. Here, this section examines private security companies, which often combine “formerly military or police functions” to provide “many different military and security services ranging from fighting wars to logistics.” These companies face criticism over their inscrutability, their slow encroachment on state sovereignty, and nebulous codes of ethics and conduct.

Private Security Companies

While certificate authorities are virtual in nature, they are also a global community, and similar to private security companies, the system of trust supported by certificate authorities is a separate layer of infrastructure and processes that supports key national transactions. Despite each nation’s desire to ensure security of its transactions and maintain state sovereignty, this sovereignty is directly dependent on the global authentication system. Governments have incentives to act as certificate authorities and sign their own certificates to reaffirm their sovereignty, but this also increases the diversification of certificate authorities, exacerbating the single point of failure problem. A few U.S. government departments and agencies act as certificate authorities, including the Departments of Defense and Homeland Security. As of 2010, the Electronic Frontier Foundation SSL Observatory had identified 46 countries acting as legitimate

---

75 EFF SSL Observatory 2012
certificate authorities, and many more countries that owned subordinate certificate authorities.

Countries can also theoretically sponsor certificate authorities while not owning them directly, similarly to countries that contract private security companies to conduct operations potentially outside the scope of state foreign policy tools. In 2010, Soghoian and Stamm identified the possibility for a “compelled certificate creation attack,” where a nation-state could take advantage of the confusing jurisdictional boundaries for certificate authorities and force a certificate authority to issue a false certificate with the express purpose of allowing surveillance on the country’s citizens or other intelligence activity. In 2010, Web browser Mozilla gained media attention when it debated whether to allow independent Chinese company China Internet Network Information Center (CNNIC) in its list as a trusted authority, thereby allowing its immediate acceptance by Firefox and other Mozilla technologies. Mozilla eventually accepted CNNIC based on results of its evaluation of the certificate authority. Much of the consternation around CNNIC was due to suspicions that the Chinese government would be tempted to direct activities of CNNIC to include surveillance and potentially man-in-the-middle attacks against U.S. sites that bought CNNIC’s certificates. This tension illustrates the difficulty with state-sponsored certificate authorities that could potentially observe citizens with the implicit backing of the country, meaning that domestic surveillance and other observation is not necessarily limited to the state.

---

Private security companies and certificate authorities may have a small number of main clients. For example, U.S. websites will seek certification by U.S. certificate authorities in most cases, but all have the option to pursue certification by authorities around the world. As a result, certificate authorities have a broad client base that can include democratic and authoritarian states and state-sponsored organizations, making potential international regulation complicated. Even U.S. regulation would be difficult because each company is globally distributed and staffed. Regulation of U.S. certificate authorities might also push customers to seek certification from foreign authorities, negatively impacting the U.S. market and increasing demand for authorities that are not held accountable to the U.S. standards of conduct that do exist.\(^78\) As of 2013, no search in the U.S. congressional record reveals any proposals to regulate the market.

Private security companies have a similar dilemma. International regulations apply to private security companies, but the transnational nature of the industry makes enforcement elusive.\(^79\) Individual employees can contract from firm to firm, so their transnational, transient nature makes regulation difficult to implement at the organizational level. Scholars of private security companies note that the current market incentives structure complicates self-regulation; because government regulation is unlikely, the companies feel less pressure to self-regulate as a better alternative. In addition, the legal framework for private security companies is vague; the smattering of international employees, contracts, and lack of standards means that no national law has

\(^{78}\) Van Eijk and Arnbak 2012).

\(^{79}\) de Nevers 2009, 487
teeth. Vague legal language around certificate authority authentications means that end users and websites are similarly in the dark.\textsuperscript{80}

**Possible Lessons from Private Security Companies**

Like certificate authorities, private security companies are a “generic” industry and “generally [distanced] from the public.”\textsuperscript{81} Up until the past few years, only key incidents have highlighted and shaped the industry in the media. Private security companies do not share a “community of fate,” which means they lack an incentive to band together for the good of the industry. Certain bodies of standards do exist, but they are not universally implemented. Certificate authorities share many of these characteristics, including the lack of interdependence as a community, despite the “fate” they all share. This is due to the diversity in authorities; governments and private companies large and small make up the more than 650 current certificate authorities in existence, which have little in common with each other in most cases.\textsuperscript{82} Recent attempts by certificate authority market leaders are just starting to focus on education and best practices through additional bodies such as the Certificate Authority Security Council, however, which will work to create a more cohesive community.\textsuperscript{83}

Geographically collocated certificate authorities likely experience the community of fate more. WebTrust is the primary standard body for certificate authorities in North America, and while its membership and influence have increased, it is still relatively small compared to the size and geographic distribution of the industry. WebTrust members undergo evaluation by accountants that verify whether they meet standards of

\textsuperscript{80} Roosa and Schultzze 2010, 7
\textsuperscript{81} de Nevers 2009, 501
\textsuperscript{82} Van Eijk and Ambak 2012
“adequacy and effectiveness.”84 85 Once a member passes, it can bear the WebTrust seal. WebTrust is also a step towards involving end users in e-commerce decisions; recent studies found that consumers are more likely to engage in online transactions with both known and unknown businesses if they bear a WebTrust seal, and that revocation of a seal can have deleterious effects on consumer behavior.86

While the studies focused mainly on behavior in business-to-business and business-to-consumer e-commerce, potential implications for certificate authorities have yet to be fleshed out. Establishing standard bodies like WebTrust in other countries opens the door to cooperation across the bodies in an effort to develop international norms for behavior and a stronger system of accountability. Even if nation-based bodies proliferate, though, users are vulnerable to untrustworthy certificate authorities elsewhere in the world. Increasing openness, transparency, and public awareness about the role that both the certificate authority and private security industries play is also key to putting more pressure on individual companies.87 Playing on the competitive nature of each industry would include pushing for emergence of market differentiators, or identifying incentives that would influence industry members to subscribe to a certain set of standards and thereby set themselves above the competition.

84 WebTrust 2012
85 Evaluation includes several categories, including Business Practice Disclosure, Service Integrity, Environmental Controls. Full documents for evaluation can be found here: http://www.webtrust.org/homepage-documents/item54279.pdf
As a “transnational service industry,” private security companies have the flexibility to change location according to the attraction of national laws. Certificate authorities share this same characteristic. For example, if the laws of the United States are too restrictive, a certificate authority can “move abroad, or melt and reconstitute itself differently to avoid them.” Problems with consumer-based pressure on private security companies include unreliable consumer competence, insufficient information, and the “difficulty in communicating customer purchasing intent,” all of which plague certificate authorities too. Proposed solutions to improve the unregulated private security company market include developing norms of professionalism across the industry, or allowing the few large market leaders to form an oligarchy and enforce barriers to entry. Entities like WebTrust also represent the type of “occupational organization” recommended for private security companies to monitor and test behavior of member companies.

However, WebTrust is only a North American organization; in order to avoid some of the problems previously discussed, the occupational organization would have to be supported as an international body and work with international member companies. Due to complexities with confusing demand across diffuse public and private sector consumers, a producer-focused approach is perhaps the most effective way to significantly change the market for private security companies. Parallels across the two industries confirm that efforts underway for certificate authorities to create awareness and community may make some strides ahead but may be limited in scope and efficacy until a greater international community is established.

89 Chesterman and Lehnardt 2007, 187
90 Chesterman and Lehnardt 2007, 193
A Path Forward

Based on the economic and political analysis of certificate authorities, the most effective international community would focus primarily on shaping producer behavior. Long-term solutions could include developing regional databases that track issuance of certificates, similar to digital rights management servers that track data assets and usage. A technical solution of this scale would take years and significant resources to produce and would require cooperation across the certificate authorities in a particular region. In the meantime, strengthening private bodies like WebTrust and the Certificate Authority Security Council, and establishing similar third-party rating organizations in other regions could help develop an international community around certificate security. The accounting community, which manages WebTrust, provides the basic framework necessary for an accountability structure in North America. To increase the influence of WebTrust, North American governments could endorse market-based incentives to encourage certificate authorities to achieve the WebTrust seal.

Market mechanisms will also conceivably vary by country. While U.S. companies and individuals rely on certificate authorities that trusted third party or content providers have approved, other nations may not place equal trust in the same large service providers. Regional solutions are slowly emerging with the appearance of auditing mechanisms like WebTrust, but in order to increase international reliability of certificate authorities, more changes must happen. This organization must be able to withhold licensing or other marks of approval based on mutual understandings of what constitutes high quality digital certificates, and buying lower quality certificates should become less

---

appealing. Previous suggestions across the literature have included leveraging existing financial services rating agencies such as Standard&Poors to expand into the digital certificate market.\(^{92}\) Demand for rating services may increase with future incidents that compromise digital certificates; the greater the damage, the more interest may eventually develop in how certificates are issued. International organizations such as the World Trade Organization and even national regulators such as the Federal Trade Commission should also extend their portfolio to certificate authority evaluation and impose an antitrust structure so that no certificate authority alone is “too big to fail” like in the case of Comodo.

**Conclusion**

The system of trust has significant ramifications for U.S. security in the next decade. Technology is evolving rapidly, and damages from cyber exploits on certificate authorities to date are not even fully understood. Unless the security community, including the U.S. government, architects the system of trust to allow agile response to attacks from malicious actors, security of global communications will harbor a strategic vulnerability. Identifying and communicating the problem would be an effective first step towards enabling agile response.

The security community, including Internet service providers, content providers, standards bodies, and even national government, can develop technical, market, and policy changes with the goal of incentivizing good behavior. For example, technical changes can begin with defining a quality digital certificate, which would assist in establishing a baseline for good behavior. Market changes can include equipping third

\(^{92}\) Backhouse, Baptista, and Hsu 2004, 1374
party organizations to censure or reward certificate authorities for quality of their certificates. Policy changes can include encouraging information sharing exchanges and participation in international fora, where certificate authorities can share anecdotal information on attacks and vulnerabilities in digital certificates to inform security practices across the community.

Members of Internet governance bodies have collaboratively addressed cyber threats before, such as the Conficker malware. Creating similar task forces focused on security of digital certificates would help make this issue a priority. Because of the market power U.S. companies currently wield and the strength of North American accountability mechanisms, the U.S. is a strong candidate to drive work on this issue. A possible solution might consist of a version of WebTrust 2.0 that grades certificate authorities on quality and is internationally recognized as the authority, most importantly by the largest certificate authorities with the highest quality ratings. While certain government institutions might resist adhering to WebTrust requirements, their resistance would provide the opportunity for bad press to highlight governmental noncompliance. At the same time, a standing international working group, potentially as part of the technical Internet Engineering Task Force (IETF) should convene to focus on the issue and encourage members to help drive national awareness efforts.

Solutions must recognize that the certificate authority industry is currently and uniquely resistant to reputational damage, while at the same time there is little brand recognition around who the certificate authorities are. Any policy solution should take this economic reality into consideration; prescriptions urging more or less of a focus on reputation need to consider the starting point. This paper examined issues of reputation
across three case studies and reviewed another example of another industry in search of the right incentives to improve its global structure. Creating bodies of standards and other community approaches are a step in the right direction, but both of these solutions will need to accommodate the resilience to reputational loss that is currently characteristic of these companies. As attacks increase and the media becomes more adept and interested in discussing issues of Internet security, including certificate authority security, consumer education may eventually result in greater pressure on the industry and more direct effects of reputation on market behavior. Before this occurs, the standards bodies and other producer-focused efforts need to tailor efforts to account for and change the industry’s resilience to reputational damage.

Changes are coming for the system of trust. The security community is currently discussing new models to replace the entire framework of certificate authorities, including convergence, where authentication would occur between the end users and notaries, replacing certificate authorities completely. This solution might only transfer the risk to different parties instead of mitigating it, but the system would be more flexible and would eliminate the single point of failure problem endemic in certificate authorities. In the meantime, however, certificate authorities are freshly in the public eye and squarely under security community scrutiny due to recent attacks. Before a new system becomes a widely implemented element of Internet architecture and governance, efforts to address certificate authority security will need to include alternatives to reputational pressure.

93 Mimoso 2012
CHAPTER 2: ROUTING SECURITY AND TRUST IN THE INTERNET

Internet routing is widely accepted as one of the core functions of the Internet that enables information to travel across the world. Every data packet carries specific information, of a specific size, and is routed to a specific destination. The Internet’s physical infrastructure enables the virtual layer of the World Wide Web (web) along with multiple other uses. In recent years, while use of the web has grown exponentially, Internet use has also diversified to include intelligence surveillance, mobile phone use, big data analysis, and an upsurge in personal data applications, among other purposes. The Internet is now performing functions it was never designed to perform when it was first born in 1969. Because of these evolving demands on and uses of the Internet routing infrastructure, cyber incidents are also resulting in different, and more significant, consequences. As a result, solutions to secure routing infrastructure must evolve to address the increasing demands and threats. This paper hypothesizes that intentional attacks on routing infrastructure are likely to increase, and current solutions do not sufficiently account for threats from nation states or how modifying the degree of trust among routing entities will affect long-term security.

Border Gateway Protocol (BGP) is the main standard of communication that routers use to facilitate movement of data packets across the Internet. BGP also enables each data packet and router to stay anonymous during these exchanges of data. BGP is a widely used but voluntary protocol that allows separate networks to exchange information with each other according to contracts and localized policies. As such, BGP

---

is the “glue” that binds the various network connections together. Protocols like BGP are inherently based on trust; BGP trusts each router to capably and reliably perform so that data goes where it is intended. This model must work in order for the Internet routing infrastructure as a whole to remain trustworthy.

In recent years, cyber incidents have revealed significant vulnerabilities in and threats to routing infrastructure. In response, researchers are attempting to evolve security solutions along with the threats. Complicating the development of secure routing and secure BGP is the fact that no central authority governs the entire collective of routing protocols. In the absence of a hierarchical authority, changes to routing protocols and norms are simply voluntary and incumbent on each individual entity to implement. Researchers have also referred to BGP as “the Achilles heel of the Internet” because of its primary importance to Internet functionality combined with its innate flaw.

History demonstrates that the increasing vulnerabilities in routing infrastructure are likely to be exploited and also require an evaluation of the trust model for BGP. This chapter first outlines the background of routing security and emerging vulnerabilities in the routing infrastructure. A review of existing literature examines debates over the key vulnerabilities and mitigation technologies, and identifies remaining gaps that solutions have not yet addressed. The chapter also includes a case study of intentional attacks that

---

99 CSRIC 2013, 3
100 Ortiz 2009, 22
targeted routing infrastructure, and analyzes solutions to these types of attacks in the context of trust. In conclusion, the paper argues that current technical solutions to BGP vulnerabilities are insufficient to address the potential threat from nation-state or other well-resourced, persistent actors. Solutions must include political and social levers to increase the resilience and trustworthiness of routing infrastructure.

**Background: Overview of Internet Routing**

Before describing the weaknesses in routing, this section will first provide an overview of routing functionality. The basic architecture of the Internet is made up of networks of routers and links connecting numerous hosts. An Autonomous System (AS) is a “unit of routing policy” that represents a single network.¹⁰² The Internet Assigned Numbers Authority (IANA), an organization under the Internet Corporation of Assigned Names and Numbers (ICANN), assigns address blocks to five regional Internet Registries (RIR), located around the world. Each address block includes sets of unique 16-bit Autonomous System Numbers (ASN), which RIRs can assign to individual ASes. The five RIRs determine which ASes, which can include commercial ISPs, are eligible to receive which ASNs. Once an AS receives its ASN, it can then sign agreements about which routing paths it will use for its address space. ASes are administered by one or more individuals, organizations, or other network operator(s), and can vary in size from representing small enterprises to a “nationwide backbone network.”¹⁰³ In 2013, more than

---


43,000 active ASes appeared on the Internet. IANA has the potential to assign over 65,000 unique ASNs.\(^\text{104}\)

The structure of ASes is inherently hierarchical and a pyramid. The largest ASes on the Internet sitting at the top of the pyramid are a small group of U.S. ISPs with near perfect connectivity to each other, often referred to as the “core.” The next band of the pyramid are other large US and European providers with “very rich connectivities to the core.” Lastly, making up the largest, bottom band of the pyramid, are the numerous smaller providers.\(^\text{105}\) Hierarchy is inherent in the ways that Internet connectivity is facilitated from the core ISPs to the smaller, dependent ASes. Address allocation also works through a hierarchy, with IANA distributing authority to RIRs, which in turn enable smaller ISPs and organizations. This hierarchy was originally intended to make address allocation scalable and flexible to accommodate regional policy needs.\(^\text{106}\)

Through this structure, RIRs are able to tailor their activities to regional politics and technical requirements.

While IANA exerts some managerial authority in its distribution of AS numbers to RIR address blocks, no national- or international-level entity regulates how routing policies are developed or governed.\(^\text{107}\) Compilation of routing policies does occur to a limited degree. ASes freely submit routing announcement and filtering information of their own accord to Internet Routing Registries (IRR), which are globally located routing policy databases often operated by RIRs. IRRs store and disseminate routing


\(^\text{106}\) CSRIC 2013, 19

\(^\text{107}\) Mueller, Schmidt, and Kuerbis 2013, 92
announcements based on these submissions, thereby creating a voluntary system of updates.¹⁰⁸

Internet routing protocols guide how routers move data within and across these networks to their destinations. To move data inside a single network, ASes follow intra-domain routing protocols such as Open Shortest Path First (OSPF) and Routing Information Protocol (RIP). Inter-domain routing protocols, specifically Border Gateway Protocol (BGP), govern how this traffic is sent from one AS to another.¹⁰⁹ Most ASes use BGP in order to maintain compatibility with peers, providers, and customers, and adhere to local jurisdictional law, but the protocol itself is voluntary.¹¹⁰ The AS will generally choose the best route based on the intra- and inter-domain protocol topology, and will then establish commercial agreements with other ASes, including among peers and between customers and providers, for how to use each other’s networks to move traffic.¹¹¹ Because BGP allows these localized agreements and policies, it effectively enables ASes to work together in flexible ways that prioritize profit. However, this same flexibility also creates vulnerabilities since people can create bogus routes and no overseer monitors which policies are legitimate.

AS routing policies also exhibit common preferences. In a hierarchical provider-customer relationship, a customer AS will pay its provider AS for access to the Internet, whereas in a peering relationship, peer ASes freely provide connectivity to each other’s customers. Each of these preferences is driven by economic incentives, since each AS is most likely to choose the path that incurs the least cost. Smaller ASes can depend partly

¹⁰⁸ Mueller, Schmidt, and Kuerbis 2013, 92
¹⁰⁹ Dolev 2006, 3184
¹¹⁰ Mueller, Schmidt, and Kuerbis, 2013 92
¹¹¹ Gao 2014, 1583
upon large backbone networks for Internet access. Providers direct traffic to numerous routers that follow many different routing policies. Altogether, this system constitutes “policy-based routing,” where an AS will choose a path that conforms to its policies though it might not always be the shortest path. Shortest paths usually mean faster service and are less vulnerable to interception, but they are not always conducive to the commercial agreements in place. This means that policy ultimately takes precedence over performance. The route that conforms to an AS commercial agreement will be the more desirable route, even if it uses a longer path to move the data.

ASes will use longer routing paths in a few difference circumstances, including for political and economic reasons. In the late 1990s, more than 70% of all Internet traffic flowed across ASes in the US. As of 2008, according to some estimates, the US carries only 25% of all global Internet traffic. As more countries build their information and communications technology (ICT) infrastructure and become more “wired,” countries are beginning to be wary of having their data traverse across infrastructure in other nations. If relations with these countries are adversarial, if they are rivals, or if they are perceived as more likely to conduct surveillance on traffic, the originators of the data will be less inclined to send traffic over other national networks. Economic policies, including tariffs and pricing anomalies, also influence which routes ISPs use. In some cases, small ISPs will enter into agreements with international ISPs and follow much more circuitous routing paths to avoid engaging with a nearby competitor.

112 ITSRA 2009, 59
113 Dolev 2006, 3185
115 Markoff 2008
Content providers are also moving content closer to end users, since data requests are increasingly for videos and other large data files. Providing connectivity to these large files will often require use of longer routing paths, which has consequences on routing effectiveness and security, since studies indicate that multiple links in a network tend to result in network failure.\textsuperscript{116} Furthermore, prioritizing routes and setting up filters to determine likely AS paths is unfortunately insufficient to guarantee routing stability.\textsuperscript{117} As the next section will illustrate, vulnerabilities can increase as routing paths lengthen.

**Literature Review**

**Routing Vulnerabilities**

When U.S. engineers originally developed BGP, they intended the protocol to maintain flexibility and resilience across military networks in case one of the routers or switches lost operability.\textsuperscript{118} However, vulnerabilities within inter-domain routing are well documented. Prefix hijacking is one of the most prevalent incidents that can occur due to BGP vulnerabilities. Intentional and unintentional actions by network operators can result in prefix hijacking, whereby an AS sends out routing policy to a network over which it has no authority. When this happens, data in transit does not reach its destination at all, or it reaches the wrong destination.\textsuperscript{119} Disruption in routing traffic occurs most often when an actor unintentionally compromises an individual router, which then sends out misinformation to other routers. Misinformation can include dictating an incorrect routing path which could send traffic to another location instead of its original

\begin{footnotes}
\footnotetext[116]{Gao 2014, 1592}
\footnotetext[117]{Gao 2014, 1591}
\footnotetext[118]{ITSRA 2009, 59}
\footnotetext[119]{Mueller, Schmidt, and Kuerbis 2013, 92}
\end{footnotes}
destination.\textsuperscript{120} A compromised router can result in significant changes to the rest of the Internet if it is located in a certain part of a network, since misinformation added to one BGP router’s routing table would be propagated across all of its peers. When a compromised router drops information completely, the information is “blackholed.”

The most significant incidents of global route hijacking to date have been unintentional. Pakistan and China vividly demonstrated consequences from global route hijacking in their attempts to control internal dissidents by blocking access to certain websites.\textsuperscript{121} Due to routing misconfigurations, both countries ended up shutting down access to YouTube and other websites, respectively, for a significant percentage of global users. Widespread views in foreign policy and technology policy circles agree that “Internet censorship is becoming a global norm,” so as nations increasingly rely on blocking access to subdue internal unrest, there may be an uptick in unintended consequences to global routing.\textsuperscript{122} As of 2009, unintentional hijacking was not illegal in any national or international jurisdiction, and the worst penalty that could occur if an entity accidentally hijacked a route was that it might be dropped from other routing paths.\textsuperscript{123}

In two separate occurrences in 2002 and 2003, the entire UUNet AS went down.\textsuperscript{124} As the largest AS on the Internet at the time, the UUNet incidents present a rare but insightful look at the consequences of a large-scale routing failure. The first incident was due to a routing software failure and the second to a distributed denial of service

\textsuperscript{120} Ortiz 2009, 22
\textsuperscript{121} ITSRA 2009, 60
\textsuperscript{123} Pilosov and Kapela 2008
\textsuperscript{124} Dolev 2006, 3183
(DDoS) attack. Seminal studies on routing infrastructure have demonstrated that deliberate attacks on the most central nodes of the Internet would result in severe consequences for connectivity across the web, and that “hidden backup links” between ASes would add to Internet resilience as a whole. However, much of the literature agrees that Internet resilience to deliberate attacks on critical nodes is low, and the Internet is susceptible to deliberate attacks on these nodes. Models show that an attack targeting only the top 0.5% of available ASes would cause significant decreases in reachability and connectivity across the Internet.

Given the increased interest in global Internet infrastructure and state experiments with censoring Internet communications inside national borders, intentional threats to the routing infrastructure may be increasingly likely. In 2009, a group of private sector subject matter experts from the Information Technology (IT) Sector worked with the Department of Homeland Security (DHS) to develop the IT Sector Baseline Risk Assessment (ITSRA). The ITSRA identified “Provide internet routing, connection, and access services” as one of six critical functions for the IT Sector. While unintentional threats to routing infrastructure had a high likelihood at the time the group published the report, the assessment identified “partial or complete loss of routing capabilities through a manmade deliberate attack” as the highest-consequence risk to internet routing infrastructure. The ITSRA used criteria of “national and economic security and public health, safety, and confidence” to determine that loss of routing capabilities would result in the most severe consequences relative to the rest of the sector’s risks. The likelihood

125 Dolev 2006, 3184
126 Dolev 2006, 3194
127 ITSRA 2009, 6
128 ITSRA 2009, 61
of this risk was low in 2009, but recent incidents and political developments may raise the likelihood of this risk.

Several self-regulating mechanisms make the stability of routing infrastructure effective most of the time. ISPs have economic incentives to maintain credibility, since their reputations result in increased peering agreements and numbers of paying customers. ISPs have financial incentives to maintain compatibility with each other and to avoid propagating bad routing information. Due to the voluntary nature of self-regulation, however, not all ISPs participate in the same ways: generally the larger providers dictate which routing policies are acceptable and which information is legitimate. Smaller providers follow suit. Because no central entity governs routing configurations or policy content, network operators in ISPs of any size can make configuration mistakes that expose vulnerabilities in the infrastructure to malicious threats. When they occur in the larger ISPs, the propagation can be much more extensive.

Solutions

In 2011, the Communications Security, Reliability, and Interoperability Council (CSRIC) acknowledged that “Over the years, this trust [among operators of gateway routers] has been compromised on a number of occasions, both accidentally and maliciously, revealing fundamental weaknesses of this critical infrastructure.” As the technical and research communities woke to the possible consequences of routing infrastructure vulnerabilities, the schools of thought on BGP security diverged into different views. For the purposes of this paper, this section will divide the schools of thought into two camps: those that advocate a more hierarchical structure featuring a
single trust root, and those that advocate a more decentralized model based on increased accountability for all participants.

*Advocacy for a Central Root of Trust*

The core argument in favor of a root of trust is that only a centralized governing mechanism over routers would provide authorities with the accountability required for wide network operator participation. The research and security communities have discussed various tools to increase BGP security, mostly focused around mitigating BGP vulnerabilities that can result in unintentional route hijacking. From 1998, the security community has widely recognized the importance of cryptography in protecting data in transit, even if protecting BGP is still not fully understood.\(^{129}\)

One of the most viable cryptography-based security solutions discussed thus far is Resource Public Key Infrastructure (RPKI), a tool that would apply a hierarchical verification system to routing, requiring approval of various routing announcements.\(^{130}\) RPKI would endow the commercial ISPs, or other holders of Internet Protocol (IP) address blocks (prefixes), with the ability to issue certificates in order to authorize which routing announcements could be sent out over its network.\(^{131}\) In this way, RPKI would align certificate authorization to IP address allocation. This function would therefore make IP address block holders a “trust anchor.” Each network operator would then be able to trace the certificates back to the trust anchor to verify that a legitimate entity had issued the certificate.

\(^{130}\) Mueller, Schmidt, and Kuerbis 2013, 93
\(^{131}\) Mueller, Schmidt, and Kuerbis 2013, 94
The CSRIC Working Group recommends that the RIRs work together with the address allocation authority, IANA, to establish a single “root of trust” for RPKI.\textsuperscript{132} Only a single root of trust (or trust anchor, used interchangeably here), would be able to mediate conflict among ASes, which the CSRIC contends are incapable of doing by themselves. The single root of trust would also prevent ASes from declaring ownership of address space they have no claim to, and would be able to assist RIRs in incident management or other issues that require pooling of common resources. Notably, CSRIC recommends that network operators maintain their autonomy in setting and communicating their own routes, and waiting until they have sufficient trust in RPKI before reconfiguring their routers to obey RPKI filtering.\textsuperscript{133} An alternative would be for each network operator to individually verify routing information, but this decentralized model would impose much higher costs.\textsuperscript{134} RPKI is most effective in filtering out unintentional route leaks, but since it only focuses on the source of the announcement and not the entire path the announcement travels, would likely be insufficient to address intentional attacks.\textsuperscript{135}

"Pretty Good BGP (PGBGP) was introduced in 2006 to simply delay ASes from accepting new paths. In simulations, delays provided ASes enough time to verify announcements and prevent propagation of bogus routes.\textsuperscript{136} The researchers proposing PGBGP considered it a “simple, incrementally deployable modification to the BGP decision process” since it does not change part of the protocol itself, merely how ASes

\textsuperscript{132} CSRIC 2013, 18
\textsuperscript{133} CSRIC 2013, 20
\textsuperscript{134} Mueller, Schmidt, and Kuerbis 2013, 94
\textsuperscript{135} Doerr et al. 2012, 25
use it. PGBGP would theoretically treat a path with “suspicious edges” as an anomaly and impose a delay. Secure BGP (SBGP) then emerged in order to hold routers accountable through a signature-based technology where routers authenticate announcements a hop at a time, but the memory and resources necessary for routers to sign are prohibitive.\textsuperscript{137}

BGPSEC, a security project of the Internet Engineering Task Force (IETF), attempts to address the gaps in RPKI by combating “unauthorized insertion or deletion of ASNs to falsify the recorded sequence of ASNs transited along the route.”\textsuperscript{138} BGPSEC would encrypt the routing announcements in addition to verifying the originators of the announcements. Verifying each ASN within a particular route would signal to other ASes whether the route had been compromised.

A 2013 working draft of the IETF identifies circumvention of RPKI as a way of conducting a man-in-the-middle attack against BGPSEC. According to the draft, similar attacks number over 9.6 million occurrences since 2007.\textsuperscript{139} The SIDR Working Group also published Security Requirements for BGP Path Validation in July 2014, which may be a significant step towards a solution. Working Group members noted that the work still does not address route leaks, and agreed on next steps towards detection and notification.\textsuperscript{140} Much of the corresponding pushback from network operators on BGPSEC is due to the increased complexity and hierarchy that BGPSEC would enforce on

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{138} CSRIC 2013, 14
\end{enumerate}
\end{footnotesize}
The literature notes that SIDR solutions are often in pursuit of the most “technically simple and unambiguous” solution, at times at the expense of governance concerns.

**Opposition to the Central Root of Trust**

The other camp appearing in the literature decries the creation of a single root, for reasons both technical and political. In the international system, states are subtly expanding their roles from blocking internal access to Internet content to “[normalizing] control and the exercise of power” in cyberspace. Deibert and Palfrey describe this shift as a change in cyber conflict’s “center of gravity,” and forecast that states are no longer satisfied with trying to control the Internet within their borders, but are now developing advanced technological capabilities that will confer more power on them in the international system. New generations of Internet controls are under development, which will enable a wide range of activity on international networks and which states ultimately intend to “shape and influence” people instead of merely censor incoming content. All of these trends are prompting states to pursue a “security first” norm in Internet governance.

Kuerbis and Mueller argue that allocating new powers to a root of trust, or even a small community of trust roots, would allow manipulation of power to revoke access.

---

144 Deibert et al. 2010, 7
145 Deibert et al. 2010, 11
Early developers of RPKI intended for the RIRs to serve as the trust anchors and empower network operators to authorize their routing paths and information.\textsuperscript{146} Because RPKI relies on and would newly apply a hierarchical system to routing, however, it could potentially open the door for certain holders of these address blocks to acquire more power by withholding or providing certificates.\textsuperscript{147}

A hierarchical security solution for a hierarchical structure presents challenges. The RPKI solution, for example, caused fears of potential regulatory requirements as well as suspicion of the RIRs and IANA gaining too much power over the chains of users below them. At the time this paper was written, IANA’s parent organization, the Internet Corporation for Assigned Names and Numbers (ICANN) had announced that at the expiration of the IANA contract, ICANN would transfer IANA’s functions from the U.S.-based organization to the international community once an acceptable proposal had been established. The U.S. government announced support for the multistakeholder system of Internet governance and did not indicate whether ICANN would become the single trust root conductive to RPKI deployment.\textsuperscript{148}

Centralization of power raises significant concerns across the academic community about how nation states would try to influence the root of trust as well as the providers below the root. Nations with authoritarian forms of government could assert legal ownership of the certificates and exercise control in many possible ways.\textsuperscript{149}

Members of the IETF SIDR working group also raised the possibility that a country

\textsuperscript{146} ENISA 2012, 25
\textsuperscript{149} Mueller and Kuerbis 2013
“holding the keys” could conceivably use that power to their advantage in a conflict by revoking other nations’ access. At the same time, it would strip ISPs of some of their autonomy, since some of ISPs’ usual functions would be ceded to the new root of trust, and their services could theoretically be shut off in case of non-compliance. In short, the scholarship against the single trust root contends that RPKI would provide a major new dependency and vulnerability for ISPs.

In addition, recent attacks on certificate authorities highlight the risks with trust anchors. Granting certificate issuers more power over Internet functionality while they are still poorly understood would likely open the door to additional threats and transfer the lack of accountability to a smaller community. If a trust anchor that uses RPKI were compromised, a malicious actor could usurp the authority’s power to sign any prefix and blackhole traffic around the Internet.

The national and international opposition and outrage in response to recent U.S. National Security Agency surveillance activities also indicate the likely reluctance of many to grant such a large amount of power to a single root of trust. Allowing one or a small number of entities to visibly manage large segments of the Internet would risk political support and potentially make them bigger targets for malicious actors. In sum, the political environment may not be conducive to a single root at this time.

These various cryptographic solutions do not address the insertion of political goals into route hijacking. If nation states are granted more power in relationships with ISPs, then a compromised provider may still allow a government insight into the traffic on its network even if the data is encrypted. Developing a single root of trust to manage

---

150 Kuerbis and Mueller 2011, 136
151 Kuerbis and Mueller 2011, 133
152 ENISA 2012, 26
inter-domain protocols would provide oversight and accountability for the routers and ASes, but it is not completely clear how the root of trust itself would remain impartial or immune from external influences. Rather than mitigating the vulnerability, the solution of a single root of trust may simply transfer the vulnerability to a more centralized entity.

An overview of dominant technical solutions highlights that the security community is still focused mostly on motivating good behavior among routers and ISPs. Both camps fall short of the final solution since this conversation is still ongoing. Those advocating a single root of trust identified the need for a third party to provide judgment on which entities are not performing well, but the implications of a root of trust frighten those wary of a regulatory regime and of nation-state manipulation. Notably, recommendations and increasing adoption of security solutions such as RPKI are primarily in response to unintentional route hijacking; only nascent efforts exist to protect against deliberate route manipulation by malicious actors. Those advocating for a distributed model of trust identify the risk of nation-state interference, but have no solution for a reliable accountability mechanism for when market dynamics are insufficient to compel good behavior. Technical solutions to reinforce market dynamics and protect data must impose constraints on states in addition to individual operators.

Case Studies

Most of the news and literature on routing infrastructure has focused on state censorship attempts unintentionally resulting in route hijacking. This section will discuss some of the recent attempts at deliberate redirection of routing paths. These types of attacks are different from others in the sense that they do not target a particular BGP flaw, but “simply [take] advantage of the fact that BGP’s architecture is based on
trust.” In 2009, researchers presented a slide deck at the DEFCON conference showing how a malicious actor could deliberately redirect traffic through other ASes. Researcher Alex Pilosov and his team also emphasized how these types of attacks are unlikely to be noticed “unless you’re looking for it.” Examining a spate of 2013 incidents provides insight into emerging deliberate exploits on routing infrastructure: various successful attempts rerouted data to Belarus and Iceland, among other locations. This case study was chosen because to date, it is the only open source example of a persistent attempt to reroute traffic for purposes other than domestic censorship since the possibility was first presented at DEFCON in 2009.

Belarus and Iceland

On November 19, 2013, U.S. “Internet intelligence” firm Renesys blogged about its discovery of systematic man-in-the-middle (MITM) attacks, a form of route hijacking, in order to deliberately exploit BGP vulnerabilities. Renesys identified 13 hijacking incidents in 2013 where unknown actors rerouted data through Belarus in February and May, and 17 incidents where data was rerouted through Iceland in July and August. Attackers around the world hit more than 1,500 IP blocks in these attacks. Traffic to and from targets including “financial institutions, [Voice over IP] providers, and world governments” was rerouted, inspected, and then passed along to the original

153 Zetter 2013
154 Pilosov and Kapela 2008
155 “A man-in-the-middle attack is one in which the attacker intercepts messages in a public key exchange and then retransmits them, substituting his own public key for the requested one, so that the two original parties still appear to be communicating with each other.” Search Security. http://searchsecurity.techtarget.com/definition/man-in-the-middle-attack. Accessed 20 July 2014.
157 Cowie 2013
destinations.\textsuperscript{158} By routing traffic away from its regular paths and through Belarus and Iceland instead, these detours created opportunities for malicious actors to monitor, intercept, or even modify the traffic before sending it along. Others in the security community posited that malicious actors may be “honing their technique” to prepare for other MITM attempts in the future.\textsuperscript{159}

Renesys identified two separate ASes, Beltelecom in Belarus and Siminn in Iceland, which hijacked routes in patterns that appeared like deliberate attempts to observe or tamper with traffic. Renesys traceroutes determined that data originally intended for California left New York and took a detour through London, Russia, Belarus, Germany, and finally back through New York on its way to Los Angeles. Similarly, the traffic passing through Iceland also deviated from normal routes. Traffic is not usually routed through Iceland because its geographical location imposes higher expenses on ASes. In May 2013, Siminn’s parent Icelandic provider Opin Kerfi announced that it was the origin of 157 routes, which actually belonged to a US provider. Traffic was then routed only through Siminn, one of Opin Kerfi’s two ISPs. Later incidents showed redirections from nine other ASes through Siminn, which later “conceded redirection” of traffic, but also claimed that the route hijacking was unintentional and Siminn itself was the victim of a vendor software bug.\textsuperscript{160} \textsuperscript{161}

Renesys stated that despite the paucity of information about the perpetrators, there is enough evidence to suggest that the hijacks and the targets were intentional. These

\textsuperscript{158} Cowie 2013
\textsuperscript{159} Peterson, Andrea. 2013. “Researchers say U.S. Internet traffic was re-routed through Belarus. That’s a problem.” \textit{The Washington Post}, November 20. \url{http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/20/researchers-say-u-s-internet-traffic-was-re-routed-through-belarus-thats-a-problem/}
\textsuperscript{161} Cowie 2013
attacks differed from previous route hijacking examples in the technical steps taken to hide the rerouting from the recipients. Most tellingly, the actors intentionally kept a path clean in North America in order to retransmit the traffic, unsuspected, after it had possibly been tampered with. Financial gain originally seemed like a likely motive because a financial institution numbered among the targets, but once Renesys discovered that traffic from more than one national government was being rerouted, the set of possible motives increased, including the likelihood of possible state sponsorship. In some cases, attacks lasted for months before providers corrected the routing tables. Impacts of the hijacking varied considerably based on the providers targeted as well as which techniques the actors used to disguise their actions. As the attacks progressed throughout 2013, techniques grew in sophistication.\textsuperscript{162}

While there is little additional information about the attacks, examining some of the geopolitical dynamic of the nations involved provides background context. Belarus is a “dialogue partner” in the Shanghai Cooperation Organization (SCO), a Eurasian regional organization that focuses on a wide range of issues, including information security policy.\textsuperscript{163} China and Russia are both members of the SCO, but China’s influence in SCO goals and activities are recognizable.\textsuperscript{164} The security community has long suspected China of “selling technologies to regimes that export its filtering and surveillance system.”\textsuperscript{165} Sri Lanka, which is also an SCO dialogue partner like Belarus, hosted “information technology experts from China's Military Intelligence Division” in

\begin{flushleft}
\textsuperscript{162} Zmijewski 2014  \\
\textsuperscript{164} Song, Weiqing. 2014. "Interests, Power and China's Difficult Game in the Shanghai Cooperation Organization (SCO)." \textit{Journal of Contemporary China} 23 (85).  \\
\textsuperscript{165} Deibert and Crete-Nishihata 2012, 349
\end{flushleft}
2010 to receive “advice on how to filter the Internet,” allegedly including gateway filtering for domestic censorship.

While anecdotal, this example of Chinese assistance to other SCO dialogue partners is worth noting due to the access and relationships that the SCO could potentially provide to Belarus. Many unknowns make this relationship far from conclusive; perpetrators of the 2013 attacks were distributed in many locations, the Belarus ISP may have been compelled by another entity and the list of additional variables goes on. Further study would be necessary in order to determine whether the 2013 route hijacking was conducted by Belarusians, if it was another incidence of Chinese using partners to test cyber capabilities, or conducted by an unrelated perpetrator.

Researchers have noted that many ASes or enterprises around the globe could take concrete actions to decrease the likelihood of these hijacks, though all methods are resource intensive, such as the recommendation for all ASes to publish their data to RIRs. Renesys advises its clients and other observers to keep AS paths as short as possible and be able to advertise backup paths in order to correctly reroute incoming traffic.166

The MITM attacks in Belarus and Iceland turned the DEFCON presentation into reality. The Washington Post ran a story on Renesys’ blog, but the exploit has yet to turn up widely across the literature. Thus far, stories of BGP vulnerabilities and solutions have focused on addressing mostly unintentional threats, but the academic, policy, and technical circles should reorient to address the wide-ranging implications from a deliberate manipulation of the BGP trust framework. States have incentives as well as disincentives to reroute data through other networks. As attribution capabilities improve, states may be less inclined to associate themselves with exploits, or reveal their

166 Zmijewski 2014
cyberspace capabilities. The possibility for discovery would deter states from engaging or sponsoring deliberate route hijacks unless the benefit of doing so was determined to outweigh the cost.

The 2009 assessment of Internet risk noted that “operators currently trust other operators’ route announcements explicitly unless they have reason not to do so.” Based on a model of trust, the community of network operators already has several forums to discuss security, compare best practices, and exchange information. However, nation states are attempting to exert more control over ISPs operating in or sending traffic across their borders, and communities of subject matter experts are unlikely to completely address this development in posing technical solutions. State influence over routing authorities or certificate issuance is immediately complicated once geopolitical tensions arise. Political or military challenges to a state could potentially influence the state to revoke routing certificates for address blocks and impact sections of the Internet. While states have mostly exerted influence over Internet access to quell internal dissent, this case study illustrates the possibility that states could attempt to influence routing to affect other nations in the future.

**Applying Social Trust Theory to BGP Security**

Examining a real-world case study of deliberate route hijacking allows some initial insights into a future where deliberate undermining of the trust-based Internet is common. In a system where trust enables all transactions, it is important to understand what causes trust to increase and decrease, as well as what type of trust can be used to

---

167 ITSRA 2009, 63
strengthen a global system. Applying a trust framework commonly used in social theories provides some insights on how to view the trust supporting routing security.

Trust is one of the most fundamental elements of why the Internet has been successful. “Trust management frameworks” refers to the conceptual set of actions for increasing and managing trust in order to enable certain transactions. Actions to increase trust depend on “trust calculation, trust propagation, and trust reinforcement,” referring to how trust is defined, spread, and maintained.\textsuperscript{168}

Li and Li acknowledge that “trust” inherently implies that a given node prefers a particular node to another because of the faith in that node to obey BGP and perform capably in a certain context.\textsuperscript{169} Therefore, a node that behaves “more normally” will be perceived as more trustworthy, and therefore is more likely to gain increased connectivity as its agreements with customers and peers increase.\textsuperscript{170} This form of trust translates relatively well to hierarchy, because increased trust results in increased influence. Routing allows different connections among disparate (and unequal) networks to emerge; some connections are designed to be better than others, which is apparent in their end to end performance.

This section seeks to first examine routing protocols through a popular framework of trust, and second to examine how deliberate exploits of the protocol would affect the results of the framework. This framework envisions public trust as two axes.\textsuperscript{171} The x axis represents a spectrum between local trust (left of the y axis) and global trust (right of the y axis). Local trust does not extend much further than one or two degrees away from

\textsuperscript{169} Li and Li 2013, 704
\textsuperscript{170} Li and Li 2013, 707
the entity in question. Global trust is easily transferred and extended to contacts several degrees away. The y axis represents a spectrum between horizontal trust (south of the y axis) and vertical trust (north of the x axis). Horizontal or social trust is held, maintained, and managed in distributed relationships among relatively equal peers, and vertical or political trust is held, maintained, and managed in a hierarchy.\footnote{O'Hara 2005}
The Internet as a whole has been said to reside in the (Local, Horizontal) or (-x, -y) quadrant of the trust axes, since end users trust few others online, authority is distributed, and no central governing authority enforces trustworthy behavior.\(^{173}\) \(^{174}\) Among peers, “competence trust, relational trust, and contractual trust” are most effective trust categories in strengthening a system or network.\(^{175}\) Vertical trust depends on establishment of a hierarchy, where a hierarchical authority can compel participants to behave in a certain way. The points further north on the y axis correspond to stronger enforcement methods, i.e. more severe consequences in the case of non-compliance. Locating BGP on the graph would place it south of the y axis, indicating horizontal trust, because of the distributed accountability. However, the efforts described in the literature include recommendations to move it north along the y axis to vertical trust created through hierarchy.


\(^{174}\) Kuerbis and Mueller 2011, 140

Applying this framework to BGP vulnerabilities shows that current solutions propose leveraging both horizontal and vertical trust. Both types of trust will be discussed here. Most market-based mechanisms would support horizontal trust. Recent recommendations for “creating market pull” on providers and routers to behave well are trying to increase horizontal trust in routing, including through involvement of the public sector. If national governments buy connectivity from ISPs, then requiring certain best practices of those ISPs could help drive change across the smaller providers as well. This recommendation largely reinforces the horizontal model of trust, where distributed entities enforce trust through market- and peer-driven accountability structures. Security firms also recommend increasing transparency among ASes about their routing paths, since the actors conducting deliberate BGP routing hijacks may have assumed that no one monitors bad traffic paths. By increasing awareness and transparency over which paths are good and bad through crowdsourcing, increased attention to the issue, and publications of trust violations, the likelihood for malicious route hijacking would theoretically decrease.

Policy and technical bodies such as the European Network Information Security Agency (ENISA) are also suggesting improvements to horizontal trust mechanisms, including anonymized information sharing among operators, development of remediation communities, and formalization of best practices. Each of these recommendations would indirectly make operator reputations more important and build available resources to equip operators during incidents. Drawing attention to good and bad actors could also have a significant effect on commercial peering and customer-provider agreements.

---

176 ENISA 2012, 56
177 Cowie 2013
178 ENISA 2012, 57
between ASes. Peer ASes do not want to carry customer traffic of an unreliable AS since discoveries that traffic has been tampered with would result in loss of customers. As previous studies have shown, the connectivity of an AS is a virtuous cycle; increasing customers will result in more nodes wanting to connect to the AS in peering agreements, and increasing peering agreements will result in more customers. Damaging this cycle is not in the financial interest of an AS.

Solutions that push BGP security towards vertical trust are those that support the single root of trust and other central authorities. The CSRIC’s basic mitigation strategy against propagating bogus routes are that 1) a database should exist specifying “who is authorized to route what and when,” 2) a mechanism should exist to disseminate this information, and 3) mechanisms should exist to help operators use the information to create route filters. Documenting all prefix addresses that ASes serve (number one in the CSRIC strategy) would require significant resources to undertake and might also be best supported by public sector funding. The main opposition to this recommendation contends that an increase in documentation will make ISPs easier to regulate, and any regulation would hamper security efforts in the long run. While a mandatory database might seem purposed to boost horizontal trust, arguments against it highlight that the likely result of this database would be expediting creation of a single root. Once the database is built, any single root would easily be able to transition into monitoring all addresses. However, if states are the emerging threat in deliberate route hijacks, granting more power to entities that are easily compelled by states may not be the wisest course.

Another byproduct of approaching security through this trust framework is recognizing the fair process effect, which holds that entities in a vertical trust framework
are more likely to accept outcomes handed to them by authorities if they perceive that the outcomes were determined in a fair manner.\textsuperscript{180} Applying this effect to the Internet has interesting possibilities. Since many nations oppose a central governing mechanism or authority over routing protocols, a viable entity will be difficult to identify. Furthermore, trusting that the entity’s processes are free from governmental intervention is a big risk. However, if the current processes of address allocation and protocol monitoring are not changed significantly, ASes may be willing to accept the outcomes handed down by this central trust root. A single root of trust is likely to displease many governments and ASes, including the U.S., but maintaining current processes under a new root may stall the most extreme opposition.

Possibly the most important factor in analyzing trust solutions for BGP security is the degree of correlation that may exist between horizontal and vertical trust, even though the body of experimental data is not abundant enough to demonstrate strong causality. However, current evidence suggests that changes to vertical trust impact horizontal trust as well. Social theorists contend that the “larger effects of losses than of gains on people’s behavior can possibly moderate the causal mechanism between vertical and horizontal trust.”\textsuperscript{181} Applying this to routing infrastructure and network operators would mean that once a node loses trust in an authority, for example an ISP or a central governing authority like an RIR, it loses a degree of trust in its peers. This relationship is also more evident than if a node gains trust in its peers due to an increased trust in authority. While a nascent theory, social theorists, policy bodies, and technical experts


\textsuperscript{181} Eek and Rothstein 2005, 30
should explore this dynamic in proposing changes to both horizontal and vertical forms of trust, since increases or decreases in peers or authorities will impact how nodes work together on security.

With this theory in mind, and given the likely emergence of the nation state as a new category of threat actor in route hijacking, horizontal trust should be pursued first before establishing vertical trust mechanisms. Many of the horizontal solutions listed previously have yet to undergo widespread adoption, so there are still many available options to try. Given the strength of the profit motive and commercial agreements in the routing community, the community should exhaust horizontal trust options, such as strengthening market discipline to compel good behavior among peers and increasing awareness of the vulnerability, before resorting to any hierarchical compliance regime.

Horizontal trust-building can also account for the presence of state actors; ASes suffer economic and reputational blowback from rerouting traffic, so are inclined to avoid entanglement with states. At the same time, new trust mechanisms must include drives to increase awareness among ASes of possible state intervention so network operators can expand protection, detection, and response activities to anticipate deliberate threats. Horizontal mechanisms also avoid making a hypothetical compliance authority vulnerable to state influence. Lastly, focusing first on horizontal trust mechanisms reinforces the self-regulated nature of the Internet, but puts more responsibility on individual participants, which is necessary for continued operation of a decentralized web.
Conclusion

Internet routing protocols are simultaneously – and frighteningly – the glue holding the Internet together and its Achilles heel. While technical vulnerabilities in BGP are widely understood, technical solutions will likely be resource-intensive to implement and have varying political consequences. As threats grow from unintentional route hijacking to deliberate rerouting, solutions will also have to account for nation-state involvement, which they have not widely done to date.

While certificate authority reputations are somewhat impervious to pressure from national governments and many market mechanisms, routing protocols are more vulnerable to reputational pressure because the transacting parties are more knowledgeable. The Lemons theory is not readily applied to the routing protocol community because there is no information asymmetry; ASes, network operators, and other parties involved each understand the expected behavior. Peer and hierarchical ASes are also more likely to pay attention to terms of commercial agreements, behavior of other ASes, and reliability over time, since the behavior of other ASes has a direct impact on their own ability to route data effectively. Most of the data available suggests that reputational levers will be effective accountability measures, since commercial agreements enable the foundational layer of connectivity and routing transactions.

Further research should be undertaken on using reputational levers to increase the cost of malicious events. For example, if the providers in Belarus and Iceland were to suffer reputational costs in the forms of broken peering agreements or decreases in customers, the cost of rerouting traffic would rise significantly and the cost-benefit analysis of engaging in these hijacks would change. Studies should also examine whether
government funding would make commercial losses worthwhile. Increasing state accountability should also supplement current market-driven accountability mechanisms for routers and ISPs. International governance forums should devise and apply reputational levers to state actors to deter them from intervening in routing protocols and processes.

Lastly, applying social trust frameworks to routing presents interesting, budding conclusions. Whereas routing has historically relied on horizontal trust through distributed networks and market-driven accountability, many of the BGP solutions currently under consideration would employ vertical trust mechanisms to correspond with routing’s more hierarchical structure. The effects of vertical trust on horizontal trust are not completely understood, and any comprehensive and authoritative policy prescriptions should begin to examine how reinforcing vertical hierarchy would affect the commercial relationships, and vice versa. The one commonly held truth across all of the solutions is that infrastructure must undergo some degree of change in order to remain resilient, and trustworthy, in the face of evolving threats.
CHAPTER 3: STAKEHOLDER MODELS FOR INTERNET GOVERNANCE

Internet governance is a sprawling topic that includes “principles, norms, rules, decisionmaking procedures, and programs that shape the evolution and use of the Internet” according to the 2005 World Summit on Information Society.\(^{182}\) The purpose of international governance forums then is to address three types of problems that surround the continued success of the Internet, which include “technical standardization,” “resource allocation and assignment…and human conduct on the Internet, encompassing the regulations, rules, and policies” guiding behavior.\(^{183}\)

Most nation-states tacitly acknowledge the U.S. as the steward of the Internet. Some nation-states, who are generally referred to as emerging powers, however, are pressuring the international community to regulate the Internet as another form of telecommunications infrastructure.\(^{184}\) Governments around the world are increasingly interested in Internet policy because of the impact that access to the global Internet has on economies, social and cultural systems, and access of citizens to ideas and information. In addition, rising populations and numbers of software and hardware engineers in emerging nations suggest that English may not always remain the language of Internet engineering.\(^{185}\) Further, emerging technologies are increasingly being developed outside the United States and a growing number of Internet users are non-Americans. Changing internet demographics, combined with revelations like those made by former National Security Agency (NSA) contractor Edward Snowden about controversial surveillance

---

\(^{182}\) Shackelford 2013, 1324
\(^{185}\) Yannakogeorgos 2012, 112
practices, are prompting adversaries and allies alike to doubt the U.S.’s ability to be a reliable guardian of the Internet.186

So far, the U.S. has resisted efforts to regulate the Internet or relinquish some of its stewardship. These requests for U.S. influence largely are at the behest of human rights advocates and powerful private Internet companies, which are the main actors that oversee Internet governance and actively resist government intervention. The U.S. approach to maintaining an unregulated Internet is also based in the legacy of voluntary self-governance in several U.S. industries, some of which resorted to regulation only after years of accidents demonstrated a compelling enough case for regulation.187

Any regulation of cyberspace will necessarily be complex, given the multi-layered infrastructure, numerous jurisdictional boundaries, and the cyber threats that are able to traverse borders instantly. Cyber policy scholars have described Internet governance as a global system, where states “inject… [their desires] into that system.”188 Given the changing risk and policy environments, the U.S. has multiple options of how to redefine its role and inject its desires in global Internet governance. This includes determining whether it should continue to act as a benevolent hegemon to ensure dominance of an open, free Internet, and to what extent it can, in response to recent international resistance. Ultimately, the behavior of the U.S. can either delay or accelerate movement towards a new governance model. I maintain that two recent examples of U.S. behavior in response to past intelligence failures and a culture of fear may be causing

potentially irreversible damage to the U.S. ability to influence Internet governance in the next several years.

To provide background on this problem, I first briefly provide an overview of the U.S. international cyberspace strategy. Second, I outline three viewpoints expressed in the literature and by the national security community on potential roles for the U.S. to play in these global Internet policy bodies. I then use two case studies to examine nation-state behavior in cyberspace relevant to governance policy positions. Based on these case studies, I conclude that revelations about U.S. behavior are significantly at odds with its expressed policies due to the perception of lack of accountability.

**Background**

The history of the Internet from its first days as ARPANET\(^{189}\) are well documented, so this paper does not go into depth on its evolution or accompanying governance models. In recent years, scholars have attempted to differentiate among the several interrelated topics and several disciplines that relate to Internet governance.\(^{190}\) To clearly scope the discussion in this paper, I utilize the definition of Internet governance developed by the United Nations Working Group on Internet Governance in 2005. They stated that “the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet.”\(^{191}\) The 2005 definition primarily referred to the issue of “global coordination of Internet domain

---

\(^{189}\) President Eisenhower established the Advanced Research Projects Agency (ARPA) in 1958, which created ARPANET to connect agency employees across the country. The resulting single network was eventually expanded, commercialized, privatized, and evolved into what became the Internet. (Thompson 2011, 2011, 466)

\(^{190}\) van Eeten and Mueller 2013, 723

names and addresses,” but it has evolved to include additional concepts including “economics, law, policy, technology and operations” of the Internet.\textsuperscript{192} The scope of this paper focuses specifically on the U.S. role in championing public policy positions.

The literature widely recognizes that a mix of code, laws, collaboration, the market, and regulatory structures (whether self-regulation or national regulations) can all be legitimate pieces of effective governance.\textsuperscript{193} This decentralized nature of Internet governance allows for facets of the same problem to be handled by different entities. Each of these bodies has an interest in addressing security of the Internet through countering cyber threats and malicious behavior. However, each of the strengths and weaknesses of the organizations themselves affect which ones wield the most influence in different subjects.

In 2011, the U.S. published the International Strategy for Cyberspace. This strategy includes the U.S. commitment to fostering cooperation among nations on cybersecurity, specifically through “multistakeholder” organizations. The Strategy also subtly describes two ways in which the U.S. government differs from international partners in how it frames Internet governance. The first recommendation in the Strategy is that important discussions about Internet governance should be brought into traditional, formalized international foreign policy institutions, instead of remaining in Internet-specific working groups and organizations.\textsuperscript{194}

International debates among nation-states about Internet governance primarily occur within institutions dedicated to the organizing the Internet. Various international

\textsuperscript{192} van Eeten and Mueller 2013, 724
\textsuperscript{193} Shackelford 2013, 1333
bodies address the key governance problems separately. The Internet Corporation for Assigned Names and Numbers (ICANN) distributes unique Internet Protocol addresses to each user on the Web\textsuperscript{195} and administers the Domain Name System (DNS);\textsuperscript{196} the Internet Governance Forum (IGF) provides a United Nations (UN) venue for dialogue about governance; and the International Telecommunications Union (ITU) traditionally covers telecommunications policy.\textsuperscript{197} \textsuperscript{198} Other organizations, governments, and corporations insert their desires into these forums as well. The Internet Engineering Task Force (IETF) is an international organization that creates standards to “influence the way people design, use, and manage the Internet.”\textsuperscript{199} IETF members include some of the most influential technology and security companies, which can shape IETF standards development and policy positions. The security community considers the IETF another forum for nation-states to push ideas about Internet governance as powerful technology companies increasingly represent state interests.

However, the U.S. Strategy advocates pushing Internet governance issues into more traditional policy and governance institutions. The Strategy specifically names the Organization of American States (OAS), the Association of Southeast Asian Nations (ASEAN) Regional Forum (ARF), the Organization for Economic Cooperation and Development (OECD), and the Group of Eight (G-8) among others as potential bodies


\textsuperscript{196} The Domain Name System translates IP addresses into domain names and domain names into IP addresses, directing the Internet user to his or her desired destination.

\textsuperscript{197} van Eeten and Mueller 2013, 724

\textsuperscript{198} Yannakogeorgos 2012, 117

that should include Internet governance in their agendas. The OECD and the G-8 have already put forward public messaging on their support for the multistakeholder model of Internet governance. This language suggests that the U.S. may prefer a stronger state role or figurehead in these discussions than is afforded by organizations like ICANN and the IGF, or that the organizations dedicated to technical management of the Internet should be run and populated primarily by private sector companies, allowing the states to be able to discuss policy issues in preexisting bodies that are more amenable to the current model.

When it comes to issues of security, many topics require international collaboration to effect change, such as decisions about holding certificate authorities accountable and securing BGP routing. If updating the code in Internet standards and protocols becomes a more viable way to increase security, instead of relying on overlapping policies to influence behavior, the IETF may become increasingly important. The IETF will continue to update standards and protocol development to increase trust in the architecture. Issue advocacy and public policy debates, such as those over appropriate access control policies, are more appropriately discussed in international fora like the OECD, which offers governments a chance to discuss economic impacts of Internet policy. As a result, the OECD may be an appropriate community to focus specifically on how market forces affect security.

The second area where the U.S. Strategy differs from other international messaging is that rather than warning about the rise of government jockeying in Internet governance fora, the Strategy recommends that multistakeholder governance “not be

---

limited to governments, but should include all appropriate stakeholders.”202 This subtle phraseology suggests that states already play a central part in governing the Internet and must simply make room for other non-governmental stakeholders, instead of assuming that states are the actors with the need to increase their influence. The Strategy also mentions the need to include other regions, such as Africa and the Middle East, which have rising populations of Internet users and will likely become part of future governance discussions.203 The Strategy does not provide much detail on governance policy issues for the U.S., but nevertheless conveys that governance issues are a priority and that nation-state influence in fora is important, inevitable, and perhaps malleable.

Key arguments for the current multistakeholder model include “that it allows for speed, flexibility, and decentralized problem-solving and stands in stark contrast to a more traditional, top-down regulatory model characterized by rigid processes, political capture by incumbents, and in so many cases, impasse or stalemate.”204 Meanwhile, nation-state leaders that participate in the Internet-affiliated organizations mentioned above are calling for a regime change. Nation-state representatives that have traditionally advocated for U.S. leadership in Internet governance are showing hesitation. Furthermore, a growing number of adversarial state leaders are proposing or proactively making changes to the current model within their powers at the national and international levels in terms of both policy and technical requirements. Many within the UN community are arguing that the ITU would be an appropriate body to preside over

203 U.S. International Strategy for Cyberspace 2011, 10
Internet governance, despite its current lack of a mandate over Internet policy. An ITU-led Internet would arguably provide more power to China and other authoritarian nations.

As these conversations occur in both traditional and Internet-related policy bodies, the U.S. role in Internet governance is a top question and concern. I next explore a few of the options proposed for a future U.S. role, before identifying two recent behaviors that may severely damage U.S. bargaining power and affect the likelihood of each option.

**Literature Review**

A review of the existing literature shows agreement across the security community that the “Internet’s reliance on nonhierarchical forms of governance” poses unique questions around the future of Internet security.\(^{205}\) However, there is divergence within the community over what form of governance the U.S. should recommend and help enforce, given the complex governance and security environment. This section discusses three of the key views. The first view is that the U.S. national security and technology communities do not know enough about the current networked model to judge whether it is good or bad for U.S. interests in the long run; the second view is that the U.S. should continue to protect the current unregulated, multistakeholder model; and the third view is that a regulated, state-administered model is inevitable due to evolving global politics, and that the U.S. should begin to prepare for and adapt to this inevitability.

\(^{205}\) Mueller, Schmidt, and Kuerbis 2013, 87
First View: Multistakeholder Model is Still Unstudied, but the Best Alternative

The first view recommends that additional study around the Internet’s unique multistakeholder, networked governance model should precede any changes to the model of Internet governance. This long-term approach is heavily based on the structural international relations theory that views nation-states as individual actors in a hierarchical international system.\(^{206}\) The difficulty in determining a U.S. role in Internet governance refers us back to the traditional, international relations structure. In this international anarchic system, states are the key actors and the principles of sovereignty are understood and relevant.\(^{207}\) Now, cyberspace and the problem of governing it may pose a new kind of model, where individuals have an exaggerated importance because of the Internet’s ability to equip and empower the individual user.\(^{208}\) Because the Internet is decentralized and managed at the technical and operational levels by multiple non-government stakeholders like ICANN and private sector companies, with no hierarchy of control, the Internet may therefore be “antithetical to the hierarchical international relations system,” which would explain the difficulties in devising the right long-term governance solution.\(^{209}\)

One argument in favor of continuing the multistakeholder model contends that the numerous influential players that manage Internet functions make a state model irrelevant. Players in a networked model include “prices and markets, traditional hierarchical firms, hierarchical state power, interpersonal and inter-organizational

\(^{207}\) Choucri and Clark 2013, 23
\(^{208}\) Choucri and Clark 2013, 23
\(^{209}\) Mueller, Schmidt, and Kuerbis 2013, 87
networks and new, scaled-up forms of peer production. Proponents of this networked model of various stakeholders predict an increased collaboration between public sector agencies, specifically law enforcement, and the private sector. In this model, the state will relies on multistakeholder forums due to the high degree of private sector control over the Internet and the Web’s adherence to international norms and standards. As a result, the state will not have the sufficient influence or ability to structure cyberspace in terms of the architecture and technology. Private sector technology companies own and operate most of the cyber infrastructure that supports the Internet. States will be part of fora, but will not be the sole actors running or shaping them, in part because the governance model that the fora shape is too dissonant with traditional constructs of state sovereignty and in part because technology companies have the sole ability to shape Internet code and administration. States will still seek to influence the governance of the Internet through providing input and preferences into these multistakeholder forums instead of asserting direct, hierarchical control.

The multistakeholder model has already had positive and negative effects on how states attempt to influence the Internet. Private sector companies are driven by economic profit, and as a result, technology companies have already demonstrated a willingness to sell services enabling states (e.g., Burma, China, Iran, Saudi Arabia, Tunisia, and Yemen) to employ packet filtering and other controlling technologies that limit user access. At the same time, however, multistakeholder initiatives exist to compel good market behavior. The Global Network Initiative (GNI), for example, was created in 2008 to

\[^{210}\text{van Eeten and Mueller 2013, 732}\]
\[^{211}\text{Mueller, Schmidt, and Kuerbis 2013, 99}\]
\[^{212}\text{Mueller, Schmidt, and Kuerbis 2013, 100}\]
\[^{213}\text{Mueller, Schmidt, and Kuerbis 2013, 101}\]
\[^{214}\text{Land 2013, 451}\]
provide a forum for companies to resist government pressure to comply with policies that encroach on freedom of information and expression. GNI offers four key opportunities to members, including a framework for decision-making, independent assessments to encourage accountability across member companies, policy engagement opportunities, and opportunities for shared learning across members.215 While GNI focuses primarily on protection of human rights and civil liberties with respect to freedom of information, other multistakeholder initiatives have the potential to drive good behavior among technology companies that wield the most influence over Internet policy.

An Internet self-regulated and self-governed by private sector stakeholders would also be difficult to secure using traditional state methods of governance since the Internet is not subject to state control. Because the multistakeholder model of governance is a newer phenomenon that does not have as long a history as the state-led model, the cost-benefit analysis of changing away from the multistakeholder model may not be well developed enough to argue one way or the other.216 Time will tell whether “hierarchically organized” states can adapt to a unique, distributed governance model.217

In conclusion, the power struggle with states and private sector actors is likely to continue within a networked governance model. Private sector companies currently manage most Internet operations, and states will continue to push their agendas through international fora for discussion. The cyberspace domain has no immediate parallel in the international relations environment, and as such there is no alternative from which to draw comparisons. The body of literature that supports this first view acknowledges that

217 Mueller, Schmidt, and Kuerbis 2013, 87
Internet governance is pioneering, and that more research and knowledge must be conducted and acquired in order to propose a model that would better serve the interests of relevant stakeholders. In the meantime, the international community of both states and the private sector should maintain a multistakeholder model. What is not discussed in depth is the innovation and technological gains that result from a private sector-led model.

**Second View: Advocacy for the Unregulated, U.S.-Sponsored Model**

The second view among those that prescribe U.S. approaches to Internet governance is that the U.S. should assert itself more dominantly in international fora and other venues that discuss issues of governance to ensure the open, free nature of the Internet. Other nations readily acknowledge that the U.S. serves as the primary advocate for the open, free public policy of the Internet and also “contains and arbitrates the technological standards the Internet rests on.”

Some authors describe the U.S. stewardship of the Internet as a “friendly dominance over allies and adversaries alike” simply by managing the technical, operational, and policy frameworks of the Internet.

Proponents of the view for continued U.S. stewardship of the Internet argue that an unregulated Internet is the best way to guarantee that people around the world obtain unfettered access to information. In addition, because of the decentralized nature of the Internet, the best model for regulation should be one “developed from the bottom-up,”

---

219 Yannakogeorgos 2012, 107
which the U.S. defends.\textsuperscript{221} A market-regulated Internet is directed heavily by the private sector and “civil society,” both of which are important to U.S. political priorities.\textsuperscript{222} Authors that have studied recent attempts of states to try and nationalize their own “intranets” contend that creating online borders can potentially violate human rights laws protecting individual access to information, ideas, and expression, and even constitute trade barriers.\textsuperscript{223}

One of the expressed reasons for this view is that self-regulation is effective already, meaning that no state control is required to solve security or other problems requiring decisive action or consensus. The Conficker incident in 2008 illustrates a success of the networked model. Conficker was a piece of malicious software that exploited a vulnerability in the Microsoft operating system and created a botnet of unprecedented size. The working group that developed a response to Conficker has been touted as an example of self-governance that works, though the scalability of self-governed incident response may remain a problem.\textsuperscript{224} Observers liken the working group to a “network club” as opposed to a true network, since all members were based in the U.S. and predating their work on U.S. values and security preferences. Other botnets\textsuperscript{225} required intergovernmental agencies working with the private sector and demonstrate an increased state presence in cybersecurity.\textsuperscript{226} The U.S. has a long history of industries conducting voluntary self-regulation, but self-regulation is uncommon in countries with

\textsuperscript{223} Land 2013, 438
\textsuperscript{224} Mueller, Schmidt, and Kuerbis 2013, 97
\textsuperscript{225} A botnet occurs when criminals “use bots [robots] to infect large numbers of computers. These computers form a network, or a botnet” (Microsoft 2013).
\textsuperscript{226} Mueller, Schmidt, and Kuerbis 2013, 99
active Internet populations. And in the case of the Internet, the U.S. policies have arguably failed to identify where self-regulating market behaviors stop being effective.\textsuperscript{227}

On the other hand, the policy community agrees that any regulator must have specific expertise in the area that they regulate.\textsuperscript{228} Nations that seek to exert their sovereignty through regulating the Internet do not have the required expertise to do so effectively.\textsuperscript{229} An alternative highlighted in the literature identifies cyberspace as a “pseudocommons” instead, which nations should view as a space where they can “exercise sovereignty through…the effects doctrine,” which “permits the regulation of activities that impact a state’s territory.”\textsuperscript{230} A pseudocommons is too dynamic to be permanently considered a global commons or state territory; as a result, authors argue that it requires a complex form of governance called “polycentric regulation” led by a multistakeholder group of multiple centers to provide accountability for each interest group and keep regime changes flexible.\textsuperscript{231}

Other authors contend that no state is likely to support a system that ranks states hierarchically because of the detrimental effect it would have on their own ability to shape global norms and policies.\textsuperscript{232} Still others contend that states cannot change the balance of power over the Internet through international institutions to begin with, since all these bodies do is discuss governance and not actually control Internet functionality.\textsuperscript{233} The current presence of states in international fora may make it seem as

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{227} Lewis 2010, 61
\item \textsuperscript{228} Waz, Joe and Phil Weiser. 2012. "Internet Governance: The Role of Multistakeholder Organizations." \textit{Journal on Telecommunications & High Technology Law} 10 (2): 345.
\item \textsuperscript{229} Shackelford 2013, 1305
\item \textsuperscript{230} Shackelford 2013, 1319
\item \textsuperscript{231} Shackelford 2013, 1340
\item \textsuperscript{232} Mueller, Schmidt, and Kuerbis 2013, 100
\item \textsuperscript{233} van Eeten and Mueller 2013, 729-730
\end{enumerate}
\end{footnotesize}
if states wield greater power over the Internet than they do in reality.\textsuperscript{234} States by default pursue greater influence in these fora, but only because they are the most visible places in which to do so. As a result, focusing primarily on international institutions will result in an exaggerated perception of state power, and focusing on the multistakeholder networks will reveal that state power likely has insufficient influence to direct governance changes.\textsuperscript{235} Weighing the weaknesses of a state-heavy model would suggest that the U.S. has a good chance of maintaining the status quo. The risk of power loss for a state interested in developing a state-led, regulated model might outweigh the benefits of the new model.

\textbf{Third View: State Regulation is Inevitable}

The third view of a potential U.S. role is that changes to the Internet governance structure are inevitable, and the current networked model will evolve into a state-controlled, hierarchical model to better match the traditional structural international relations environment. Several authors are proposing that a shift in Internet governance is inevitable for two reasons. The first is that the U.S. no longer asserts as much control over independent bodies that manage the technical operations of the Internet.\textsuperscript{236} The second reason authors argue that a state-controlled Internet is inevitable is that state actors are demonstrating increasing power on the international stage in favor of their own terms of using and managing the Internet, which began before the Snowden allegations further eroded trust in the U.S.-led model.\textsuperscript{237}

\textsuperscript{234} van Eeten and Mueller 2013, 722
\textsuperscript{235} van Eeten and Mueller 2013, 730
\textsuperscript{236} Lewis 2010, 56
\textsuperscript{237} Lewis 2010, 56
Policy experts worried about U.S. primacy warn about the increased presence of authoritarian states, either through government or private sector representatives, because of the potential to influence protocols and standards.\textsuperscript{238} China, for example, has indicated that its rapid increase in Internet users as well as Internet infrastructure development justify an “ability to participate in and demand reforms” of governance bodies.\textsuperscript{239} Other countries are pushing forward policy agendas that would restructure the Internet to better accommodate their political and social needs. If other states start to pursue control over the Internet at some point as a form of displaying their national sovereignty, the way in which they do so may or may not be amenable to U.S. values and policies.\textsuperscript{240}

One construct often used to describe transitions to or from state-controlled models focuses on “norms.” Recent literature has looked at the propagation of cyberspace controls around the world, and specifically “norm regression” as defined by the “growth and spread of practices that degrade cyberspace as an open commons of information and communication.”\textsuperscript{241} The governance of the Internet was architected by “transnational networks of engineers with private sector companies and individuals shaping cyberspace.”\textsuperscript{242} In this case, the norm was lack of regulation and the belief that “state censorship and surveillance were thought to be difficult due to the decentralized design of the Internet.”\textsuperscript{243} Despite the long history of an unregulated Internet however, lack of regulation may not last. Recent studies debate the “ineffectualness of multilateralism”

\textsuperscript{238} Yannakogeorgos 2012, 103
\textsuperscript{239} Liu 2012, 48
\textsuperscript{240} Lewis 2010, 63
\textsuperscript{241} Deibert and Crete-Nishihata 2012, 341
\textsuperscript{242} Deibert and Crete-Nishihata 2012, 339
\textsuperscript{243} Shackelford 2013, 1306
with the U.S. at the helm of Internet governance conversations “as the United States strives to lead and others fail to follow.”

Leaked papers for a 2012 meeting of the International Telecommunications Union (ITU), a UN agency, revealed proposals on the part of several nations to “regulate the Internet by crowding out bottom-up institutions, imposing charges for international communication, and controlling the content that consumers can access online.” State censorship and surveillance occur frequently due to advances in technology. Nondemocratic states are increasingly active in Internet governance forums, and Western nations are using less traditionally free market tools such as capital controls to stabilize their economies and various industries. These trends taken together may signify a future governance structure for the Internet that is not built on the unregulated, free-market structure it is today.

In 2013, Brazilian President Dilma Rousseff advocated greater state control over the Internet at the United Nations General Assembly in September 2013 to protect against behavior like that of the U.S. She announced that Brazil would put forward ideas to “[establish]…a framework for the governance and use of the Internet, and to ensure the effective protection of data that travels through the web.” The framework would align with some principles the U.S. champions already, including freedom of speech, but would be a significant departure from the current unregulated model.

244 Yannakogeorgos 2012, 14
Some American believers in this view argue that the U.S. should learn how to support and adapt to a state-controlled model. James A. Lewis, a cybersecurity scholar from the Center for Strategic and International Studies, argues that the historical and current lack of regulation and government control of the Internet is not due to “immutable characteristics of cyberspace” as much as a result of the political environment during the 1990s.\textsuperscript{248} Chinese authors contend that “existing research has already repudiated the early belief of a totally decentralized and uncontrollable Internet system as merely a myth.”\textsuperscript{249}

Examining the political, social, and cultural circumstances at play during the birth of the Internet shows that globalization was emerging and technology was changing rapidly. The U.S. commercialized the Internet during the 1990s under the administration of President Bill Clinton. The administration favored a decentralized Internet, one that was subject mostly to industry codes of conduct instead of government control.\textsuperscript{250} Administration Advisor Ira Magaziner stated in 1998 that the Internet would be managed through “de-centralized, private, non-profit bodies” that are “stakeholder-based” instead of by the government.\textsuperscript{251} Private sector companies and Internet architects collectively used descriptions of the “untrammeled, borderless” nature of the Internet and its newness compared to other industries as justification for lack of government intervention, since government regulation or control over Internet functions might impede technological competition or growth compared to other nations.\textsuperscript{252}

\textsuperscript{248} Lewis 2010, 55
\textsuperscript{249} Liu 2012, 47
\textsuperscript{250} Lewis 2010, 60
\textsuperscript{252} Lewis 2010, 56
Research is currently examining the likelihood of increased state control in response to cyber incidents. A recent study examined a background vulnerability of Internet routing architecture, Border Gateway Protocol, as well as Conficker as a short-term, discrete threat, and found that states are more likely to adapt to the unregulated Internet governance model to secure it instead of changing it.\textsuperscript{253} A key example of a change to the decentralized networked model has been proposed in Resource Public Key Infrastructure (RPKI), which uses hierarchical validations of routing information to verify that senders are who they say they are.\textsuperscript{254} However, RPKI is not widely used yet, in part because the certificate issuer at the trust anchor could conceivably acquire more significant regulatory power over entities purchasing certificates underneath them. National policy has not evolved enough to address or force these issues of architecture vulnerabilities, so states are adapting instead.

Proponents of a regulated model contend that a “self-organizing global commons” of the sort that managed the Conficker incident will not work much longer from the U.S. perspective for two main reasons. First, foreign government military and intelligence capabilities will increasingly and easily bypass private sector attempts to protect networks, and second, the private sector does not have an effective business case to invest in sufficient cybersecurity for the nation, meaning that states will be compelled to have a hand in regulating network security.\textsuperscript{255} The alternative to an unregulated Internet, however, may not be state-led intranets, but rather a hybrid of the current multistakeholder model with increased roles for states.

\textsuperscript{253} Mueller, Schmidt, and Kuerbis 2013, 90  
\textsuperscript{254} Mueller, Schmidt, and Kuerbis 2013, 94  
\textsuperscript{255} Lewis 2010, 58
In sum, the current literature describes three views of Internet governance. The first is that not enough is known whether the current networked, unregulated model is a good or bad one, and as a result, the international community should not make assumptions and seek to change it just yet. The second view is that an evolution towards a regulated model is not inevitable, and the U.S. should leverage its global power position and remain diligent in defending an open, free Internet that guarantees access to information and ideas around the globe. The third view is that regulation is inevitable as the world changes, as the current model may prove ineffective at addressing large-scale security incidents, and as increasing numbers of nation-states push for changes in global Internet policy and administration.

**International Behaviors**

In this section I discuss two case studies of behavior among states and private sector actors relevant to key governance policy positions and security concerns. Two problems that would arguably plague a state-led or multistakeholder model are restricting Internet access, either by cutting off access altogether or censoring specific websites, and surveillance activities. Both of the case studies provide justification for accountability of both government and private sector companies. Both also demonstrate the inherent tendency to overcompensate that is likely to continue as reliance on Internet capabilities increases.

**Internet Access**

Several nations, including both democratic, Western-friendly nations and more authoritarian countries, have requested that Internet access providers suspend services to customers across the country in order to quell local unrest or in the name of state security.
This section discusses a few of those cases in some detail to illustrate current and potential state and private sector behavior over a regulated Internet. This paper does not describe the arguments for and against degrees of Internet access in detail, but provides an overview of one of the issues that influences ideological approaches to Internet governance.

As of 2009, both democratic and undemocratic nations were conducting Internet filtering.\(^{256}\) This includes gateway filtering, which automatically occurs at the gateway points that connect national physical infrastructure to global Internet networks, and indirect filtering, where a government compels third-party Internet Service Providers (ISP) to block certain content.\(^{257}\) The Great Firewall of China is an example of gateway filtering, and was so named because of the government control over Internet access points. This control limits viewer ability to reach certain websites and, as a result, the government can control individual behavior and access to information.\(^{258}\)

Numerous countries have compelled service providers to suspend access in response to local unrest, protest, or online behavior unacceptable in the eyes of the state leadership. In 2005, the king of Nepal partially blocked Internet access during a controversial transition of the monarchy.\(^{259}\) In 2008, Pakistan cut off access to YouTube after anti-Islamic content appeared on the video sharing website, but the state inadvertently conducted route hijacking,\(^ {260}\) disrupting access for users around the globe. The disruption prompted an outcry from freedom of speech advocates and heightened

\(^{256}\) Deibert and Crete-Nishihata 2012, 339  
\(^{257}\) Land 2013, 442  
\(^{258}\) Land 2013, 441  
concerns about fundamental Internet routing vulnerabilities. Another example of censorship during times of unrest occurred in Iran in 2009, when citizens inspired by the Green Movement united and communicated through Facebook and online social media tools. Iran compelled service providers to suspend access to Facebook in order to avert protester activity.²⁶¹

The largest instance of service suspension to date occurred on January 28, 2011, when the Egyptian government shut off access following protests against the Hosni Mubarak regime.²⁶² Internet security experts posited that the speed at which the service providers cut off access is due to the close relationships of the ISP with the Egyptian government. The Egyptian shutdown ultimately deterred similar U.S. legislative language up for debate in the U.S. Senate, the “Protecting Cyberspace as a National Asset Act (S. 3480), which “would mandate that all ISPs, search engines, and software firms comply with any federal government order to ‘preserve those networks and assets and our country and protect our people [sic].’”²⁶³ The draft “Internet kill switch” language was quickly abandoned after Egypt’s actions illustrated potential domestic and international consequences.²⁶⁴ All these examples demonstrate the temptation of an insecure government to quell popular unrest, as well as the international political consequences of doing so.

Notably, the U.S. Communications Act of 1934 allows for an interpretation of sweeping U.S. government powers to “take extraordinary measures” during the threat of “war or national emergency” to include terminating forms of communications that

²⁶¹ Cramer 2013, 1076
²⁶³ Cramer 2013, 1083
²⁶⁴ Cramer 2013, 1083
arguably include the Internet. Furthermore, in 2011, the Pentagon decided that a cyber-attack can qualify as an act of war, enabling the President to activate powers in the Communications Act if necessary. Scholars have clarified that the Department of Defense document’s use of “act of war” is technically closer to “use of force,” and would not necessarily trigger a decision by Congress to declare war. The significance of the terminology, however, is that even the “state or threat of war” in the language of the Communications Act is adequate to trigger Presidential action without requiring a decision by Congress. Alternative solutions to government control during a cyber-attack are not clear either. Proponents of a private sector solution note that private sector companies may be able to use capabilities like active defense in response to the use of force, but private sector financial interests have the tendency to supersede concern for national security, making this solution controversial.

Congress and Administration officials have recently called for revision of the Communications Act to “cabin the President's emergency powers.” The U.S. has also been noticeably quiet about friendly nations limiting access to their citizens, as in the cases of the United Kingdom and Uganda. Some authors point out that U.S. advocacy of global Internet freedom is also inconsistent with the sweeping domestic power of the executive branch combined with minimal regulation of the private companies that control

---

269 Thompson 2011, 491
270 Cramer 2013, 1084
the networks.\textsuperscript{271} This inconsistency has so far avoided public debate because of the desire to keep regulation at a minimum. However, greater criticism about the U.S. stewardship of the Internet may eventually cause policymakers to make language around U.S. actions more precise.\textsuperscript{272}

While states exhibit consistent willingness to use a last resort and cut off Internet access for domestic security reasons, the private firms that operate the Internet also participate in censorship activities. Google recently experienced a controversy about the “Innocence of Muslims” film that incensed anti-U.S. protests around the world.\textsuperscript{273} Google decided to block access to the video from specific countries but not completely, despite pressure from the U.S. government and the White House.\textsuperscript{274} A few years earlier in 2010, Google ultimately decided to disallow China from using the search engine after the Chinese government pressured Google to censor multiple sites offensive to the government.\textsuperscript{275} Google reopened its services in 2012. Furthermore, Vincent Cerf, who is widely acknowledged as “the father of the Internet,” stated in 2012 that he does not believe the Internet is a universal human right.\textsuperscript{276} Rather, those who have access should be free to conduct their business without government intervention or restriction.

The argument over appropriate policies toward Internet access is ongoing. States and private sector firms alike participate in filtering and other censorship activities, and U.S. policies allow for executive powers to enforce significant access control, even if

\textsuperscript{271} Cramer 2013, 1081
\textsuperscript{272} Cramer 2013, 1081
\textsuperscript{274} Land 2013, 453
\textsuperscript{275} Cramer 2013, 1076
recent actions demonstrate a commitment to open, permanent access. Examining recent history reveals that filtering and blocking are more likely to occur when state authority or national identity is threatened, or perceived as threatened. The state also compels private sector technology companies to comply with state requests. Internet access will continue to remain a significant issue in Internet governance policy, since it has direct implications for a government’s ability to influence its people. It is supported by a multistakeholder model, but creates severe tensions across the international community as nations condone, condemn, or attempt to undermine each other’s’ approaches to controlling access.

**Surveillance**

A second key issue in Internet governance, related to Internet access, is surveillance. The U.S. still suffers from its historic intelligence failure in 2001, and cries in recent years of a potential Cyber Pearl Harbor to come have prompted the U.S. to build up its intelligence capability, including programs allowing it to spy on enemies and allies alike.\(^\text{277}\) Revelations of this surveillance capability, as well as the U.S. relative decline in influence, may signal a change in structure of the current Internet governance model.

States have benefited from private sector innovations in security technologies such as deep packet inspection and keyword-based filtering, which were created by private companies. These technologies are now used by nation-states to control the flow of information.\(^\text{278}\) Egyptian protesters during the Arab Spring discovered documents indicating arrangements for Egyptian security services to buy German-UK computer

\(^\text{278}\) Deibert and Crete-Nishihata 2012, 352
network exploitation services for government use.\textsuperscript{279} Furthermore, some authors have noted the “false choice…between Internet freedom and sovereignty,” since the U.S. conducts surveillance on Internet traffic, enforces content-filtering regulations, and on occasion asks service providers to provide or remove content.\textsuperscript{280}

Russia has a fundamentally different understanding from the U.S. of what constitutes cybersecurity and as a result, how to govern the Internet. Like China, Russia uses the term “information security” instead of cybersecurity, which includes the content of data packets in addition to the traffic mechanisms.\textsuperscript{281} As a result, it relies on surveillance and censorship as a security measure to ensure that content is approved. U.S.-Russia relations have also experienced heavy strain in the last few years. Not only does Russia perceive the U.S. as having an “imperial attitude,” believing itself to be the “sole superpower,” but Russia also harbored former NSA whistleblower Edward Snowden against the express wishes of the U.S., in a decision that condemned U.S. surveillance practices and weakened U.S. international power.\textsuperscript{282} Resistance to U.S. demands is part of a larger pattern of Russia establishing its dominance in Internet governance and foreign policy decisions.

Snowden’s public disclosures about controversial activity by the signals intelligence agency have had an impact on U.S. influence in international Internet policy fora as well. Revelations in 2013 about NSA surveillance activities on other governments, including Germany and Brazil, may detract from the U.S. stance of pushing for an open, free Internet. The argument for U.S. sponsorship of the current model may

\textsuperscript{279} Deibert and Crete-Nishihata 2012, 352
\textsuperscript{280} Shackelford 2013, 1312
\textsuperscript{281} Shackelford 2013, 1305
\textsuperscript{282} Kruger 2013, 50
continue to suffer blows as U.S. allies begin to argue that the U.S. is no longer a
trustworthy steward of the Internet, and that it “has done a disservice” to all people living
in surveillance states “by creating a new international norm that massive-scale
surveillance is acceptable.”

Gatherings in Internet fora such as the IGF and the ITU reveal “an emerging coalition” of states unhappy with U.S. behavior, now including
states traditionally more adversarial as well as U.S. friends. Specific examples of allies
distancing themselves from U.S. policies include the European Union, whose leadership
suggested terminating data-sharing agreements with the U.S. and “requiring American
website providers to prominently warn Europeans that their data is subject to U.S.
government surveillance.” Strained relationships with allies as well as with less
friendly nations suggests a decrease in U.S. bargaining power in these discussions and
consequently a decrease in influence over Internet governance discussions.

In December 2013, eight U.S. Internet technology companies including Apple,
Facebook, and Google, issued an open letter and launched a campaign advocating for
reduced U.S. surveillance activity. The letter stated that “The balance in many
countries has tipped too far in favor of the state and away from the rights of the
individual.” The collaborative effort is a significant step towards changing government
authority with respect to surveillance, and the companies’ call for international standards
of reasonable surveillance is an interesting glimpse of the multistakeholder model at

http://weeklywonk.newamerica.net/articles/breaking-the-internet/
284 Meinrath 2013
285 Meinrath 2013
surveillance-of-users.html?pagewanted=all
287 Wyatt and Miller 2013
work, with private sector players suggesting changes in state behavior. Furthermore, the private sector actors are advocating normalization of “practices and laws regulating government surveillance of individuals and access to their information.” This policy position illustrates the tension existing between the U.S. government and its private sector relationships, and may also open the door to additional discussions of Internet regulation in the international community.

Analysis

In this section, I discuss the implications for the U.S. role based on the contradictory behaviors outlined in the case studies. In 2011, the U.S. State Department began a program to equip dissident or minority communities in foreign nations with “shadow” Internet access, or “Internet in a suitcase.” This is the latest of many efforts to provide concealed wireless networks and anonymization software to citizens in other countries with significant access restrictions.\(^{288}\) Then-Secretary of State Hillary Rodham Clinton explained that “There is a historic opportunity to effect positive change, change America supports,” referring to the U.S. ideology about what constitutes reasonable Internet access for citizens around the globe.\(^{289}\) The State Department has supported these efforts as “promoting free speech and human rights for their own sake, not as a policy aimed at destabilizing autocratic governments,” but the governments may perceive them as the latter. The multistakeholder model supports varying state behavior with respect to access by allowing each country to exert its own preferred degree of control, but still allows international criticism from other stakeholders that prefer a more open regime.


\(^{289}\) Glanz and Markoff 2011
Continuation of the U.S.-led multistakeholder model implies that additional technologies and efforts like the Internet in a suitcase will continue, which can cause anxiety and resentment in the foreign governments that are enforcing the restrictions.

The primary distinction between surveillance behaviors across states is that U.S. surveillance programs focus mostly on monitoring foreign nations in order to secure its authority, whereas other nations conduct internal surveillance to maintain a pulse on domestic unrest and identity. Nevertheless, the distinction is too nuanced to let the U.S. escape international criticism. The Snowden revelations may be serving as a “Black Swan” event, a rare event with massive consequences powerful enough to change the prevailing wisdom.\footnote{Taleb, Nassim Nicholas. 2010. The Black Swan. New York: Random House. xxii.} Commentators suggest that only major reforms including restraints on U.S. intelligence and surveillance capabilities can restore trust in the U.S.-led model.\footnote{Meinrath 2013} Otherwise, the recent suggestions made by the U.S. Internet companies may signal an increased appetite for additional boundaries around international behavior more reminiscent of the third, regulated model.

The two examples of U.S. behavior related to Internet access and surveillance may severely damage U.S. bargaining power. Ironically, the debate over Internet access demonstrates the unprecedented power that the Internet gives to an individual. States are aware of this transfer of power, and surveillance of that user’s activity strips that power away. The issue of surveillance highlights the fundamental tension that exists between the argument for a U.S.-led model and the argument for a regulated model. Concerns about the U.S. government’s ability to limit the scope of its own surveillance activities cast significant doubt about its ability to remain the steward of the Internet. As the key
proponent of global Internet access, the U.S. cannot also be the world’s premiere surveillance capability. The two are at odds, and this contradiction makes Internet access appear to be an illusion. The access-surveillance contradiction indicates the third model of regulated governance may be the most likely, though as surveillance capabilities decrease across governments, willingness to allow full access may decrease as well.

**Conclusion**

Arguments about Internet governance are about bids for supremacy. States anxious about retaining their authority are more likely to engage in controlling behaviors, whether that includes limiting Internet access or conducting massive-scale surveillance. The Internet provides states with new tools to assess state authority and control, and cooperation from private sector actors supports this behavior. Examining U.S. behavior reveals contradictory conclusions. U.S. democracy-building efforts to increase Internet access align with traditional U.S. values of civil liberties, but U.S. surveillance programs reveal that open access does not mean freedom or trust, and might even come at the cost of privacy. This contradiction will weaken possibilities for the U.S. to maintain its role as steward of the multistakeholder model, and may even signal additional international regulations or norms more in line with the third, regulated model. Maintaining state authority and national identity are constant characteristics of states in the international system, and states including the U.S. will adapt to find other ways of securing both of these elements if access and surveillance no longer provide them.
CONCLUSION

Global use of the Internet reveals a near universal trust in it. Examining a few of the areas where researchers, institutions, and states are learning that the Internet is not so trustworthy shows that security still lags behind the capability to exploit. This thesis focused on three different aspects of eroding trust in the Internet: authentication problems with certificate authorities, weaknesses in Internet routing, and political risks to the U.S. ability to shape solutions. Looking across these three examples, one is struck by the need for trust to support the virtual, physical, and political aspects of the Internet.

Many of the security measures recommended in the literature and captured here will no longer be on the cutting edge in a short while, since threats, vulnerabilities, consequences, and risk mitigation strategies are constantly changing. The nature of Internet security and Internet governance is evolving; it has not stopped expanding and transforming since it was first created. In fact, many of the issues discussed when the first chapter was written in August 2013 are already in need of updates.

On April 7, 2014, researchers revealed Heartbleed, a vulnerability in the OpenSSL technology commonly used to encrypt websites. Not only was Heartbleed one of the most acute flaws in SSL to date because of its ubiquitous presence in websites all over the Internet, Heartbleed raised critical issues. First, it revealed that cyber criminals stole and held private SSL keys, so these actors may still have the capability to impersonate a transacting party without triggering an alarm by a certificate authority, at least while organizations are reissuing certificates, which takes time. Second, Heartbleed was widespread and pervasive enough that it prompted a near-global education campaign on the vulnerabilities of storing personal data online and recommended protections. Many
of these recommendations reiterated the conclusions drawn in Chapter One about specific actions for the authorities themselves, but they also provide updated context for the web’s system of trust.

In the system of authentication, certificate authorities serve as third parties that use public key infrastructure technology to verify two parties that wish to transact with each other. Many U.S. certificate authorities pay accounting firms to validate them and make websites inclined to include them in their list of trusted entities. However, certificate authorities are still a global, poorly understood market, and no central mechanism provides or enforces a code of conduct. Many governments own certificate authorities or have the power to distribute subordinate certificates. Complicating this problem is that attacks on certificate authorities often have cascading effects that end users do not understand. Because certificate authorities are the entities that guarantee trust in web connections, a compromised authority results in compromised web access.

This chapter examines some of the recommendations for increasing accountability for private security companies in order to apply them to certificate authorities. The most salient recommendation may be creating “communities of fate,” where member organizations create and hold each other accountable to norms of professionalism, similar to mechanisms used by legal and medical communities to identify and bar bad actors from practicing. However, a robust, active international community of certificate authorities, along with increased user awareness, needs to emerge before this community will be able to influence changes in behavior. One of the best models to develop so far is the accounting-led WebTrust. Establishing regional bodies or offices of WebTrust, supported by regional consortia and national governments, would help turn digital
certificate security into an international priority. With this context in mind, Heartbleed provided a baseline of understanding that the Internet is not secure, and may pave the way for future awareness efforts to help educate companies of all sizes as well as the general public to help correct the Lemons problem.

If public and private sector leaders, including the U.S. government and the largest certificate authorities do not work together to grow market mechanisms to hold certificate authorities accountable, the Lemons problem could reach its natural outcome where bad certificates flood the market and drive out the good certificates. This scenario would likely result in an uptick in cybercrime, since criminals could more easily spoof websites and access customer information. Over time, weak certificate authorities could degrade trust in e-commerce in general, possibly resulting in decreased global e-commerce and negative impacts on the global economy. However, the more popular this issue becomes and the bigger and more frequent the breaches that occur, the more likely the market is to create solutions. Hopefully it will do so before trust in e-commerce is irrevocably damaged.

Chapter Two highlights how recent threats to BGP include deliberate attempts by patient, organized actors. Threats are not staying limited to misconfiguration or even states looking to censor their own people, but are possibly expanding to include state entities conducting surveillance on other states. Furthermore, proposed solutions to these vulnerabilities are either too expensive or resource-intensive to be market viable, or they stop short of accounting for the state actor deliberately eavesdropping on traffic. While consequences of BGP eavesdropping remain low, the likelihood that states and cyber criminals decide to experiment with this capability could increase. Many security
professionals claim that fearing the state actor is alarmist, but only recently has this threat been observed in the wild. Whether the Belarus and Iceland attacks will remain the only example remains to be seen, but risk mitigation activities should expand to address this type of threat in the meantime, including through technical security solutions to BGP and greater awareness of the threat by ASes.

While the potential for exploit is not new, the threat environment and trust in Internet security has changed significantly, making this type of routing attack more of a concern. Examining different trust frameworks from social theory illuminates different styles of security solutions: those that seek to increase trust among peers and distributed networks, and those that seek to increase trust in hierarchy by ascribing more power to those at the top of a hierarchy. This chapter concludes that one form of trust also influences the other, and while some of the solutions posed are viable and some are gradually being deployed, their effects on how trust affects commercial, regulatory, and state relationships should be studied more in depth. One of the potential solutions is building security into the protocols so that peers are more likely to trust each other if they are using BGP security solutions. This topic should remain a priority in IETF working groups as well, which should study the current solutions through the lens of the Belarus incident to identify gaps.

If BGP routing does not become more secure, cyber crime is likely to increase as actors discover how to manipulate the system of trust. States may also be more likely to reroute traffic to snoop or manipulate it before sending it on its way, especially as kinetic conflicts arise. This may temper dissident use of the Internet to communicate, at least on unencrypted networks. Only a few security firms currently monitor BGP activity around
the globe, but if deliberate rerouting continues, service providers should examine folding this issue into their security portfolios to develop a practitioner community focused on BGP security.

Chapter Three puts the two examples of encryption and authentication into perspective by examining the policy angle. Internet governance bodies like ICANN manage some of the functions of the global Internet, and at the time this paper was published in December 2013, the U.S. was still advocating for a multistakeholder model of governance. However, because governance of Internet functions does not rely on a hierarchy of state governments, the question of what effective governance looks like in an age of increasing threats is an important one. International forums and discussions held after December 2013 will inform and perhaps revise the conclusions in this chapter, as the first fallout from the Snowden revelations is arguably over. The discussion of Internet stewardship began to transition from alarmist discourse on moving to intrastate infrastructure to a more tempered dialogue, albeit with an undercurrent of doubt in the U.S.

Examining two case studies of state behavior provides more detail on where the U.S. is likely to experience challenges. Currently, states are conducting domestic surveillance and blocking access to the Internet, and U.S. policy positions are unfortunately contradictory. U.S. policies on controlling Internet access reflect the 1934 Communications Act’s concepts of executive intervention during time of war. This language, as well as the appearance of draft legislation to define emergency powers on the Internet, may have undermined trust in the U.S. ability to govern the Internet fairly without compelling ISPs and other producers and providers to serve state interests. The
National Security Agency surveillance activities pale in comparison to activities of more authoritarian states that unapologetically consider monitoring and ensuring “information security” in the state’s national interest. However, the U.S.’s hawkish policy positions and ambiguous civil dialogue on acceptable levels of surveillance weaken its clout in multilateral forums. Together, these two examples of contradictory behavior indicate that the U.S. ability to win allies and persuade other nations of its policies may not be strong for long.

We can use the trust framework discussed in Chapter Two to examine the U.S. ability to steer Internet governance. As vertical trust in the U.S. reputation decreases, trust is also likely to decrease in other peer relationships among states. Many government agencies and delegations represent the U.S. in international forums, so further study should pursue how agency reputations evolve in this environment. In this context, horizontal trust among peers can represent trust that other nations, individuals, and companies place in each other. If trust continues to decrease in the U.S., states may seek to build trust elsewhere, such as through creating national Internets such as the one suggested by Brazil. A Balkanized Internet made up of intrastate networks would significantly impact global e-commerce and also create new vulnerabilities, and may in the long term create demand for a completely new Internet relying on new protocols. The more realistic scenario is that states will become more likely to increase or revise their intelligence budgets to anticipate, protect from, or compete with foreign surveillance.

Regardless of U.S. shortcomings in stewarding Internet functions and providing a policy framework, its system of government still provides one of the world’s most effective examples of separation of powers and checks and balances. As a result, the U.S.
should help devise and champion the accountability structures for any future multistakeholder models to ensure public policy issues as well as address allocation functions remain as free from state influence as possible. This would assist in cementing vertical trust in an accountability authority, which in turn would have a positive effect on the participating peer relationships.

It is not inevitable that trust in the Internet will completely dissipate. But as problems emerge in the virtual, physical, and policy levels of the Internet, it is apparent that the Internet is not trustworthy. At the same time, Internet use and applications are continuing to evolve. For example, the Internet of Things is ushering in a new generation of devices that will place more demands on Internet capability while requiring a new layer of trust. If we step back from appreciating the connectivity, innovation, and power the Internet confers on its users, we realize that it all depends on preserving this trust. Solutions should not only address some of the technical concerns, but attempt to understand and accommodate the shifting web of trust dynamics.
BIBLIOGRAPHY


http://www.economist.com/node/16941635

“At UN debate, Brazilian President urges protection of Internet users.” 2013. UN News Centre, September 24.  


http://www2.safenet-inc.com/email/2014/dp/GlobalCustomerSentiment/index.html#631

http://www.pewinternet.org/2014/04/30/heartbleeds-impact/

http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf


http://online.wsj.com/news/articles/SB100014240527023038222045777470532859210296


http://mitpress.mit.edu/sites/default/files/titles/content/9780262514354_sch_0001.pdf


http://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf


Electronic Frontier Foundation. 2010. EFF SSL Observatory.
https://www.eff.org/observatory


Healey, Jason. 2014. “Cyber Conflict.” Discussion at the RSA Conference, San Francisco, California, February 27.


BIOGRAPHY

Adrienne Marlena Allen is a Master of Arts candidate in Global Security Studies at Johns Hopkins University. Born in Washington, DC in 1983, Ms. Allen graduated from the University of Virginia with a Bachelor of Arts in English in 2005 and received a Graduate Certificate in Applied Intelligence from Mercyhurst University in 2010. Ms. Allen is a cybersecurity policy analyst at Booz Allen Hamilton, and specializes in national level cyber risk management, cyber incident response planning, and homeland security. She lives in Washington, D.C. with her husband Matt.