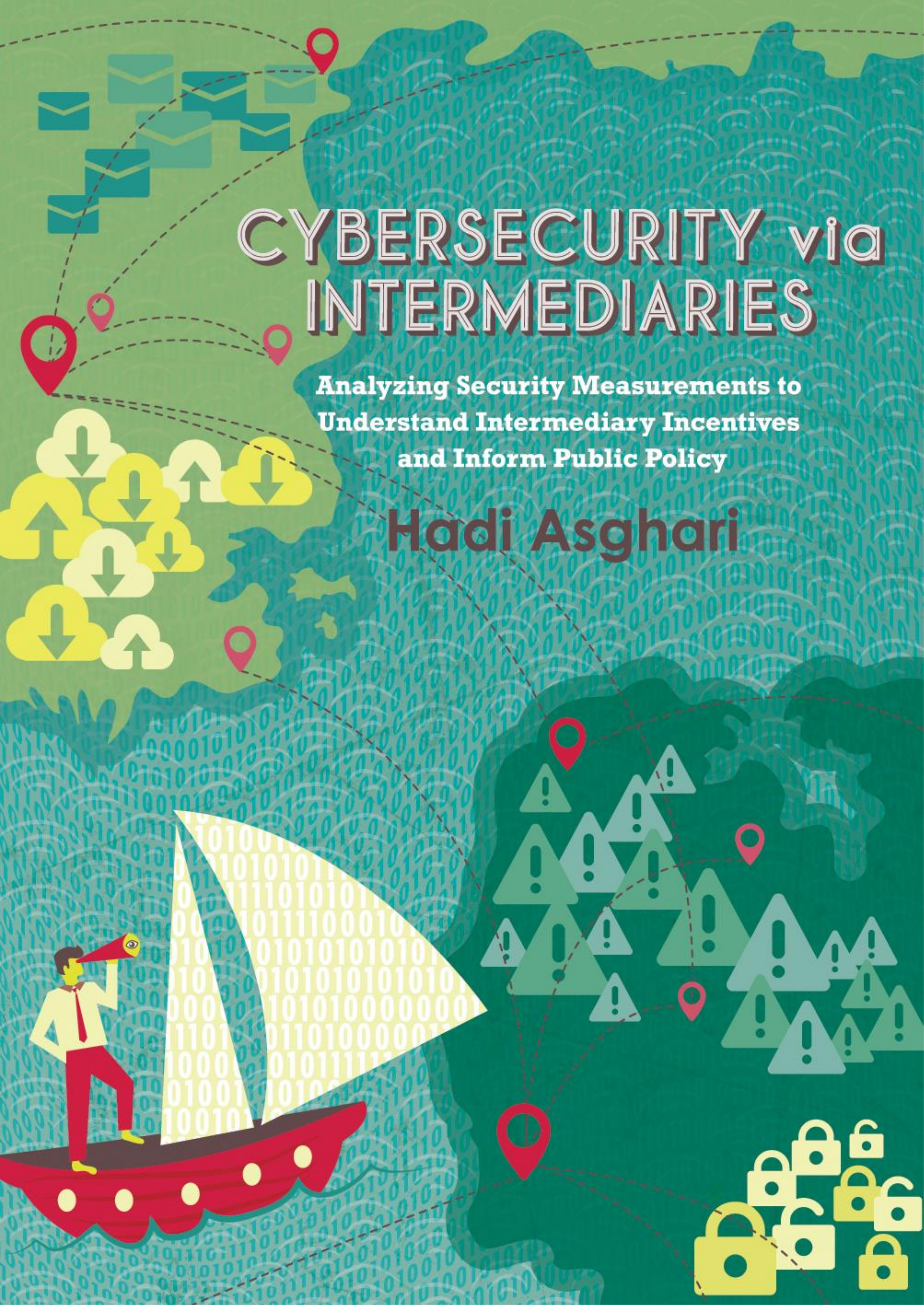
CYBERSECURITY via INTERMEDIARIES

Analyzing Security Measurements to Understand Intermediary Incentives and Inform Public Policy

Hadi Asghari



Cybersecurity via Intermediaries

Analyzing Security Measurements to Understand Intermediary Incentives and Inform Public Policy

PROEFSCHRIFT

ter verkrijging van de graad van doctor
aan de Technische Universiteit Delft,
op gezag van de Rector Magnificus prof. ir. K.C.A.M. Luyben,
voorzitter van het College voor Promoties,
in het openbaar te verdedigen op 29 februari 2016 om 15:00
door

Hadi ASGHARI

Master of Science in Management of Technology
geboren te Teheran, Iran

This dissertation has been approved by the promoter:

Prof.dr. M. J.G. van Eeten

Composition of the doctoral committee:

Rector Magnificus	Chairman
Prof.dr. M. J.G. van Eeten	Promoter
Independent members	
Prof.Dr.-Ing. R. Böhme	University of Innsbruck
Prof.dr. M. L.P. Groenleer	Tilburg University
Prof.dr.ir. H. J. Bos	VU Amsterdam
Prof.dr.ir. J. van den Berg	TU Delft
Prof.dr. J. P.M. Groenewegen	TU Delft
Dr. J. J. Vereijken	ING

ISBN 978-94-6233-244-7

Cover design: Erin Holmberg

This research has been funded by the Netherlands School of Public Administration (NSOB), the Netherlands Ministry of Economic Affairs, and the Next Generation Infrastructures (NGInfra).

Distributed by Delft University of Technology, Faculty of Technology, Policy and Management, Jaffalaan 5, 2628BX Delft, the Netherlands.

Printed in the Netherlands by GildePrint.

This dissertation is available online at http://repository.tudelft.nl.

Keywords*:* cybersecurity, economics, governance, technology policy, Internet measurement, ISP, botnet, deep packet inspection, certificate authority, data science.

When my heart's ardor oft was unrestrained,

Me thought few mysteries unsolved remained,

Seventy-two years I've pondered every day,

And know none hath the true solution gained.

Omar Khayyam (12th century)

Table of Contents

List of Figures

List of Tables

Summary

The Internet has enabled tremendous economic and social innovation in the past decades. At the same time, rarely a month passes without hearing news about a large-scale cyber-attack. These security failures are driven by vulnerabilities in the underlying infrastructure, human mistakes, and massive interdependencies. A typical organizational network runs hundreds of services and thousands of devices that execute millions of lines of code. Any part of this code may have vulnerabilities that can lead to a security breach.

It seems improbable that we can eliminate all vulnerabilities and obtain security via technology alone. In recent years, interdisciplinary research has clarified the many economic and behavioral dimensions of security. Examining the incentives of attackers and defenders has helped explain why certain security failures occur and others not. This consequently allows assessing the effectiveness of technologies and policies to improve security. Moreover, preventative measures are costly, and organizations need to make tradeoffs on what to protect. The core of this research is rooted in the field of *Information Security Economics.*

One of the most promising areas of research in the field has concentrated on the incentives and role of Internet intermediaries. Intermediaries are organizations that provide the Internet's basic infrastructure and platforms, and enable communications and transactions between third parties and services. Examples include broadband providers, payment systems, and search engines. The role of intermediaries has gradually increased in the Internet ecosystem. Their scale, centrality, access to users, and capabilities has made them focal points for public policy and governance. This is also the case for cybersecurity.

Security incentives of intermediaries are mixed. Sometimes, they see cybersecurity as a necessity to maintain user trust; other times, they see it as costs to avoid. Public policy that wishes to improve cybersecurity needs a sharp understanding of the behavior and incentives of intermediaries. This information might be traditionally gathered through surveys

and expert interviews. The biggest drawback of such methods is that they collect *opinions* or reputations that might or might not correspond to the actual behavior or incentives. Luckily, we can do better, as we have entered an era of abundant data. Machines on the Internet continuously record various aspects of network security and incidents. This leads to the dissertation's research question:

What can security measurements tell us about internet intermediary behavior? What incentives explain these behaviors, and how do firm characteristics, market forces, and regulatory conditions shape these incentives? What does this imply for cybersecurity policy?

Using metrics to make policies has many advocates, including in the security community. However, two key difficulties have kept researchers with access to the security data – computer scientists – away from rigorous policy work. The first is that security data contains information about technical identifiers, such as IP addresses or autonomous system numbers, which map imperfectly to real world entities such as machines or companies. Often, they are simply assumed equivalent, as no clear, easy, or consistent conversion exists. The second difficulty is that linking security metrics to incentives requires critical thinking about the measurement and the underlying phenomenon. Examples include reporting the number of security incidents in a network, without considering its size, or including variables in a model that cannot possibly be causally explained. Such mistakes would be sins for many quantitatively trained social scientists. One explanation is that the policy sections of many computer science papers are written as proof-of-concepts, with the researcher's core interest and expertise lying in the technology and measurement. However, when the goal is to contribute to the policy debate and answer substantive questions, then careful thinking about causal mechanisms, incentives, and dealing with real world mess is necessary.

The dissertation tackles these difficulties, and answers the research question through four peer-reviewed empirical studies, each addressing a separate substantive policy question; a literature review contribution to an edited volume; and a peer-reviewed methodological reflection paper. The empirical studies addressed topics chosen among urgent cybersecurity debates involving intermediaries. They included longitudinal and cross-country datasets, methodological innovations, and manual mapping of technical identifiers to the real world. They revealed new insights, and serve as examples on how public policy can be formed using security measurements. The studies were well received in academia, and the findings incorporated in industry discussions and policy development, validating the approach. Summaries of the studies follow.

Chapter 3 studies *the role of Internet Service Providers (ISPs) in mitigating botnets*. Using two global and longitudinal datasets of botnet activity (consisting of approximately 150 and 300 million unique IP addresses), we estimated infection rates for ISPs in sixty countries, and supplemented this with market data. We found that well-established ISPs in relatively well-governed jurisdictions control the bulk of the bots. There are dramatic differences in infection rates among ISPs, suggesting discretion to enhance mitigation. Large ISPs have lower infection rates, pointing to the positive role of automation in handling infection reports and lower costs per cleanup. Finally, we observed that regulatory involvement incentivizes ISPs to spend more efforts on mitigation.

Chapter 4 studies *the success of national anti-botnet initiatives (ABIs) in cleanup of Conficker bots.* Conficker is one of the largest botnets ever seen, and despite successful efforts in reverse engineering its code, releasing software patches, and dismantling the control infrastructure, hundreds of thousands of bots remain infected. We transformed six years of noisy sinkhole data into parameters that capture infection trends across 62 countries; and determined whether countries with ABIs had different growth, peak, or decay rates. We found that two institutional factors, the general level of ICT development and the prevalence of unlicensed software, influenced Conficker spread and mitigation more than ABIs. The success of ABIs in cleaning old bots hinges on more factors.

Chapter 5 studies *vulnerabilities in the Certificate Authority (CA) ecosystem and reflects on proposed technical and legal fixes*. We analyzed two datasets that had collected all TLS/SSL certificates on the public web (approximately 1.5 and 3 million certificates), and connected this with certificate prices. We found many CAs, a highly concentrated market—with three companies controlling 75% of the market globally. And most surprisingly, up to a factor of ten price difference for identically secure certificates. We found perverse incentives at work, with the major CAs benefiting from the systematic vulnerabilities. As the misaligned incentives are caused by a technical design failure, without a technical fix, regulation cannot succeed.

Chapter 6 studies *ISP incentives to deploy Deep Packet Inspection (DPI) for bandwidth control*. We processed logs of a crowd-sourced test that determines whether ISP's use DPI to restrict peer-to-peer file sharing (approximately 800,000 tests). We found that despite the public and regulatory unease about the technology, more than two thirds of ISPs used DPI, at least for bandwidth management. Using multivariate modelling, we further found that DPI use was higher in countries with Internet filtering. The two are not directly linked. This suggests that some ISPs piggybacked on the norm of interfering with network traffic for their own agenda. We also observed once more that ISPs have considerable discretion. DPI varied significantly, even among ISPs that operate in the same country, i.e., under similar market and regulatory conditions.

The dissertation concludes by reflecting on the broader regularities among the studies. I reflect on the process of analyzing security measurements to extract behavior and incentives. I present two tools that I developed and are now used by other researchers: *pyasn* to determine which technical entity historically owned an IP address, and an *AS-to-ISP map* to link those technical entities to actual ISPs. Measurement-sets need to have certain features be usable for policy research. I discuss these in a reflection paper that was peer-reviewed by, and presented to, an audience of measurement experts.

Concerning the implications for cybersecurity policy, I conclude that cybersecurity can be improved by understanding and aligning the economic incentives of Internet intermediaries. This is actionable for policymakers and regulators, and may be more effective than alternatives, such as raising awareness among consumers and businesses, or mandating specific technical solutions. The policy mechanisms for alignment need not be law. Softer mechanisms, such as regulatory guidance, or facilitating positive or negative reputation effects, may work better in some situations. In each case, measuring, analyzing, and understanding the properties of these markets and the incentives of its players is critical to developing effective cybersecurity policies.

Samenvatting (Dutch Summary)

Het internet heeft de laatste decennia een enorme economische en sociale innovatie mogelijk gemaakt. Tegelijkertijd gaat er geen maand voorbij zonder nieuws over een cyber-aanval op grote schaal. Dit falen in veiligheid worden veroorzaakt door kwetsbaarheden in de onderliggende infrastructuur, door menselijke fouten, en door massale wederzijdse afhankelijkheden. Een typisch organisatienetwerk ondersteund honderden diensten en duizenden apparaten die miljoenen regels computer code uitvoeren. Een deel van deze code kan kwetsbaar zijn en dat kan leiden tot een bres in de veiligheid.

Het lijkt onwaarschijnlijk dat we alle kwetsbaarheden kunnen uitbannen en veiligheid kunnen verkrijgen via de techniek alleen. Recent interdisciplinair onderzoek heeft economische en gedragsdimensies van internetveiligheid verhelderd. Het bekijken van de prikkels waaronder aanvallers en verdedigers werken helpt verklaren waarom het soms mis gaat en soms niet. Dit maakt het vervolgens mogelijk om de effectiviteit van veiligheidstechnologieën en -beleid te evalueren en verbeteren. Veiligheidsmaatregelen zijn kostbaar. Organisaties maken afwegingen over wat ze willen beschermen en hoe. De kern van dit onderzoek is geworteld in *information security economics*.

Deze dissertatie draagt bij aan dit veld. Een van de meest veelbelovende onderzoeksgebieden in het veld heeft zich geconcentreerd op de prikkels en rol van zogenaamde *internet intermediaries*. Intermediaries zijn organizaties die de basale infrastructuur en platforms van het internet aanleveren, en de communicatie mogelijk maken tussen derde partijen en diensten. Voorbeelden zijn breedband-aanbieders, betalingssystemen, en zoekmachines. De rol van intermediaries is gaandeweg groter geworden in het ecosysteem van het internet. Hun schaal, belang, toegang tot gebruikers, en bekwaamheid heeft hen de focus gemaakt van veel beleids- en governance-studies. Dit is ook het geval voor cyberveiligheid.

De percepties voor een beter veiligheidsbeleid van intermediaries verschillen. Soms ziet men cyberveiligheid als noodzakelijk om het vertrouwen van de gebruiker te waarborgen; en soms ziet men het als een kostenpost om te vermijden. Beleid dat graag de cyberveiligheid zou willen verbeteren heeft een scherp begrip nodig van het gedrag en de prikkels van intermediaries. Deze informatie zou traditioneel vergaard worden door enquetes en interviews met experts. De grootste tekortkoming van zulke methoden is dat men meningen of reputaties vergaard die al dan niet corresponderen met het daadwerkelijke gedrag of de prikkels. Gelukkig kan dit beter, aangezien we een tijdperk van overvloedige data zijn binnengetreden. Machines op het internet leggen continue allerlei aspecten van netwerkveiligheid en incidenten vast. Dit leidt tot de onderzoeksvraag van de dissertatie:

Wat kunnen veiligheidsmetingen ons vertellen over het gedrag van internet intermediaries? Welke prikkels verklaren dit gedrag, en hoe worden deze gevormd door de eigenschappen van bedrijven, markten en regulering? Wat impliceert dit voor cyberveiligheidsbeleid?

Het gebruiken van *metrics* om beleid op te zetten heeft veel voorstanders, ook in de veiligheidsgemeenschap. Toch zijn er twee knelpunten die onderzoekers met toegang tot de meetdata – computerwetenschappers – ervan hebben weerhouden om relevant beleidsonderzoek te doen. Het eerste knelpunt is dat veiligheidsdata informatie bevat over technische identiteiten, zoals IP-adressen of *Autonomous System* nummers. Deze verhouden zich niet een-op-een tot objecten of actoren in de echte wereld, zoals machines of bedrijven. Vaak worden deze identiteiten simpelweg gelijkgesteld, omdat er geen makkelijke en automatiseerbare manier bestaat om ze accuraat te koppelen.

Het tweede knelpunt is het koppelen van veiligheidsmetrics aan gedragsprikkels. Dat vereist kritisch denkwerk over de relatie tussen de data en het onderliggende fenomeen – zoals de veiligheidsprestatie van een actor. Zo wordt bijvoorbeeld het aantal veiligheidsincidenten in een netwerk gerapporteerd zonder de grootte van het netwerk mee te wegen, of worden er variabelen meegenomen in een model die met geen mogelijkheid causaal te verklaren vallen. Zulke fouten zouden door veel kwantitatief getrainde sociale wetenschappers als methodologische zondes gezien worden. Een verklaring voor dit soort fouten is dat de beleidsaanbevelingen van veel computerwetenschapspapers geschreven zijn als een soort *proof-of-concept*, om te laten zien dat het in principe mogelijk is, maar zonder de bovenstaande knelpunten op te lossen. De echte interesse en expertise van deze onderzoekers ligt in de technologie en het bouwen van meettechnieken. Als het doel is om bij te dragen aan het beleidsdebat en het beantwoorden van inhoudelijke vragen, dan wordt het noodzakelijk om veel preciezer na te denken over de causale mechanismen, de prikkels, en het rekening houden met de inherente rommeligheid van de complexe empirie.

Deze dissertatie behandelt deze moeilijkheden, en beantwoordt de onderzoeksvraag door vier *peer-reviewed* empirische studies die elk een ander inhoudelijke beleidskwestie adresseren; een literatuurstudie dat als hoofdstuk is geaccepteerd voor een *edited volume*; en een *peer-reviewed* paper dat reflecteert op methodologie. De empirische studies focussen op enkele urgente cybersecurity debatten rondom de rol van intermediaries. Allen bevatten een vergelijkende studie tussen een paar dozijn landen met een longitudinaal benadering; enkele methodologische innovaties; en het grondig en handmatig in kaart brengen de relatie tussen technische identiteiten en actoren in de echte wereld. Ze geven nieuwe inzichten, en dienen als voorbeelden over hoe publiek beleid kan worden gevormd via *security*-metingen. De studies hebben breder ingang gevonden in discussies tussen industrie en overheden. Dat onderstreept de waarde van de gevolgde aanpak. Samenvattingen van de studies volgen hier onder.

Hoofdstuk 3 bestudeert *de rol van de Internet Service Providers (ISPs) bij het bestrijden van botnets.* Met twee mondiale en longitudinale datasets over botnet activiteit (het betreft ongeveer 150 en 300 miljoen unieke IP-adressen), schatten we hoe geïnfecteerd ISP's zijn in zestig landen, en we koppelen dit aan data over de markten van deze ISP's. We ontdekten dat gerenommeerde ISP's in goed bestuurde jurisdicties het merendeel van de bots in hun netwerken hebben, en dat er dramatische verschillen zijn in de infectiegraad tussen de ISP's. Dit suggereert dat ISP's zelf invloed hebben op de omvang van het probleem. Grote ISP's hebben, gemiddeld, een lagere infectie-graad. Dit wijst op de positieve invloed van automatisering in het behandelen van besmette machines, waardoor de kosten voor het opruimen lager zijn. We vonden ook bewijs dat regulering helpt om ISP's meer aandacht aan bestrijding te laten besteden.

Hoofdstuk 4 beschrijft *het succes van anti-botnet initiatieven (ABI's) in de schoonmaak van Conficker bots.* Conficker is een van de grootste botnets ooit gezien, en ondanks succesvolle pogingen om de Conficker code te ontcijferen, om software patches uit te brengen, en het ontmantelen van de Conficker infrastructuur, zijn er nog steeds honderdduizenden bots geïnfecteerd. We transformeerden zes jaar aan *sinkhole* data die veel ruis bevatte in robuuste tijdseries data, zodat we trends in de infecties kunnen modeleren in 62 landen. We onderzochten of de landen met ABI's een ander patroon van groei, piek en verval hebben. We ontdekten dat institutionele factoren (zoals de kwaliteit van ICT-infrastructuur) de verspreiding en beperking van Conficker meer beïnvloeden dan ABI's. Het succes van ABI's in het opschonen van bots hangt dus af van additionele factoren.

Hoofdstuk 5 bestudeert de *kwetsbaarheden in het Certificate Authority (CA) ecosysteem en verkent technische en juridische oplossingen voor deze problemen.* We analyseren twee datasets die alle TLS/SSL certificaten hebben verzameld op het publieke web (ongeveer 1.5. en 3 miljoen certificaten) en hebben deze verbonden met de prijzen van de certificaten. We vonden veel CA's, maar ook een zeer geconcentreerde markt (drie bedrijven hebben 75% van de mondiale markt in handen). Ook ontdekten we, zeer verrassend, dat er grote prijsverschillen bestaan voor certificaten die technisch gezien identiek zijn. We vonden perverse prikkels. De grote CA's hebben profijt van de kwetsbaarheden in het systeem. Aangezien er aan de verkeerde prikkels een technische kwetsbaarheid ten grondslag ligt, kan regulering zonder technische oplossingen niet slagen.

Hoofdstuk 6 bestudeerde *het gebruik van Deep Pack Inspection (DPI) door ISP's voor de beheersing van het verkeer op hun netwerken.* We verwerkten ongeveer 800.000 logbestanden van een gecrowdsourcete test die vaststelt of ISP's DPI gebruiken om peer-to-peer file sharing te beperken. We ontdekten dat meer dan tweederde van de ISP's DPI gebruiken voor beheersing van de bandbreedte van het verkeer van gebruikers, ondanks het bedenkingen die hiertegen bestaan onder consumenten en toezichthouders. Door gebruik te maken van multivariate modelering, vonden we verder uit dat DPI gebruik hoger was in landen die internetverkeer inhoudelijk censureren. Censuur en beheersing van bandbreedte zijn niet direct aan elkaar verbonden. Dat we ze toch gezamenlijk aantreffen, suggereert dat sommige ISP's meeliften met op de wettelijke plicht tot censuur om tegelijkertijd het netwerk te beheersen voor hun eigen agenda. We zagen ook dat, net zoals bij de botnet studie, ISP's veel beslissingsruimte hebben. DPI verschilde significant, zelfs tussen ISPs die in hetzelfde land opereren, dus onder gelijke marktcondities en regels.

De dissertatie sluit af door te reflecteren op de van de onderzoeksvraag en de bredere patronen die in de studies gevonden zijn. Ik reflecteer op wat ik geleerd heb over het analyseren van veiligheidsmetingen met het oog op het identifceren van gedrag en prikkels. Ik bied twee open-source tools aan die ik ontwikkeld heb en die nu door andere cybersecurity-onderzoekers worden gebruikt: *pyasn*, een tool om vast te stellen welke technische entiteit ooit eigenaar was van een IP-adres, en een *AS-to-ISP map*, de deze technische identiteiten (IP adressen en AS nummers) aan ISP's verbindt. Technische meetdata hebben bepaalde eigenschappen nodig om bruikbaar te kunnen zijn voor beleidsonderzoek. Een eerder hoofdstuk reflecteerde hierop.

Wat betreft de implicaties voor cybersecurity beleid, concludeer ik dat cybersecurity verbeterd kan worden door het empirisch in kaart brengen van de prikkels van Internet intermediaries en deze vervolgens meer in lijn met de beleidsdoelen rondom cybersecurity te brengen. Dit biedt handelingsperspectieven voor beleidsmakers en toezichthouders die wellicht effectiever zijn dan de alternatieven, zoals het voorlichten van consumenten en bedrijven, of het aanbevelen of opleggen van specifieke technische oplossingen. De beleidsmechanismen voor het afstemmen van prikkels hoeven niet per se via wetgeving; zachtere mechanismen, zoals aandacht van toezichthouders of het faciliteren van positieve en negatieve reputatie-effecten via transparante benchmarks kan al effectief zijn. In elke situatie bleek het cruciaal om de eigenschappen van de markten en de prikkels die daarin werkzaam zijn te meten, te analyseren, en te begrijpen als basis voor effectief cybersecuritybeleid.

Doctoral Propositions

1. Cybersecurity is about attacker and defender incentives, as much as it is about technology. Public policy seeking to improve security should target incentives; technology follows. Organizations seeking to improve security should foremost hire and empower security talent; technology follows.

2. Intermediaries, the companies providing the Internet's infrastructure and platforms, often care about cybersecurity, but in selective ways driven by their incentives. Research can uncover these incentives and public policy can correct the biases that emanate from them.

3. New cybersecurity legislation is not always necessary for incentivizing intermediaries. Policy mechanisms such as regulatory guidance, extending duty of care, and facilitating positive or negative reputation effects, have been found to be effective under certain conditions.

4. Security is a tradeoff, and more is not always better. An empty bazaar, free of theft, is worse than a vibrant one, with the occasional thief. To be socially optimal, tradeoffs should reflect the full range of costs and benefits of additional security.

5. Cybersecurity recommendations (such as proposition #3 and #4) are too generic to shape actual policies. Measuring, analyzing, and understanding the behavior and incentives of actors involved in a particular market is necessary to develop effective policies.

6. The real world is messier than what many security models acknowledge, rendering them impractical. The following rules of thumb help balance rigor and practicality. First, engage with practitioners. Second, assume regional homogeneity if necessary, but not a global one. Third, expect data wrangling.

7. Interdisciplinary Internet research produces novel insights by applying practices and theories of one field to another. This might not appeal to the native fields, as it is not specialized. I advocate starting early: expanding the number of multidisciplinary minors and encouraging students to join.

8. Ubiquitous data collection and improved statistical tools are creating a paradigm shift and leading us toward a scientific revolution. The horizon is both exciting and troubling. A key question that shapes this future is: who owns the massive troves of data?

9. Online privacy will be much harder to solve than cybersecurity. There is no clear antagonist and the term means many things. Furthermore, in the context of online tracking, users, intermediaries, and different government agencies have conflicting incentives.

10. Moore's law has led to continuous advances in artificial intelligence and human-machine interfaces. This can be expected to continue. Thus, in my lifetime, there will be language chips that allow me to speak fluent Dutch, and you fluent Persian, with minimal effort. ("Asghari's law of machine translation")

These propositions are regarded as opposable and defendable, and have been approved as such by the promoter, Prof.dr. M. J.G. van Eeten.

Foreword

Writing a dissertation is journey of many months. There is much to learn, do, and obsess about. We are asked to research topics that are novel, practical, relevant, scientific, societal, and many other things, and to learn it all by doing. There are moments of disparity, feeling nothing important is being achieved; and moments of discomfort, knowing one is in uncharted waters. There is a battle for articulation, foremost with oneself. In the process, we contribute to the body of knowledge built by the giants before us, and develop emotionally. Luck also has its role…

I had the fortune to coauthor many chapters with fantastic scholars from different disciplines. I would like to thank them for the fun collaboration and what they taught me: Prof. Johannes Bauer, Prof. Milton Mueller, Prof. Nico van Eijk, as well as Axel Arnbak, and Michael Ciere.

I was blessed during these five years with many patient friends and loved ones. They kept my spirits high when I was in the dumps, and brainstormed with me during the highs of my work. I am grateful to all of them. These include my parents Ali and Tahereh, and in particular among friends and loved ones, Ardalan Haghighi Talab, Arman Noroozian, Carlos Ganan, Christa Hubers, Daniel Hogendoorn, Ken Arroyo, Meghan Hardy, Nargess Asghari, Rene Mahieu, Reza Amrollahi, Samad Khatibi, Saman Sattari, Shahab Zehtabchi, Shahriar Boroujerdian, and Shirin Tabatabie, were magnificent at one stage or another.

Lastly, I wish to thank whole-heartedly my promoter and advisor, Prof. Michel van Eeten, who I have now worked closely with for six years. Michel has coached me into doing great science, being effective, and being diplomatic. (The jury is still out on the last). His enthusiasm and clever ideas energized the dullest moments; and as a mentor and a friend, he has helped me conquer constant self-doubt.

Hadi Asghari, Delft, June 2015

Chapter 1: Introduction

1.1 Problem Definition

The Economics of Information Security

Cybersecurity is high on the agenda for organizations and governments. Month after month, we hear about new, large-scale, and sometimes embarrassing attacks. In 2014, large companies such as Home Depot, JPMorgan Chase, and Sony suffered breaches that compromise of millions of customer records and company secrets (Elgin, Riley, and Lawrence 2014; Glazer 2014; Zetter 2014). All sectors were affected, including companies offering security services to governments (Walsh 2014). The Identity Theft Resource Center (2014) reported a total of 783 breaches for the year in the United States alone. We lack comparable statistics from European countries, as reporting data breaches is not mandatory in all sectors in Europe. However, judging by malware trends, the situation is no better on this side of the Atlantic (e.g. see Microsoft 2015, 44).

Such high profile breaches occur despite a wealth of research in cybersecurity[1]. The American National Academy of Engineering has listed cybersecurity as a grand challenge since 2008 (Squatriglia 2008); the E.U. has similarly funded security research heavily since its Seventh Framework Programme in 2007 (European Commission 2013). A Google Scholar search for articles with the words Internet and Security after 2008 returns more than a million results. Although scholars debate whether cyber-attacks have worsened—relative to the growth of the Internet or

[1] The International Organization for Standardization defines cybersecurity as "the preservation of confidentiality, integrity and availability of information in the Cyberspace" and cyberspace as "the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form" (ISO/IEC 27032:2012). Other national and international organizations provide slightly varying definitions of these terms (Maurer and Morgus 2014). Van den Berg et al (2014) distinguish between information security and cybersecurity, with the former relating to the technical risks, and the latter to the business-oriented risks.

fluctuations in statistical trends (Edwards, Hofmeyr, and Forrest 2015)—the direct and indirect costs of cybercrime are still in the billions (R. Anderson et al. 2013).

Attackers exploit vulnerabilities in systems and mistakes by humans to breach their targets. A typical network hosts thousands of devices that run millions of lines of software and contain an unknown number of vulnerabilities. A significant amount of security literature has focused on identifying and fixing these vulnerabilities: approximately 60,000 critical vulnerabilities were reported between 2005 and 2014 (CVE 2015). But there seems to be no end in sight.

No one believes that we will eliminate all vulnerabilities, nor the human mistakes leading to security failures. That being said, some security systems fail more than others. Theories from economics and other social sciences have been helpful in explaining why.

Anderson (2001) argued that information security has as much to do with defender incentives as with technical vulnerabilities. For example, when those in charge of protecting a system do not bear the consequences of failure, they often underinvest in security (R. Anderson and Moore 2006). The incentives of attackers are equally important: the anticipated success and value of an attack needs to outweigh its costs (Savage 2011; Florêncio and Herley 2013b).

These and related insights have helped us better understand security failures and defenses. This interdisciplinary approach to cybersecurity, which combines computer science, economics, psychology, and law, is named *Information Security Economics.* Chapter 2 provides a survey of this field.

Internet Intermediaries as Focal Points

In recent years, the role of Internet intermediaries in cybersecurity has received special attention from researchers. *Intermediaries* are organizations that provide the Internet's basic infrastructure and platforms, and enable communications and transactions between third parties and services (Perset 2010). Examples include broadband providers, payment systems, search engines, and other services provided by firms such as Apple, Amazon, Facebook, Google, or Microsoft. In the absence of a central authority, these companies decide on technical standards and enforce procedures, making them de-facto rule makers (Van Eeten and Mueller 2012; Hall and Biersteker 2002). Their influence is felt in many Internet operations.

Intermediaries can play a positive role to improve cybersecurity, at least in theory. Their centrality means they see much of what goes on in the network, and they have direct access to users. They are often resourceful and technically apt, and their scale makes them easier to engage by policymakers. In practice, however, their incentives concerning cybersecurity are mixed. They often see cybersecurity as a necessity to maintain user trust. They also see it as costly. Many times, they voluntarily take steps to protect their customers from attacks. But there are also times that they avoid action, or do things that impose costs on other actors or on society at large (Van Eeten and Bauer 2008; R. Anderson et al. 2008; Schneier 2012; Fryer, Moore, and Chown 2013).

Public policy that wishes to improve cybersecurity needs a sharp understanding of the behavior and incentives of intermediaries.

Inferring Behavior and Incentives from Security Measurements

Information about the behavior of companies and organizations can be gathered via a variety of means. Surveys and interviews have been traditional methods used for this purpose. They however have a major drawback when it comes to security economics: they collect opinions that might or might not correspond to actual behavior. A better approach is to measure security issues directly and infer security behavior and incentives from these measurements. Machines on the Internet continuously record various aspects of network security and incidents. Using security measurements to improve security policies and investments has long been advocated (Geer, Hoo, and Jaquith 2003; Pfleeger and Cunningham 2010; Böhme 2010).

Despite the appreciation for security measurements, and the availability of more and more data, a number of difficulties have hindered the development of policies using measurements. First is that incident data and security measurements often are linked to technical identifiers, while policies are about real-world entities, and the mapping between identifiers and entities is imperfect. As an example, security metrics are often compiled at the level of Autonomous Systems (ASes). An AS is “a connected group of one or more IP prefixes run by one or more network operators which has a single and clearly defined routing policy” (Hawkinson and Bates 1996). An AS is a technical entity closely related to real-world Internet Service Providers (ISPs). Most research papers simply equate the two. However, the mapping between the two is not one to one: most large ISPs have an AS; some ISPs have multiple ASes, and sometimes one AS is shared by multiple ISPs; there are also ASes that are not really ISPs, e.g. enterprises and educational networks. Equating ASes and ISPs yields results that are much too inaccurate to answer policy questions.

The second difficulty is that different sets of skills are required to analyze measurements to infer behavior. Cybersecurity papers are often written by researchers from technical disciplines, such as computer science, who develop a measurement tool, run it, and process its data. Making behavioral inferences from measurements requires some familiarity with theories from the social sciences. Without them, papers often end up with major errors, such as including variables that cannot be causally explained to increase a high R-square, or being mute about various biases. Such errors would be sins for many quantitatively trained social scientists. One explanation is that the policy sections of many measurement papers are written as proof-of-concepts, and the core interest and expertise of the community remains in the measurement itself.

When the goal is to use security measurements to contribute to cybersecurity policy, then careful thinking is required about the messy relations between identifiers and entities, and about possible causes and effects.

These three themes—security economics, intermediaries, and measurements—are at the heart of this dissertation.

1.2 Research Questions

The goal of this dissertation is to find opportunities for improving cybersecurity via Internet intermediaries. This objective requires us to understand the security behavior and incentives of intermediaries, and assess how these will be affected by public policies. This leads to the following main research question:

> *What can security measurements tell us about internet intermediary behavior? What incentives explain these behaviors, and how do firm characteristics, market forces, and regulatory conditions shape these incentives? What does this imply for cybersecurity policy?*

The dissertation answers this question through six standalone chapters: four peer-reviewed empirical studies, each addressing a separate substantive policy question; a literature review contribution to an edited volume; and a peer-reviewed methodological reflection paper. The empirical studies were chosen based on two criteria. First, they contributed to a key cybersecurity debate involving intermediaries. Second, we had access to security measurements relevant to the study. The chosen approach has both benefits and limitations.

The benefit of engaging in substantive policy questions is that it enforces a level of rigor and accuracy in the analysis of measurements. Industry experts will quickly point out in conversations that patterns about technical identifiers and real-world entities differ. And policymakers will expect plausible causal explanations. We make a number of methodological innovations through the studies to answer the policy question as well as the main research question. These include steps in processing, triangulating, and aggregating the security measurements; solutions for the mapping of technical identifiers to real world organizations; supplementing metrics with firm and market data; and in interpreting the results. All studies involved comparison among several-dozen countries, with some longitudinal angle. The findings received considerable attention[2] in academia, industry discussions, and policy development, which arguably validates the innovative insights that can be gained by this approach.

A clear limitation of answering a question via stand-alone studies is the generalizability of the findings—both methodologically and substantively. In the conclusion chapter, I reflect on the findings of the individual studies, and explore the broader regularities in terms of the dissertation's main research question.

[2] These are listed in chapter 8.

Topics of the Studies

The first two studies focused on the threat posed by botnets. Botnets are collections of computers infected by malware under the control of an attacker. They become a platform for launching other cyber-attacks. Mitigating botnets has turned out to be a decade long challenge (see Microsoft 2007; Microsoft 2015).

The first study concerned the role of Internet Service Providers (ISPs) in mitigating botnets. ISPs were depicted as natural control points for infected machines (e.g. R. Anderson et al. 2008), which our study assessed empirically. It further asked whether ISPs differed in infection rates and mitigation efforts, and if so, what explains the difference? The final version of the study used two global and longitudinal datasets of botnet activity—with approximately 150 and 395 million unique IP addresses—to compare infection rates for ISPs across 60 countries.

The second study looked at the success of national anti-botnet initiatives (ABIs). These initiatives assist ISPs in botnet mitigation, by sharing data, tools, and support costs. We explored their effectiveness in the case of the large and old Conficker botnet. Despite successful efforts in dismantling Conficker's control infrastructure and making patches available, hundreds of thousands of machines remain infected (ESET 2014). We used six years of Conficker sinkhole data to model infection trends across 62 countries; and determined whether countries with ABIs had different growth, peak, or decay rates.

The third study examined the incentives of Certificate Authorities (CAs). CAs sell the digital certificates required to encrypt Internet communications. An extensive breach at a Dutch CA, DigiNotar, highlighted systematic vulnerabilities in the entire ecosystem (Fox-IT 2012). This study analyzed the CA market by connecting market shares with certificate prices. The market shares were estimated using two datasets of publicly visible TLS/SSL certificates—with approximately 1.5 and 3 million certificates. This revealed unforeseen perverse incentives; and helped evaluate regulatory and technical options proposed to mitigate the vulnerabilities.

The fourth study investigated ISP incentives to deploy Deep Packet Inspection (DPI) technologies for bandwidth management. DPI gives the capability to block, slow down, or prioritize Internet traffic based on content—a major shift from traditional Internet routing. This new capability created controversies, tying into debates on cybersecurity, network neutrality, censorship, and privacy (Bendrath and Mueller 2011). We investigated the extent to which DPI was used with this backdrop; what factors drove its adoption across 46 countries; and whether or not the commercial incentives for ISPs to manage bandwidth outweighed the external regulatory and consumer concerns about privacy. This was done by analyzing approximately 800,000 crowd-sourced tests measuring whether an ISP used DPI to restrict peer-to-peer sharing.

Contributions

An itemized list of the dissertation's contributions is presented here; they are discussed in detail in the concluding chapter.

First, it contributes in a substantive manner to the cybersecurity challenges it studies. The findings—on botnet mitigation, CA vulnerabilities, and DPI use—were in several cases incorporated in policy discussions and development.

Second, it contributes to the economics of cybersecurity literature through methodological innovations on analyzing and interpreting security measurements. These include guidelines for the processing of measurements, mapping tools, and reflections on making inferences.

Third, it contributes to the economics of cybersecurity literature by furthering discussions on the role of intermediaries in Internet governance[3]. The dissertation concludes by reflecting on how cybersecurity can be improved through Internet intermediaries.

1.3 Dissertation Outline

The remainder of this dissertation is organized in seven chapters. These are listed in Table 1.1, along with the relevant publications. Chapter 2 reviews the state of the art in the economics of cybersecurity and deepens the problem definition given in this chapter. It explains the theories

[3] Governance refers to all processes of governing, whether undertaken by a government, market, or network, whether over individuals, formal or informal organization, or territory, and whether through laws, norms, power, or language (Bevir 2012).

linking incentives and cybersecurity, reviews the field developments in recent years, and argues for the role of intermediaries and security measurements. The chapter is forthcoming in the Handbook on the Economics of the Internet.

Chapter 3 to 6 cover the four studies. All chapters have been published partially or fully in a journal or peer-reviewed conference. I was fortunate enough to do all studies in collaboration with great researchers who are also listed in Table 1.1. The bulk of the empirical analysis was done in all studies by me; all authors contributed to the analysis of incentives and policies. The legal analysis in the CA study was done fully by my colleagues at the Institute for Information Law at the University of Amsterdam. I am the lead author on at least one of the publications used for each chapter.

Chapter 7 reflects on a number of conditions security measurements need to have in order to be usable for policy research. I wrote this paper halfway through the PhD research to highlight some challenges of using secondary data. It was peer-reviewed by, and presented to an audience of measurement experts.

Finally, chapter 8 concludes the dissertation by drawing broader conclusions from the studies to answer the main research question.

Table 1.1. Dissertation overview

Ch.	Publications	Measurements
2	Asghari, Hadi, Michel J.G. van Eeten, and Johannes M. Bauer. 2016. "Economics of Cybersecurity." In *Handbook on the Economics of the Internet*, edited by Johannes M. Bauer and Michael Latzer. Cheltenham and Northampton: Edward Elgar.	-
3	Asghari, Hadi, Michel J.G. van Eeten, and Johannes M. Bauer. 2015. "Economics of Fighting Botnets: Lessons from a Decade Mitigation." *IEEE Security and Privacy* 13 (5): 16–23. doi:10.1109/MSP.2015.110. Van Eeten, Michel J.G., Hadi Asghari, Johannes M. Bauer, and Shirin Tabatabaie. 2011. "Internet Service Providers and Botnet Mitigation: A Fact-Finding Study on the Dutch Market." The Hague: Netherlands Ministry of Economic Affairs. http://goo.gl/ODJEBg.	Spam-trap, Conficker sinkhole, GOZeus sinkhole

Ch.	Publications	Measurements
4	Asghari, Hadi, Michael Ciere, and Michel J.G. van Eeten. 2015. "Post-Mortem of a Zombie: Conficker Cleanup After Six Years." In *Proceedings of the 24th USENIX Security Symposium (Security '15)*. https://goo.gl/LnguCn.	Conficker sinkhole
5	Arnbak, Axel, Hadi Asghari, Michel J.G. van Eeten, and Nico van Eijk. 2014. "Security Collapse in the HTTPS Market." *Communications of the ACM* 57 (10): 47–55. doi:10.1145/2660574. Asghari, Hadi, Michel J.G. van Eeten, Axel Arnbak, and Nico van Eijk. 2013. "Security Economics in the HTTPS Value Chain." Paper peer reviewed and presented at the 12th Workshop on the Economics of Information Security (WEIS 2013), June 11-13, Washington, DC. doi:10.2139/ssrn.2277806.	SSL Observatory, HTTPS Ecosystem Scans
6	*Major revision of:* Asghari, Hadi, Michel J.G. van Eeten, Johannes M. Bauer, and Milton L. Mueller. 2013. "Deep Packet Inspection: Effects of Regulation on Its Deployment by Internet Providers." Paper presented at the 41st Research Conference on Communication, Information, and Internet Policy (TPRC 2013), September 27-29, Arlington, VA. *Related Publication.* Mueller, Milton L., and Hadi Asghari. 2012. "Deep Packet Inspection and Bandwidth Management: Battles over BitTorrent in Canada and the United States." *Telecommunications Policy* 36: 462–75. doi:10.1016/j.telpol.2012.04.003.	M-Lab Glasnost
7	Asghari, Hadi, Michel J.G. van Eeten, and Milton L. Mueller. 2013. "Internet Measurements and Public Policy: Mind the Gap." In *Proceedings of the 6th USENIX Workshop on Cyber Security Experimentation and Test (CSET '13)*. doi:10.2139/ssrn.2294456.	-

Note 1: the spam trap data is courtesy of Dave Rand; the other measurement sets are available to researchers at the following sources: Conficker sinkhole (http://confickerworkinggroup.org), GameOver Zeus sinkhole (https://goz.shadowserver.org), EFF SSL Observatory (https://eff.org/observatory), U. Michigan HTTPS Ecosystem Scans (https://scans.io/study/umich-https), and M-Lab Glasnost (http://measurementlab.net/tools/glasnost).

Note 2: The following datasets supplemented the measurements in each study:

- Own-constructed AS-to-ISP mapping and CA certificate price dataset
- Geo and AS lookup databases from MaxMind (https://maxmind.com) and RouteViews (http://routeviews.org)

- ISP market data from TeleGeography (https://telegeography.com/research-services)
- Country level indicators from the International Telecommunications Union (http://itu.int/en/ITU-D/Statistics), OpenNet Initiative (https://opennet.net/research/data), Privacy International (https://privacyinternational.org/reports), Software Alliance (http://bsa.org/anti-piracy), StatCounter (http://gs.statcounter.org), and the World Bank (http://data.worldbank.org).

Chapter 2: The Economics of Cybersecurity[1]

This chapter presents the state of the art in the economics of cybersecurity. It elaborates the underlying concepts, as borrowed from economics. It answers the dissertation's central question theoretically, by reviewing what is known about the behavior, incentives, and role of intermediaries in cybersecurity.

2.1 Introduction

The Internet has enabled tremendous economic and social innovation yet the underlying systems, networks and services sometimes fail miserably in protecting the security of communications and data. Security incidents occur in many forms, including but not limited to the leaking and theft of private information, unauthorized access to information, malicious alteration of data, or software and service unavailability. Enumerating all the technical ways in which security may be breached would generate a lengthy list as the network, devices, users, and services can all be attacked. A typical network runs hundreds of protocols and hosts devices operating thousands of applications consisting of millions of lines of code. Looking for solutions opens up an equally unwieldy range of ideas, technologies, and complications. Not surprisingly, books on information security are typically voluminous. For example, Anderson's (2008) *Security Engineering* is over 1000 pages long. Despite its length, the book can address most topics only briefly. Even research focusing on specific problems and solutions can be dauntingly complex. For example, the design and use of passwords has generated hundreds of papers but the jury on best practices is still out (Bonneau et al. 2012). Achieving cybersecurity under these conditions may appear like a hopeless endeavor and failure unavoidable.

[1] To appear in: Asghari, Hadi, Michel J.G. van Eeten, and Johannes M. Bauer. 2016. "Economics of Cybersecurity". In *Handbook on the Economics of the Internet,* edited by Johannes M. Bauer & Michael Latzer. Cheltenham and Northampton: Edward Elgar. Reprinted with permission.

Given the complexity of the problem, it seems indeed improbable that security can be attained by eliminating all vulnerabilities. Moreover, preventative security measures are costly. Some level of uncertainty will therefore have to be accepted and choices need to be made trading off competing objectives and limited resources. Recent research has developed approaches to better explain why certain security failures occur and others do not. These contributions clarified that security is not merely a technical problem that can be fixed with engineering solutions but that is also has important economic and behavioral dimensions that need to be addressed (R. Anderson and Moore 2006). Examining the incentives of players in the information and communication technology (ICT) ecosystem has been particularly fruitful in explaining the landscape of vulnerabilities and attacks that can be observed. The core of this work is rooted in information security economics.

A key insight that catalyzed the development of this field is that many systems do not fail for technical reasons but because of the specific incentives shaping the behavior of individuals and organizations. For instance, if the individuals in charge of protecting a system do not have to bear any costs or other consequences in case of failure, they may exert insufficient care (R. Anderson and Moore 2006). Attackers similarly respond to the set of pertinent incentives, for example by selecting targets and attack strategies based on expected financial or political benefits and risks. Technical tools to carry out attacks are often chosen opportunistically as attackers will use whatever means happen to work in a given scenario. These insights and the abundance of technical and non-technical vulnerabilities and attack vectors imply that it is more promising to approach cybersecurity as a defender-attacker dynamic with an emphasis on the incentives of players rather than with a focus on the vulnerabilities. Another consequence is that for the foreseeable future information systems will need to be defended against attacks with a combination of technology and human vigilance.

Given the abundance of interdependencies in the ICT ecosystem, cybersecurity at the individual and system levels is influenced by how the incentives of different actors align. Sometimes individual and group incentives are compatible with both the private and social costs and benefits so that decentralized decisions will be workable and effective to achieve desirable levels of security. However, more often such an alignment cannot be taken for granted and several questions arise. Are markets, networked governance, and individual organizational decisions—the predominant coordination mechanism in the Internet—sufficient to safeguard cybersecurity (Van Eeten and Mueller 2012)? Or does such decentralized coordination fail because market and non-market players are not prepared or capable to effectively deal with the risks? If market failure is pervasive, the incentives of decentralized players will be systematically biased and may result in underinvestment or overinvestment in security (Lewis 2005; Shim 2006). A classical response to market failure is government intervention but the incentives of government actors are not necessarily aligned with the common good. Parts of government, including secret services and the military, may have an interest to exploit vulnerabilities for surveillance purposes. Consequently, conflicts within government may prevent effective public sector responses to information security risks. Moreover, the global scale and connectivity of the Internet has created interdependencies that may require coordinated action beyond the national or global level to design effective responses, greatly compounding the challenges. Security economics has in the past decade successfully examined many of these questions and helped greatly in the design of rational responses.

Most of the work in the field has focused on information security as a means to fight criminal activities, rather than on the protection of national security and cyberwar. The two topics, while related, raise different theoretical and practical issues. Some scholars have argued that the societal impact of cybercrime is more important than the hype-prone concept of cyberwar. Cybercrime has been more amenable to empirical research; protecting national security in comparison is more about scenarios of potential impacts. It is important to understand the perspective used by each approach to conceptualize risk, costs and benefits, and the role of government (see, for example, Singer and Friedman 2013). Cybercrime is often discussed in a framework of risk management, using cost-benefit and trial-and-error approaches. This approach typically results in tolerating some level of risk and vulnerability. National security deals with massive economic and social disruptions, often focusing on worst-case scenarios. In such scenarios, prevention and resilience are often the main emphases (Van Eeten and Bauer 2009; Van Eeten and Bauer 2013).

In this chapter, we set out to survey the state of the art of the existing research with a focus on the criminal threats to cybersecurity.

The next section briefly outlines key topics addressed in economic analyses of information security. Sections 2.3 through 2.5 discuss software and platform security, end-user and organizational security, and Internet intermediary security. Attacker behavior is addressed in section 2.6 , followed by an exploration of policy options in section 2.7 and concluding remarks in section 2.8 .

2.2 Cybersecurity as an Economic Problem

Cybersecurity may refer to technical, legal, and organizational measures directed at maintaining or enhancing the integrity and security of information assets. It can be assessed at the level of individuals and organizational, or at aggregated levels such as nations or cyberspace as a whole. Many of the Internet's technical and behavioral standards, conventions, and norms emerge from decentralized repeated decisions of actors participating in it—ranging from component and hardware manufacturers to network operators, software vendors, application and service developers, content providers, and various users. These actors are heterogeneous and have different skillsets and motives. The architectural design adopted by Internet engineers created the socio-technical framework that constrains and enables these actors. While information security was initially not a pressing concern, the early choices that solidified the unique open design of the Internet inadvertently created later challenges of safeguarding cybersecurity (Lessig 1999; Hofmann 2010).

The field of economics of information security studies factors that actors perceive as relevant for security decisions ('incentives'), their influence on economic actions by individuals and organizations, and how these actions lead to emergent properties of the system. The early concepts and theories applied in the field originated from neo-classical microeconomics, and in particular the field of information economics. Economic sciences, however, constitute a wide discipline (Groenewegen 2007; Colander 2005). Concepts and theories from other fields, such as behavioral economics and new institutional economics, have also over the years made their way into the economics of information security. In this section, we look at four basic concepts.

Externalities. Cybersecurity has both private and public good characteristics: while investment in security protection entails private costs and benefits for the decision-maker, it may also benefit or harm other Internet actors. These interdependencies are called externalities—formally defined as the direct effect of the activity of one actor on the welfare of another that is not compensated by a market transaction (Rosen 2004). Much of the economic literature on security economics is concerned with externalities that can be negative or positive. In both cases, the price of the direct market transaction will not reflect the full social costs or benefits of the product or service, because the third party effects are not taken into account by the transaction partners. Consequently, systematic deviations from an optimal allocation of resources occur even in an otherwise functioning market economy (Musgrave and Musgrave 1973). Individual security measures may have positive and negative externalities, depending on whether attacks are targeted or non-targeted and whether the associated risk is interdependent or not (Kunreuther and Heal 2003). There are several ways to correct for such externalities and 'internalize' them into decision-making. A traditional response is collective action by government or the participants in an exchange. Many information markets are multi-sided ('platform') markets; the platform intermediary may have incentives to internalize externalities caused by others to improve its business case and competitiveness. In fact, these platforms can be seen as institutional arrangements to reduce transaction costs and address externalities (Rysman 2009).

Information Asymmetry. Another key focus in the information security literature relates to the situation in which information is incomplete and unevenly distributed among players; such as when buyers in a market do not have sufficient information to reliably separate between high quality and low quality products. For example, a subscriber looking to purchase Internet access may not be able to distinguish ISPs with strong security practices from those with lax ones. This makes buyers unwilling to pay a premium for the better product and consequently discourages suppliers from offering them—a situation dubbed a 'market for lemons' (Akerlof 1970). Information asymmetry afflicts many Internet services when it comes to security and privacy, where it is impossible to determine how secure a service is.

Property Rights. Although rarely explicitly recognized in the literature, a fundamental economic problem at the heart of many information security issues may be the absence of clearly defined property rights in personal and other information (Branscomb 1994). It is this absence that gives players in the Internet more or less free reign to appropriate information from users and store large amounts of data.

Alignment of Incentives. Cybersecurity can be improved by introducing measures that align incentives of individual actors so that deviations between private and social costs and benefits are reduced. If successful, such strategies can reduce or even eliminate security-related market failures and deficiencies. Table 2.1 presents selected high-level options for aligning incentives among Internet actors. One can strengthen the incentives for security investment and other protective measures among defenders. One can also disincentivize attackers by increasing the costs or reducing the benefits of cybercrime and other malicious actions. Although the differentiation between defenders and attackers is sometimes muddied—government agencies with an interest in vulnerabilities to spy on others, white hat hackers who attack with the goal to improve defenses—the approach is useful in exploring principal options.

In the next sections of this chapter, we survey the security economics literature organized around these actors. We shall provide examine the incentives of each actor, their interactions with the ecosystem, and security issues that they create or resolve. Among the attackers, our focus will be on cyber criminals, economically motivated and by far the largest group.

Table 2.1. Improving cybersecurity by aligning incentives of actors

Improving Cybersecurity

Incentivizing Defenders	Disincentivizing Attackers
Who:	*Who:*
- Software vendors	- Criminals
- End users and organizations	- Hacktivists
- Internet intermediaries	- Nation states
How:	*How:*
- Reducing information asymmetries	- Improved law enforcement
- Addressing negative externalities	- Reducing benefits of crime
- Education and capacity building	- Disrupting criminal resources

Approaches to Studying the Economics of Cybersecurity

The security economics literature can be categorized into analytical, empirical, and experimental research.

Analytical studies employ methods such as game theory to deduct theoretically how actors behave in security dilemmas. Key variables, such as prices, regulation, and the type of competitive interaction are parameterized. Determining cooperative and non-cooperative equilibria of the game allows researchers to explore the conditions under which cybersecurity improves or deteriorates. As it may be difficult to derive solutions to games analytically, researchers also use computational and simulation methods to approximate outcomes. These methods offer interesting results but their practical use may be limited by the required simplifying assumptions. Results are often highly stylized and application to more complicated real world situations may need careful and cautious interpretation.

Empirical studies start by collecting and observing actual cybersecurity behavior and performance. While many of the efforts are descriptive, additional insights may be gained by combining datasets of Internet measurements or surveys with data analysis to unveil how a market functions and how its actors behave. Empirical studies are a promising avenue but they also have their unique challenges, which include the dynamic nature of the phenomenon, insufficient or unreliable data, and problems of endogeneity that complicate establishing causality especially in cross-sectional comparative studies.

Experimental studies use lab or online experiments to test various hypotheses—with fewer assumptions and proxies than the other two methods. This raises challenges as to how generalizable the findings may be.

In subsequent sections of this chapter, we look at all three categories of works. We focus mainly on the recent literature as it usually also relates to earlier work and point to classics and influential work in the field. We have chosen this approach to keep the material more manageable but also because much of the earlier research has been updated and extended in recent years. Moore and Anderson (2012) and volume 3, issue 1 of IEEE Security & Privacy, published in 2005 are earlier surveys of the field. For the purposes of this chapter, relevant literature has been drawn from papers presented at a number of leading security conferences, including the annual Workshop on the Economics of Information Security (WEIS), a detailed examination of journals where scholars of the field typically publish and through keyword search in other journals.[2]

2.3 Software and Platform Security

The Internet and its services are run by software. Many security issues arise because of poorly written or misconfigured software. The Common Vulnerabilities and Exposures database, a 'dictionary of common names for publicly known information security vulnerabilities', lists 60 000 software vulnerabilities between 2005 and 2014 (CVE 2015). They can be found in all operating systems and pieces of software. Anderson (R. Anderson 2001) was one of the first to explore the fundamental economic reasons behind this phenomenon.

Software products share a number of interesting characteristics with other 'information goods' (Shapiro and Varian 1998). High initial devel-

[2] In addition to WEIS, proceedings of USENIX Security, IEEE S&P, ACM CCS, SOUPS were perused. Key journals that were reviewed in detail included IEEE Security & Privacy, Communications of the ACM, Telecommunications Policy, and Information Systems Research. Key search terms for other journals included 'economics, security' and 'internet, security'.

opment and production costs are accompanied by close to zero incremental costs for additional copies. Information goods often exhibit direct and indirect 'network effects'. Direct network effects exist if the utility of a software product increases with the number of users (e.g. because documents can be shared with a larger group). Indirect effects exist if, as the user base grows, more complementary software and products become available, further increasing the utility of the software. In the absence of cheap and efficient converter technology, network effects can lead to switching costs and consequently 'lock-in' effects (Gottinger 2003): The costs of equipping an organization with new hardware and software, the costs of switching from one solution or format to another including the associated costs of document conversion, and the costs of learning new skills all create rigidities that work in favor of sticking with the existing solution. This provides advantages for the first mover and disadvantages for competitors that enter a market late. Consequently, software markets have a 'winner-takes-all' dynamic that incentivizes vendors to move their products to market fast and to grow as quickly as possible.

In their battle for dominance, software vendors might initially give away their products for free or at a low price but change their pricing to generate a profit once they have a large user base and lock-in. Software vendors will attempt to lure developers to their platforms by making application programming interfaces (APIs) available for free or at a low cost as developers bring additional users. This might also imply that developers are given latitude and are permitted to work under lax rules for security technologies in the platform (R. Anderson and Moore 2006). Vendors will lure customers with bells and whistles that are visible features or provide convenience. Security is rather intangible and does not easily fit into these considerations, it might even reduce functionality. That is why in the short term the market does not value security. After a firm gains dominance, the incentive structure changes: The costs of releasing software patches and mending brand damage incentivize firms to change course. An example is Microsoft whose reputation was tarnished after a series of spectacular worm attacks in the early 2000s. In response, the company started an internal code-review campaign resulting in the release of Windows XP Service Pack 2 with many security enhancements in 2004 (Van Eeten and Bauer 2008). Nowadays, Windows vulnerabilities make fewer headlines. Vulnerabilities have moved 'up the stack' to other applications, including open-source software. But all in all software vendors cause severe negative externalities as they do not bear much of the costs of insecure software.

Security software has an interesting extra hurdle. Since security is hard to measure, the average user basically has to take the word of a vendor claiming the product provides better security protection than another. Thus it becomes a classic lemons market (Schneier 2007). A running joke states that antivirus software competes on every feature except security. Judging by the large sums spent on security products (R. Anderson et al. 2013) consumers demand security. If they are lacking clear and reliable information they will likely underinvest in some key areas and overinvest in hyped ones.

A number of ideas have been presented for aligning incentives of the players in the software market. To be fair the responsibility rests not solely on software vendors as they are not instigating the attacks. Even in a perfect market some users might choose software with a lower degree of security and remedy remaining problems using other countermeasures. Anderson et al. (2008) name an obligation to provide free and timely software patches for security products, mandating 'secure by default', and responsible vulnerability disclosure as policy options. Previously software certification has been suggested but this has not worked as anticipated. We look at these options later in the chapter.

Zittrain (2008) raised concerns that the market might evolve toward users preferring locked-down devices to reduce the threats from malware and other side-effects of insecure software. Given the rise of mobile devices there is some evidence to that effect, as the major application stores are controlled by the respective firms or consortia (e.g. Apple's App Store, Google's Play Store, and Microsoft's Windows Store). Application stores for web-browsers are another example. Application stores have their own share of security problems and exhibit a wide variation in their security mechanisms. J. Anderson, Bonneau and Stajano (2010) compared the incentives of ten different application stores and concluded that soft liability and signaling have the best chance for improving security without stifling innovation. The shift towards software as a platform and the rise of application stores means that some software vendors become Internet intermediaries who have different incentives (e.g., Fershtman and Gandal 2012).

2.4 End-User and Organizational Security

Users may be individual end-users and organizations ranging from small to very large size. Our focus is on the incentives and decisions of organizations outside the IT security industry that need to protect information assets related to their core business. We start by looking at larger organizations with dedicated IT budgets and then turn our attention to smaller organizations and individuals with limited skills to assess and manage security risks.

Information Security Investment in Large Organizations

Rational large organizations would make security investment decisions based on several relevant factors, including the type of risk they are facing, the monetary and non-monetary consequences of failure, the resilience of their operations, etc. In practice, the available budget is often a key determinant of their security investments (Cavusoglu, Mishra, and Raghunathan 2004). The total cost of security includes investment in technology, the hiring of experts, as well as the indirect productivity costs that might be caused by security controls. Although security spending figures tell little about the rationality of expenses they are a useful proxy for the total resources available. Framing security as an investment problem eases communication with upper management and helps set limits as it might make sense not to defend against certain threats.

Gordon and Loeb (2002) first explored optimal security investment conceptually. They proposed a model in which information assets are categorized based on their value, potential loss in case of a breach, and their vulnerability. The authors showed that under varying assumptions firms will be better off concentrating efforts on information assets with midrange vulnerabilities as extremely valuable information may be 'inordinately expensive' to protect. To maximize expected benefits a firm should spend only a small fraction of the expected loss on securing an asset (except in cases when law requires an asset to be protected regardless of value).

A number of scholars have extended this simple and elegant model, for instance by looking at the timing of investment, by proposing different caps for security investment, and by relaxing model assumptions. Ioannidis et al. (2013a) show in a utility-theoretic model that security investment turns out to be cyclical when costly projects are deferred due to uncertainty related to the costs of future vulnerabilities. Böhme and Moore (2009) model the interaction between defenders that face investment decisions under uncertainty and attackers who repeatedly target the weakest link. They empirically validate their model and conclude that underinvestment can be reasonable under certain scenarios: When reactive investment is possible, when attacks are not catastrophic, and when uncertainty exists about attacker capabilities. Although difficult, quantifying cybersecurity risks and costs is an integral part of the investment models. Brecht and Nowey (2013) focus on establishing the costs of information security. They offer a comprehensive comparison of three alternatives to using surveys for determining such costs. Demetz and Bachlechner (2013) compared approaches using a configuration management tool as an example, and found that there is considerable potential for new approaches to complement existing ones. These selected findings illustrate the difficulties of operationalizing and implementing cost-benefit approaches to assessing security investment.

The level of investment aside, what security practices should an organization put into effect? A high-level distinction is between practices that have an observable impact on security, and those that are adopted for compliance reasons, due diligence, or keeping up with what are considered 'best-practices'. The security benefits of alternative approaches also depend on the goals of an organization, which might include protecting the organization's intellectual property, finances, and customers from attacks. Sometimes security solutions might be focused on other objectives than security, for instance on achieving customer lock-in, as is the case with security measures in printers designed to ensure that third party ink cannot be used. In the case of best practices or standards, security measures are not adopted per se for their effectiveness, but rather for the sake of compliance. Standards such as the ISO 27000 series, the common criteria, or sector specific security regulation may fall in this category if implemented mainly to disclaim liability in case of failure. From the perspective of policymakers such measures can still be useful for the ecosystem as a whole if an evaluation of their aggregate results indicates that they have desired effects on security.

The security incentives of large organizations are, in short, mixed. Tolerating some level of insecurity is economically rational, and as long as the organization accepts the risks and compensates the direct and indirect costs, it limits the externalities of its security decisions. An organization can also decide to transfer security risks to a third party via cyber-insurance. But this arrangement has not been widely adopted thus far. Other policies are required if incident costs are not borne by the organization and externalities are created. One means is data breach disclosure laws (sometimes referred to as security breach notification laws) intended to mitigate harms to third parties caused by an organization's underinvestment in security. Organizations are required to notify all affected customers in cases of breaches leading to compromise of personal information. If they fail to do so they become liable for damages and face fines.

Security in the Healthcare Sector

Organizational security has also been studied in the context of particular sectors. The healthcare sector is a good example illustrating many key aspects of security decisions. It deals with confidential and sensitive patient data and has been subject to sector-specific regulation such as the U.S. Health Information Technology for Economic and Clinical Health (HITECH) Act and the Health Insurance Portability and Accountability Act (HIPAA). While confidentiality has considerable importance for earning the trust of patients and professionals, it is not the core business of health organizations. Consequently, attitudes towards such regulations might mainly be driven by a desire to be compliant. Given the interest in how an attitude of compliance affects security decisions, the health care sector has been studied in detail by researchers.

Gaynor et al. (2012) studied around 200 reported data breaches in hospitals from 2006 to 2011 and found that increased competition was associated with a decline in data protection. They suggest that hospitals in competitive markets may be inclined to shift resources to visible activities rather than data protection. Kwon and Johnson (2011) analyzed two thousand healthcare organizations and found that proactive security investments, associated with longer intervals between subsequent breaches, were most effective when voluntarily done. Miller and Tucker (2011) looked at encryption as a tool for increasing data security, in particular in states that provide safe harbors when it is used. They found that data breaches perversely increased after healthcare organizations adopted encryption software, possibly due to a false sense of security and/or a moral hazard problem. The effectiveness of sector regulation might be tied to the specifics of its formulation, as Kwon and Johnson (2013) suggest in a more optimistic study of the effects of the financial incentives created by the HITECH Act. They conclude that mitigating data breaches depends more on security resources and capabilities than regulatory compliance and reiterate that policy should provide guidelines to invest in a combination of security resources, capabilities, and cultural values, rather than impose single-solution requirements.

Individuals and Small Organizations

End-users that lack dedicated IT staff often rely on a variety of heuristics to make security decisions. These decisions are prone to mistakes that fraudsters can exploit (Stajano and Wilson 2011). The sheer number of such users means that even a small vulnerable fraction can cause major security risks for others and in the aggregate. An example is the market for fake anti-virus software: hundreds of thousands of users have been conned into paying for malware that claims to be an anti-virus product (Stone-Gross et al. 2013).

Psychology and behavioral economics provide explanations for such behaviors. Understanding how end-users interpret error messages and make security decisions can be used to design user interfaces that nudge users towards better security choices (Sunshine et al. 2009; Camp 2013). Bravo-Lillo et al. (2011) provide an enlightening example: novice users perceive ‘saving’ a file as being more dangerous than ‘opening’ it, as it implies persistent changes to the system. Similarly, Wash (2010) discusses ‘folk models’ formed by users about security threats and how they influence online behavior.[3] Given these difficulties, end-users might be willing to pay for extra security services. Just as an example, Wood and Rowe (2011) estimated that customers of U.S. Internet service providers are willing to pay $4 to $7 a month premium for mitigating malware harms. However, this willingness often does not translate into actual purchasing behavior due to information asymmetries and the market for lemons problem.

[3] Due to the scope of this chapter, we will not delve further into these topics. The interested reader is referred to works presented at the annual Symposium on Usable Privacy and Security (SOUPS).

Users are not always wrong to ignore security advice (Herley 2009). Typical advice concerning passwords is outdated, almost all certificate error warnings appear to be false positives, and if users spent even a minute a day reading URLs to avoid phishing, the costs would greatly outweigh phishing losses. Florêncio and Herley (2010) investigated password policies concluding that websites with the most restrictive policies are insulated from the consequences of poor usability: for example, universities have stricter password rules than Google and Facebook, as they won't lose revenue if users have a hard time logging in. The latter defend against more attacks using other effective authentication controls that maintain convenience (such as the location of access). This example shows an interesting trade-off between different aspects of implementing security protections.

Due to carelessness and limits of human intuition, end users can create considerable externalities for the Internet economy. However, they also fuel the Internet economy by shopping online and clicking on ads. Improving end-user security at the expense of convenience might result in a negative net-gain, an economic trade-off that possibly can be done away by larger organizations. For example, when online merchants were pushed by Mastercard and VISA to adopt the 3D security anti-fraud measure or accept liability for the fraud losses, some found that the additional checks resulted in higher dropout rates during checkout. These exceeded the cost of accepting liability for the fraud, which led some merchants to opt out of the security program.

2.5 Internet Intermediaries

One of the most promising areas of security economics research has concentrated on Internet intermediaries. These entities provide the Internet's basic infrastructure and platforms, and enable communications and transactions between third parties and services. Players include Internet Service Providers (ISPs), hosting providers, payment systems, e-commerce platforms, search engines and participative platforms as show in Figure 2.1 (Perset 2010). The role of intermediaries has increased over the years gradually modifying the original vision of an 'end-to-end' design of the Internet. Most intermediaries are private businesses and IT forms the core of their business. We will first make some general observations applying to all intermediaries, and then look at different types separately.

Intermediary markets are highly concentrated because of *network effects* and *economics of scale*. Network effects, as previously explained, reflect the increasing value of a service as more users adopt it. Economies of scale are cost advantages that firms gain due to their size. In many markets—for instance search engines, participative platforms or certificate authorities—a handful of companies control large market shares, sometimes up to eighty or ninety percent of the revenues or user base (Noam 2009). Some of the largest Internet intermediaries are among the world's top firms and well-known brands–e.g. Google, Facebook, eBay, Amazon, Apple and Microsoft.

Intermediaries raise interesting governance issues. They are in some sense gatekeepers of the Internet economy with direct access to end-users. They become de-facto standardization bodies and their mundane technical choices frequently have more profound effects on outcomes than formal Internet governance structures (Van Eeten and Mueller 2012). Their scale makes them focal points for regulation, whereas a network of thousands of organizations and millions of end users can hardly be regulated by traditional governance arrangements. However, like in the case of other players, the security incentives of Internet intermediaries are mixed. In some cases, security is a cost to avoid, in particular if it conflicts with business interests. In many cases however, intermediaries take security seriously and are among the largest defenders of users against attacks, as they have incentives in maintaining trust in the Internet economy. Often, their role as multi-sided platforms which are enabling other market players will generate strong incentives to internalize some of the externalities in the system. Moreover, many intermediaries have the resources, knowledge, and capabilities to provide security.

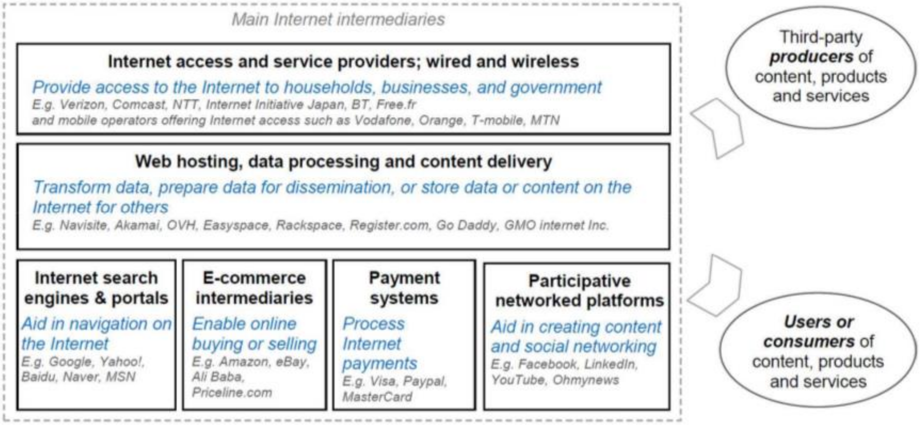

Main Internet intermediaries
Internet access and service providers; wired and wireless
Provide access to the Internet to households, businesses, and government
E.g. Verizon, Comcast, NTT, Internet Initiative Japan, BT, Free.fr
and mobile operators offering Internet access such as Vodafone, Orange, T-mobile, MTN
Web hosting, data processing and content delivery
Transform data, prepare data for dissemination, or store data or content on the Internet for others
E.g. Navisite, Akamai, OVH, Easyspace, Rackspace, Register.com, Go Daddy, GMO internet Inc.
Internet search engines & portals
Aid in navigation on the Internet
E.g. Google, Yahoo!, Baidu, Naver, MSN
E-commerce intermediaries
Enable online buying or selling
E.g. Amazon, eBay, Ali Baba, Priceline.com
Payment systems
Process Internet payments
E.g. Visa, Paypal, MasterCard
Participative networked platforms
Aid in creating content and social networking
E.g. Facebook, LinkedIn, YouTube, Ohmynews
Third-party producers of content, products and services
Users or consumers of content, products and services

Figure 2.1. Internet intermediary roles (Perset 2010, fig. 1)

Internet Service Providers

Internet service providers (ISPs) are companies that connect subscribers to the global Internet. ISPs come in different sizes—from small regional ISPs to multinational tier-1 networks. There are several thousand ISPs worldwide but the 200 largest ones serve about 80 percent of broadband and mobile Internet markets (Van Eeten et al. 2010). Since ISPs have access to their subscribers' Internet traffic they are affected by and involved in policy debates on privacy protection, network neutrality, copyright enforcement, infrastructure resilience, the blocking of malware, and the disruption of botnets.[4] In many countries, ISPs have historically been regulated in a less intrusive fashion than traditional telecommunications companies. In the U.S. they were historically classified as 'information service providers' and in other countries as value-added service providers. As part of these legal arrangements, they were shielded from liability for traffic carried on their networks as long as they followed certain required business practices (e.g. notice and take-down procedures).[5] We shall focus this section on the role and incentives of ISPs with

[4] These debates are all important for the Internet economy; this chapter retains a focus on cybersecurity.

[5] In the U.S. these safeguards were contained in the safe harbor provision of the Digital Millennium Copyright Act (DMCA) of 1998. While American ISPs were reclassified as common carriers early in 2015 (see Federal Communications Commission, In the Matter of Protecting and Promoting the Open Internet, GN Docket No. 14-28, adopted February 26, 2015), they are subject to similar protections under common

regard to malware and botnets as some of the most pernicious cybersecurity threats.

Bots are computers infected with malware that puts them under remote control by attackers. The attackers may directly harm the owners of these machines through fraud or extortion. They may also combine infected computers into botnets of varying size or rent them out to other criminals. In either case, they become platforms to launch attacks on other parts of the Internet and therefore are a serious problem for the whole Internet ecosystem. Numerous botnets remain active despite more than a decade of countervailing measures. Depending on whether one differentiates according to the malware families used or by the number of different attackers using them, their number ranges between tens and thousands. The largest botnets may at peak consist of millions of bots (Symantec 2015).

The security community has had some success in seizing control over botnets through both technical infiltration and apprehension of the command and control infrastructure (Fryer, Moore, and Chown 2013). However, a key problem that remains is cleaning up the infected machines. Clayton (2011) contemplates alternative approaches to clean-up and concludes it might make sense for governments to subsidize ISPs or other third parties to clean up malware on end-user machines. In the same vein, there have been calls to treat botnets by employing a public health approach. In this framework, a 'cybersecurity health agency' would provide education, monitoring (e.g. infections and intrusion trends), epidemiology (e.g. malware analysis), immunization (e.g. patch coordination), and incident response (Sullivan 2012; Kelley and Camp 2012).

Van Eeten et al. (2010) evaluated the role and incentives of ISPs in botnet mitigation by comparing spam-bots in 200 ISPs between 2005 and 2009. They found that large retail ISPs are indeed effective control points but that the number of infected machines per subscriber differs significantly among ISPs. This difference was relatively stable over time, suggesting

carrier law. In the European Union, such protections are contained in the 'mere conduit' provision of the Electronic Commerce Directive.

that systematic differences exist in ISP policies and management practices as well as among users. The authors further found that larger ISPs have lower average infection rates, possibly due to automation of detection and clean-up that allow reducing the unit cost of providing security. Moreover, the data reveals that ISPs located in countries with an attentive regulator have cleaner networks. Other researchers have suggested that coordinated action by the largest networks can be very effective in stopping malware (Hofmeyr et al. 2013), and that a correlation exists between well managed networks and end user security (J. Zhang et al. 2014). Different approaches to incentivize ISPs and other networks to improve security practices have been proposed. Tang et al. (2013) perform a shaming and faming experiment with networks that have high outgoing spam, a sign of botnet activity. They report that performance improved in a treatment group that was subject to information disclosure. In recent years, public-private partnerships between ISPs and a national anti-botnet center have been the most called upon model for clean-ups (OECD 2012). By splitting costs, these models recognize the role of ISPs and the public sector, and that ISPs are not solely responsible for clean-ups. The verdict on the effectiveness of these models is still out.

Hosting Providers

Hosting providers are organizations that operate servers used by customers to make content and services available to the Internet. Many hosting providers are also registrars: entities that sell and register domain names. As with virtually all services on the Internet, these businesses are abused by criminals. Phishing sites, command-and-control servers for botnets, and the distribution of child pornography, malware and spam all require such services. Like ISPs, hosting providers can thus play a key role in fighting cybercrime. Much of the criminal activity runs on compromised servers of legitimate customers but some run on servers rented by the criminals themselves. In either case, the hosting provider typically becomes aware of the problem only after being notified of the abuse. Responses to abuse reports vary widely, ranging from vigilant to slow to negligent (Canali, Balzarotti, and Francillon 2013; Stone-Gross, Kruegel, et al. 2009; Bradbury 2014). In a small number of cases, the hosting provider passively or actively facilitates the criminal enterprise and shields it from takedown attempts—a practice referred to as ‘bulletproof hosting’.

While there is a wealth of research on security issues in hosting infrastructure, only a fraction has been done from an economic perspective. Moore and Clayton (2007) have studied hosting provider incentives to take down phishing sites. They found evidence for a 'clued-up' effect: it took time before a provider became aware and incentivized enough to start taking down sites. Once that effect occurred, takedown speed rapidly increased and stayed at this improved level. In a follow up study, Moore and Clayton (2009) expanded the research to other forms of Internet content and various notice and takedown regimes. The findings show that requester's incentives outweigh other factors in predicting takedown speed including the content, penalty, and evasion technology. Another study by Vasek and Moore (2012) looked at the responses of hosting providers to notifications of sites that were compromised with malware. It found that notifications that included comprehensive technical data of the detected problem were more likely to trigger takedown action on the side of the providers. This might be related to the competing incentives of providers: they do not want to disrupt service to their customers, while also protecting them and others from the negative consequences of compromised security. Extensive evidence helps them to legitimate countermeasures vis-à-vis their customers.

The overall effects of takedown actions seem limited. Criminal activity might be concentrated at some providers or registrars. Getting those providers to act can dramatically reduce the level of abuse in those networks, but the attackers are prepared for this and merely migrate their activities to other providers (Liu et al. 2011; Levchenko et al. 2011). The result is a game of whack-a-mole. Organizing collective action against criminal activities in the hosting sector is made more difficult because this market is not nearly as consolidated at many other online markets. In the absence of reliable reputation signals, it seems unlikely that market incentives alone will result in higher security levels across the thousands of hosting providers.

Payment Service Providers and Certificate Authorities

Payment and other financial service providers (FSPs) are no strangers to attacks. Annual global losses from financial fraud amount to billions of dollars (R. Anderson et al. 2013). At the same time, these intermediaries have benefited tremendously from the growth of online payments, and in relative terms, fraud has been stable or diminishing (Financial Fraud

Action UK 2015). This is because they have become good at detecting fraud while maintaining convenience, for instance by profiling credit card transactions in real time in their back-end systems, rather than imposing additional security measures on the users directly. One advantage they have is that calculating the monetary gains and losses of certain trade-offs is easier for them than for other sectors. For example, after a data breach credit card issuers can calculate the relative cost of replacing cards or refunding victims of fraudulent cases (Graves, Acquisti, and Christin 2014). The FSPs have also been helped – perhaps paradoxically - by legal regimes in the U.S. and some European countries that limited the liability of consumers in cases of fraud. The burden of proof for fraud was put on the FSPs who actually had the capability to do something about it (Van Eeten and Bauer 2008). In short, financial service providers are in a position to internalize some of the externalities in the sector and thus absorb and mitigate the sector-wide costs of fraud.[6]

Related to payment providers and ecommerce platforms are certificate authorities (CAs)—organizations that issue digital certificates. Such credentials are intended to enable secure online communications, assuring confidentiality and integrity of information and transactions. A series of high profile breaches at CAs in recent years, most notably the breach and bankruptcy of DigiNotar in 2011 brought to light serious weaknesses in the current system (Arnbak and Van Eijk 2012). Vratonjic et al. (2013) looked at how TLS/SSL certificates are deployed on the top one million websites and found many misconfigurations. Durumeric et al. (2013) gathered all digital certificates in use in the public web and found hundreds of CAs with the authority to issue certificates that are recognized by browsers. If any of these CAs were to be breached, certificates can be maliciously issued for any other website, a serious negative externality. Arnbak et al. (2014) used the same data to calculate the market shares of CAs and connect them with their prices. Surprisingly, they found the market share of the most expensive CAs was much larger than cheaper CAs for identical certificates. This observation points to information

[6] Much research has been done into the technical aspects of online fraud, including analyzing malware, detecting fraudulent transactions and reverse engineering banking protocols. These topics touch upon economics but fall out of our scope. Crypto currencies are another topic that has received much attention in the literature due to its technical, economic, and regulatory aspects. The interested reader is referred to the conferences of the International Financial Cryptography Association (IFCA).

asymmetries that create advantages for the largest players. A technical fix to the protocols is required, but their adoption is complicated as long as CAs benefit from the status quo. Other intermediaries however, such as browser vendors and top websites, could play a role in pushing for new standards.

Search Engines and Participative Platforms

Search engines, portals, and participative platforms are used to find content and connect to others. While these intermediaries have explored many different business models in the last decades, the market has converged on a business model in which users receive services for free while revenues are generated from targeted advertising. This development is driven by a combination of network effects and the 'economics of attention': in a world abundant with information, the scarcest resource is the attention of users (Shapiro and Varian 1998). These platforms fight for user attention (Davenport and Beck 2001). Since the marginal cost of information is close to zero, offering services at a low price or free is an economically rational strategy as it maximizes the size of the potential audience. Key players combine 'free' with a variety of nudging techniques to keep users on the platform (an interesting glimpse into this is the controversial study by Kramer et al. (2014) on changing the emotional content of Facebook news feeds to see how it effects users). Creating a revenue stream via advertisement is, of course, not new: broadcasting and newspapers have used the model for decades. The key difference is that targeted advertising can extract higher value (Goldfarb and Tucker 2011).

In terms of cybersecurity, these platforms overall seem to internalize costs to keep their users satisfied. Just to illustrate, Google has a team dedicated to protect users against state-sponsored attacks (Grosse 2012). This is not done out of nicety but as a competitive necessity: MySpace lost to Facebook partially as a result of increased spam and abuse on its network (Dredge 2015). Another example is handling 'click fraud'. When a bot imitates a legitimate user clicking an ad to generate revenue, the advertisers and the platforms are harmed financially and by the erosion of confidence. Chen et al. (2012) suggest that platforms will likely pay the costs of click fraud investigations thus internalizing some of the costs to the system at large. Schneier (2012) draws an analogy with ‘feudal security’ in the past: platforms provide users with security in exchange for allegiance. This approach has some benefits but it also comes with serious risks particularly with regard to privacy. Evidence of this tension is visible in how the platforms balance the interests of users and advertisers: Facebook Connect is preferred by many websites as a federated identity and password system over alternatives because of the user details it shares (Landau and Moore 2012).

2.6 Attacker Behavior

Over the past years, cybercrime has become highly differentiated and professionalized with a vast ‘underground’ (illegal) market that supplies various services required for an attack (Franklin et al. 2007). The division of labor can be illustrated with Zeus, an effective financial malware that caused considerable damage. It was coded by competent programmers that sold it as a do-it-yourself (DIY) kit for several thousand dollars (Riccardi et al. 2013). Fraudsters customized the malware and distributed it to their victims by either renting spamming services, directly deploying it via ‘pay-per-install’ services, or via other methods. After the malware was distributed, the attackers waited for victims and eventually managed to steal money and move it into other accounts. Finally, the money needed to be cashed out without leaving a trail. This was done using people known as ‘money mules’. Thus, four major types of players were involved in Zeus, even though their roles may be carried out by vertically integrated players.

Cybercrime is also affected by the social relations among criminals. Because there is a risk of being cheated by a fellow criminal, Herley and Florêncio (2010) argue that prices in the underground markets are driven down to reduce the risks for buyers. In turn, this makes it less attractive to offer valuable items and creates a cycle of decay. The authors suggest this leads to a two-tier structure with IRC markets as the lower tier, filled with goods that are hard to monetize. Organization of criminal activities rather than ad hoc action is the route to profit. Repeated transactions are also a mechanism that incentivizes buyers and sellers to uphold their promises. Wondracek et al. (2010) looked at parts of the online adult industry employing practices that can be as best described shady: acquiring traffic and infecting visitors for a fee. Their measurements showed that traffic brokers honored the amount and origin of traffic they were contracted for. Another mechanism, deployed in recent years on marketplaces active in the 'dark web', are seller ratings (Christin 2013). Similar to eBay, criminal buyers rate criminal sellers after a transaction; the reputation effect increases the incentives of criminals to stay honest. Despite these differences, both tiers of the underground market generate large negative externalities for society.

To be economically rational, the anticipated success rate and monetary value of an attack need to outweigh its costs. Florêncio and Herley (2013b) use this insight to explain the large gap between potential and actual harm online – the fact that most users do not get their accounts hijacked despite using pet names and birthdates as passwords. Automating attacks to scale is hard because of user diversity; it is also hard to know in advance which users offer sufficient financial prospects to be worth an attack. Herley (2012) presents this as the reason why Nigerian scams—the prince with five million dollars in dire need of your help—are so obvious. These scams are expensive to run and the attacker wants only the most gullible users. In short, many attacks cannot be made profitable on scale, which is one of the reasons why many doomsday scenarios did not unfold as predicted.

Focusing defender efforts on bottlenecks in the attacker monetization chain can be an ingenious way to reduce attacks. A monumental study has been the work of Levchenko et al. (2011) investigating the spam value chain. The team tracked a billion spam URLs and placed orders for the offerings (including Viagra). The study found that spammers fulfilled most purchases with real products (albeit generic versions). Interestingly, spammers refund unsatisfied customers to appease the scarcest resource in the spam value chain: the payment channel. Credit card companies put pressure on the acquiring banks who provide spammers with the ability to receive payments. Such financial relationships are very hard to replace, much harder than the technical infrastructure used for spamming and rogue pharmacies. Spam can be sent extremely cheaply via botnets, making conversion rates as low as one in 12.5 million viable (Kanich et al. 2008). Other elements are also readily available. But setting up relations within a credit card network turns out to be a bottleneck, as it requires legal documents, fees and time. Astonishingly, ninety-five percent of spam-advertised sales used merchant services from a handful of banks. After the study was released, Pfizer and Microsoft, two big targets of spam advertised goods, asked VISA and MasterCard to act against these banks. This made a detrimental blow to spam profitability and production globally (K. Thomas et al. 2015).

Obviously, criminals do not like getting caught and paying a fine or spending time in jail reduces profitability. Law enforcement has been traditionally weak in cyberspace due to crimes crossing jurisdictions. This is gradually changing and law enforcement agencies are ramping up efforts, as evidenced by multiple high profile arrests in recent years (Krebs 2011). Anderson et al. (2013) believe investing in law enforcement abilities to arrest cybercriminals to be very efficient, as many attacks are run by a small number of gangs.

2.7 Policy Options

We have so far looked at the incentives of various actors in the Internet economy and how these affect their security decisions. We have seen that actors impose positive and negative externalities on others and the problems caused by asymmetric information. These are classic examples of market failures that weaken security incentives and will typically lead to suboptimal investment in security. We also saw that some actors, notably among Internet intermediaries operating in multi-sided markets, are willing to bear the costs of mitigating security failures of others. The unique competitive position of this group puts it in a position to make trade-offs between security and other qualities, possibly bringing the entire sector closer to a social optimum. However, in many situations no such endogenous mechanisms are available. This raises the question of whether and how forms of market failure can be remedied and what could be done to strengthen incentives to provide security. A traditional response to market failure is government intervention, but given the conflicting incentives of the state other forms of governance have been proposed as more effective (Brown and Marsden 2013; Moore and Anderson 2012). We continue with a brief discussion of theoretical and empirical contributions to the literature on policy options.

The Costs of Cybersecurity Breaches

Ideally, private and public policy measures would take the actual and potential cost of cybersecurity breeches into account. This is one of the preconditions of rational investment decisions by the private sector and of rational policy design. Unfortunately, while estimates and numbers abound, their reliability and representativeness is difficult to assess. Many reports are generated by players with a stake in inflating the numbers. They often are based on weak evidence and/or overly simplified strong assumptions. The employed methods typically are not publicly available, complicating an assessment of the validity and reliability of the information. Damage is typically assessed at a highly aggregated level and difficult to link to specific incidents. Florêncio and Herley (2013a) show that estimates are frequently biased by a few individual observations. Anderson et al. (2013) argue that the cost of prevention often exceeds the actual damage by orders of magnitude. With these caveats in mind, it is noteworthy that a joint study conducted by McAfee and the Center for Strategic and International Studies (CSIS) estimated the global costs of cybercrime at $445 billion, or about 0.6% of global GDP (CSIS and McAfee 2014).

Absent systematic and reliable metrics, it is at least possible to identify the types of costs good metrics would include. Because of the highly interconnected nature of the Internet, security incidents not only affect the immediate targets of an attack but also have second- and third-round effects on other stakeholders. From a policy perspective, the relevant cost is the total cost to society, which also includes the costs incurred by stakeholders other than those immediately affected. A comprehensive assessment of the costs and benefits of cybersecurity therefore should include the entire ecosystem of players including: users, private sector organizations, public sector organizations, Internet infrastructure providers (software vendors, ISPs, hosting providers, registrars), incident response units, society at large (including opportunity costs, lost efficiency gains, diminished trust and use of the Internet, etc.). It should also include revenues and profits made by cybercriminals, malevolent hackers, and all those seeking to profit from undermining the security of the Internet as these constitute 'bads' (that is costs) to society (Van Eeten, Bauer, and Tabatabaie 2009).

Addressing Information Asymmetries

Several approaches can help address information asymmetries, including mandatory breach disclosure, vulnerability disclosure, certification schemes, and the publication of security metrics.

Mandatory Breach Disclosure. Data breach disclosure and security breach notification laws aim to reduce harms caused to consumers resulting from breaches, and to incentivize organizations to invest in security to avoid bad reputation, by requiring them to notify all affected individuals when personal information has been compromised as a result of an attack or negligence. Critics of mandatory breach disclosure argue that they might perversely desensitize consumers or cause them to overreact. Data breach laws have been enacted in past years across a number of countries and most U.S. states. Romanosky, Telang and Acquisti (2011) found only weak empirical evidence in support of the effectiveness of disclosure laws. Between 2002 and 2009 disclosure requirements reduced identity theft by a mere 6.1 percent. This might be related to a finding by Nieuwesteeg (2013) that the vast majority of security breaches remain unreported, possibly due to firms calculating the risks of being discovered as smaller than notification and reputation costs. These costs include impacts of disclosure on stock market valuations of firms (Gordon, Loeb, and Zhou 2011). As other countries are considering adopting similar laws, there are discussions on how to design the details of such requirements. Thomas et al. (2013), for instance, recommend estimating and communicating the severity of breaches.

Vulnerability Disclosure. Should there be a mandate to publicly disclose a newly discovered software vulnerability? On the one hand, it forces vendors to acknowledge and prioritize releasing a patch; on the other hand it gives attackers information they might otherwise not have. Arora et al. (2010) looked at past evidence by analyzing the U.S. National Vulnerability Database (NVD) from 2000 to 2003. The data suggests that disclosures accelerated patch release. Ransbotham and Mitra (2013) evaluated differences between immediate disclosure and 'responsible disclosure', a procedure for first revealing the vulnerability in private to vendors before making it public after a certain period. Combining a dataset of intrusion detections from several hundred clients with the NVD for 2006 and 2007, the findings cautiously suggest that responsible disclosure is indeed beneficial.

Certification Schemes. Security certifications by trusted third parties have been proposed as fixes to the 'lemons market' problem affecting security aspects of products. Certifications schemes have been tried for software (R. Anderson and Moore 2006), for websites using various 'trust seals', and the ISO 27000 information security standards. The success of these schemes hinges on who pays for the certification, who bears the costs of errors and what the certificates actually measure. Product sellers paying for certification have incentives to go to lax certification authorities. Even worse, Edelman (2011) observes an 'adverse selection' problem in that fraudulent websites have a higher probability of purchasing trust seals. Some certificates only demonstrate compliance with legal provisions. A great example of this is that DigiNotar passed the WebTrust EV audit for CAs just months before its spectacular collapse, while forensics revealed serious security problems (Prins 2011). This is not to say that security certification is not useful. It can still guarantee a basic level of good practices. However, it will not fully solve information asymmetry.

Publishing Security Metrics. Other market signals have also been proposed that simultaneously reduce asymmetry and allow organizations to self-evaluate. Organizations often believe they are doing enough to safeguard security. If they are presented with evidence that they do worse than their peers, they might increase efforts (e.g., Tang et al. 2013). The need for reliable measurements in cybersecurity has been known for a long time (Geer, Hoo, and Jaquith 2003; Pfleeger and Cunningham 2010). However, getting security metrics or measurements right is not an easy task. One should care not to confuse measurable properties with metrics that function as security indicators (Böhme 2010 provides a systematic overview). Designing, measuring, and reporting security metrics is a promising way to help markets produce security more efficiently.

Addressing Externalities

Among the instruments proposed to help mitigate externalities are cyber insurance, liability rules, and better law enforcement.

Cyber Insurance. Insurance for cybersecurity incidents was proposed early on as a solution to align incentives, reduce information asymmetries, and enable firms to better manage risks (Schneier 2004; Böhme 2005). Scholars suggested that insurers would charge different premiums for different levels of cybersecurity and contingent on security practices, which would increase incentives for users to purchase more secure products and adopt better security policies. Nonetheless, these expectations did not materialize and the market for cyber insurance shrunk relative to the Internet economy (Böhme and Schwartz 2010). Shetty et al.

(2010) argue that quantifying cyber risks is fundamentally hard for insurers because of information asymmetries. In addition, the interdependent nature of cyber risks deviates from how risk is typically addressed in insurance markets, complicating the design of workable insurance policies.

Assigning Liability. Making users, organizations, and intermediaries liable for online harms caused by security breaches in their systems could tip security incentives toward higher investment. Fryer et al. (2013) examines the issue thoroughly by looking at liability theories and reviewing proposals in the security economics literature, for example, to make software vendors liable for bugs (August and Tunca 2011) or early calls to make users of bots liable for negligence attacks. In general, 'hard liability' will be a difficult sell in cybersecurity. In cases of clear negligence, it might make sense; however, tort law, existing 'duty to care' and consumer protection laws might be sufficient for the courts. Moreover, the forensics of establishing the facts of a case and measuring harm might not be easy. Due to the interdependencies, cascading harms might occur implying that firms may go bankrupt, become extremely risk-averse innovators, or resolve to create 'shell' companies. 'Softer' mechanisms—such as peer pressure, reputation effects, and regulatory coordination—might be much more effective. An alternative approach suggested by Ioannidis et al. (2013b) is to have an 'information steward' value harms to the ecosystem and allocate costs derived from externalities fairly among targets. Certain intermediaries such as Amazon Marketplace might be doing exactly this.

Better Law Enforcement. An alternative way to reduce externalities – and cybercrime – is to increase costs for attackers. This can be achieved by improving defenses, stricter law enforcement and by increasing the punishment for cybercriminals. Looking at the direct, indirect and defense costs imposed by cybercrime, Anderson et al. (2013) conclude that a more balanced approach is to spend less in anticipation of crime and more in response to it. Given the trans-border nature of many forms of cybercrime, this will also require improved international collaboration among law enforcement agencies.

2.8 Conclusion

In this chapter, we have seen that the economics of cybersecurity is a powerful tool to analyze security failures. By surveying the literature, we looked at the incentives of software vendors, organizations, end-users, Internet intermediaries, and attackers; where they align and produce security; and where the market fails. We highlighted the role of Internet intermediaries in securing the ecosystem. We then listed policy interventions proposed to address market failures. We further saw that the empirical evidence on policies is not always clear. In part, this is due to measurements difficulties, in part because aggregate outcomes are unclear, and in part because the responses of the dynamic system in which cybercrime develops are difficult to anticipate. For example, in the technology race between attackers and defenders tightened security eventually may lead to even more malicious forms of intrusion.

In the end, focusing on incentives rather than the technology helps understand trade-offs and develop sound cybersecurity policy. Given the dynamic nature of cybersecurity, all the issues discussed in this chapter are the subjects of ongoing research. Among emerging topics are security on mobile communications platforms, in the cloud, in the Internet of Things (IoT) and the industrial Internet, user behavior and education across life stages, the establishment of better national and international governance frameworks for security, and the development of better and more reliable metrics.

Chapter 3: The Role of ISPs in Botnet Mitigation[1]

3.1 Introduction

It has been more than a decade since the start of the fight against *botnets*—networks of computers that are infected with malware and controlled by criminals. The many countermeasures have involved end users, ISPs, industry associations, and government. Despite some successes, botnets are still among our most urgent security threats. Botnet mitigation has occurred under the specter of dire predictions about how defenders are losing ground against innovative criminals. Security vendors tend to haunt us with stories about the exponentially growing number of malware variants. However, the empirical facts are less alarming. Microsoft publishes what's arguably the best available data on malware infection rates (e.g., Microsoft 2010; Microsoft 2015). Roughly speaking, at each cleanup cycle, approximately 1 percent of all Windows computers running automatic updates were infected. Most of these machines were unique from one month to the next, which means that the average rate of 1 percent infected users per month translates to roughly one in 10 users experiencing an infection in the course of a year. In an earlier study using a completely different method, we came to a similar estimate (Van Eeten et al. 2010). However, infection rates been relatively stable since 2009 and looks nothing like the dire predictions.

[1] © 2015 IEEE. Reprinted, with permission, from Asghari, Hadi, Michel J.G. van Eeten, and Johannes M. Bauer. 2015. "Economics of Fighting Botnets: Lessons from a Decade Mitigation." *IEEE Security and Privacy* 13 (5): 16–23. Sept.-Oct. 2015. doi: 10.1109/MSP.2015.110. In reference to IEEE copyrighted material used with permission in this thesis, the IEEE does not endorse any of TU Delft's products or services.

Section 3.3 has been extended with parts of an earlier work: Van Eeten, Michel J.G., Hadi Asghari, Johannes M. Bauer, and Shirin Tabatabaie. 2011. "Internet Service Providers and Botnet Mitigation: A Fact-Finding Study on the Dutch Market." The Hague: Netherlands Ministry of Economic Affairs. http://goo.gl/ODJEBg.

Acknowledgements. We thank Dave Rand, the Conficker Working Group, and ShadowServer for providing the data used for this research. We also thank Shirin Tabatabaie for her contribution to earlier stages of the research.

That said, even these infection rates imply significant direct cost to our economies. The cost of cleanup alone is estimated at a few billion US dollars worldwide. The overall direct and indirect costs of the criminal business models based on botnets are very hard to estimate. They likely run into the tens of billions per year (R. Anderson et al. 2013). The scourge of botnets cannot be adequately understood as a mere technical problem. After all, malware has been around since the 1990s, well before botnets emerged. The rise and persistence of botnets reflect changes in the underlying economics of both attackers and defenders—for instance, end users' do not bear the full cost of infections. This has led to increasing pressure on ISPs to undertake mitigation and has prompted the launch of national initiatives to support ISPs in this effort.

3.2 Economic Incentives of Attackers and Defenders

The global malware outbreaks of the early 2000s, such as the ILOVEYOU and CODE RED computer worms, were disruptive and highly visible. Their authors seemed motivated by the quest for notoriety. Then, as more economic transactions moved online and the cost of abusing vulnerabilities decreased, profit-driven criminals entered the scene and rapidly expanded their activities (Franklin et al. 2007). Their incentives changed malware from visible and disruptive to stealthy code that kept the victim's machine up and running as part of a criminal infrastructure. Criminals discovered an expanding array of business models to monetize these infected machines: sending spam, performing distributed denial-of-service attacks, harvesting user credentials, committing financial fraud, hosting phishing sites, performing click fraud on advertising networks, and more.

As cybercrime expanded, the underworld's economic organization also changed. An increase in specialization (for example, malware authors and botnet herders), the emergence of markets for attack tools and services, and a new complex system of monetizing online crime contributed to increases in the virility of attacks. The global migration to broadband, the ability to move attacks in an agile way across national borders, and the limited reach of national law enforcement further boosted the benefit–cost ratio for cybercriminals pursuing a broadening range of online crimes (Moore, Clayton, and Anderson 2009).

However, criminal incentives are only one side of the problem. Another crucial part of the problem relates to the incentives of the defenders—most notably the owners of the infected machines. Botnets typically attack third parties, not owners. This reduces the odds that owners will discover the infection and, more important, undermines their incentive to better secure their machines, as the damage is borne by others or society at large (Wash and MacKie-Mason 2007). At the same time, the benefits of investment in security partially accrue to other users. Hence, "private" cost and benefits of security as seen from an individual user's perspective deviate from "social" costs and benefits to society at large. This is a classic form of an economic externality (the direct effect of the activity of one actor on the welfare of another that is not compensated by a market transaction)—a form of market failure.

ISPs are increasingly called on to undertake mitigation. They are seen as a natural control point because they are the infected machines' gateway to the Internet. Industry groups such as the Messaging Anti-Abuse Working Group and Internet Engineering Task Force, country regulators such as the American Federal Communications Commission, and international organizations such as the Organisation for Economic Cooperation and Development (OECD) have pushed for ISP best practices that include contacting and cleaning up infected customers' machines (Livingood, Mody, and O'Reirdan 2012; OECD 2012; Federal Communications Commission 2012). Complementary to increasing pressure on ISPs, several countries have established national anti-botnet initiatives. These entail national call centers for infected ISP users, codes of conduct for ISPs, and joint mitigation schemes such as centralized clearinghouses that collect and channel infection data to ISPs and their customers.

We empirically assessed the effectiveness of these mitigation strategies. To do this, we first needed a sound way to estimate infection rates across ISPs.

3.3 Methodology

To develop relative infection rates for ISPs, we first processed global datasets of botnet activity and extracted infected machines' IP addresses. Second, we attributed each IP address to an ISP at that point in time. Third, we counted the IP addresses seen in each ISP per day. Fourth, we calculated a normalized measure by dividing this count by the number of subscribers of each ISP. We designed all steps to ensure an effective metric.

Data on Infected Machines

There is currently no authoritative data source to identify the overall population of infected machines around the world. Commercial security providers typically use proprietary data and shield their measurement methods from public scrutiny. This makes it all but impossible to correctly interpret the figures they report and to assess their validity.

The publicly accessible research in this area relies on two types of data sources:

- *Data collected external to botnets*. This data identifies infected machines by their telltale behavior, such as sending spam or participating in distributed denial of service attacks;
- *Data collected internal to botnets.* Here, infected machines are identified by intercepting communications within the botnet itself, for example by infiltrating the command and control infrastructure through which the infected machines get instructions.

Each type of source has its own strengths and weaknesses. The first type typically uses techniques such as honey pots, intrusion detection systems, and spam traps. It has the advantage that it is not limited to machines in a single botnet, but can identify machines across a wide range of botnets that all participate in the same behavior, such as the distribution of spam. The drawback is that there are potentially issues with false positives. The second type typically intercepts botnet communications by techniques such as redirecting traffic or infiltrating IRC channel communication. The advantage of this approach is accuracy: bots connecting to the command and control server are really infected with the specific type of malware that underlies that specific botnet. The downside is that measurement only captures infected machines within a single botnet. Given the fact that the number of botnets is estimated to be in the hundreds (Zhuang et al. 2008), such data is probably not representative of the overall population of infected machines.

Neither type of data sources sees all infected machines, they only see certain subsets, depending on the specific data source. In general, one could summarize the difference between the first and the second source as a tradeoff between representativeness versus accuracy. The first type captures a more representative slice of the problem, but will also include false positives. The second type accurately identifies infected machines, but only for a specific botnet, which implies that it cannot paint a representative picture. This study draws upon three data sources: one of the first type (spam data) and two of the second type (from the Conficker and Gameover Zeus botnets).

Spam Dataset. The spam data is drawn from a *spam trap* – an Internet domain set up specifically to capture spam, whose email addresses have never been published or used to send or receive legitimate email traffic. There is no legitimate way to deliver email to the domain. All the email it receives is indeed spam – as confirmed by logging the content of the messages. The spam trap we used has been running for more than a decade. It logs the IP addresses of machines sending the spam.

Spammers use thousands or even millions of infected machines in a botnet to send out spam. Of the total volume of spam messages that are sent every day, the overwhelming majority is sent through an infected machine. The IP address of the machine that delivered the spam message, therefore, very likely indicates the presence of an infected machine (Zhuang et al. 2008).

We reduced the false-positive rate by including only sources located in retail ISP networks. In 2010, the spam trap recorded an average of 888,000 unique IP addresses and 162 million spam messages per day. Triangulation of the spam data with other security vendors' spam reports shows that the sample is representative.

Conficker Dataset. Conficker started spreading in late 2008 and quickly infected millions of Windows machines. Security experts reverse-engineered the malware and sinkholed[2] its C&C infrastructure shortly after. While this effectively neutralized the botnet, cleanup of machines has

[2] Sinkhole servers are used to disrupt botnet command-and-control (C&C) infrastructures. The sinkholes work in this fashion: computers infected with bots frequently attempt to connect to C&C servers to receive new payloads (i.e., instructions). Security experts redirect the bots to servers they own, by registering or confiscating the C&C domain names. They then log all connections made to them. Since these domains do not host any content, all these connections are initiated by bots.

been slow. This dataset is based on log-files generated by the sinkhole servers; and reliably identifies the IP addresses of the Conficker bots. The sinkhole logs all bots that connect: in 2010, six million unique IP addresses appeared in the sinkhole every day; in 2014, this number was one million.

The Conficker dataset is unique in several ways. First of all, it is not a small sample of a much larger population, but rather captures the universe of its kin. This is because of the way the bot works – most of them will eventually contact one of the sinkholes. Second, this dataset is free from false positives, as, apart from bots, no other machine contacts the sinkholes. These features make the dataset more reliable than the spam. The difference, however, is that the dataset is only indicative of the patterns applicable to one specific botnet. Although Conficker replicated very successfully, it is now an inactive botnet. This means ISPs and other market players may have less powerful incentives to mitigate these infections, different from spam bots, for example.

Gameover Zeus Dataset. Gameover Zeus is considered one of today's most dangerous botnets, partly owing to its sophistication and association with financial fraud. It has withstood multiple takedown attempts, including an international attempt in June 2014. Our third dataset contained IP addresses from a part of the botnet that has remained sinkholed from this attempt—1.9 million unique IP addresses in 42 days. This provided a recent snapshot to compare with the longitudinal sets.

In short, each of our datasets had its strengths and weaknesses, and there was little overlap among them[3]. These differences make the datasets complementary.

Identifying the Location of Infected Machines

For each unique IP address that was logged in one of our data sources, we looked up the *Autonomous System* (AS) and the country where it was located. ASes are the technical entities that own IP addresses. The AS

[3] The low overlap among the datasets is surprising, and has been observed by other researchers (e.g., Metcalf and Spring 2014). One explanation could be that the size of the botnet population is much larger than our samples. Another is there is specialization among bots: a machine that is being used to send out spam is not used to perform network attacks, and vice-versa.

lookup was done with *pyasn* (https://github.com/hadiasghari/pyasn), an open-source tool we have developed for this purpose. We looked up the country using MaxMind's GeoIP database (https://www.maxmind.com). As both AS and geo-location information change over time, we used historical records to establish the origin for the specific moment in time when an IP address was logged in one of our data sources.

Given our research question, we were interested in determining the actual legal entities (companies) that own each AS, and also identify the ones that are broadband ISPs. There is no existing dataset for this purpose[4], so we built our own AS-to-ISP mapping.

We started by selecting countries to include in the study. We ranked all countries based on their number of bots and selected those that cumulatively made up the top 80 percent—in total 39 countries. For comparison, we added all other OECD and EU countries and omitted four countries because of insufficient or incoherent market data. The final set contained 60 countries. For each country, we obtained a list of major ISPs offering broadband access from the commercial TeleGeography GlobalComms dataset (https://www.telegeography.com). To cross-check the completeness of our market data, we compared it with World Bank Data (http://data.worldbank.org/indicator) on the number of Internet subscribers in each country. The ISPs controlled more than 85 percent of the broadband market share in their countries.

Next, we generated a list of ASes to map in each country. We ranked ASes by their IPv4 address space, and selected as many to cumulatively account for 80% of the IPv4 address space in the country, with a minimum of 10 ASes; for seven countries that had a long tail of small ASes (including Russia and U.S.), a lower threshold of 65%-75% was chosen. To this selection we added ASes that were top global hosts of bots (among the top 80% in terms of bot sources), so that smaller malicious ASes were not

[4] This is not surprising. First, ASes are owned by a variety of different organizations: fixed-broadband and mobile ISPs, hosting providers, educational networks, enterprises, etc. Second, large organizations often own a multitude of ASes, with different names, for instance as a result of acquisitions. Third, estimates of the number of ISPs vary widely, depending on whether one counts only transit providers, retail broadband providers, or includes virtual ISPs and resellers of other ISPs' capacity.

excluded. Finally, all ASes from previous mapping efforts (in 2010 and 2012) were added, as they were important at their time.

We used WHOIS records to lookup the name of the entity that administers each AS. We then consulted a variety of sources – such as industry reports, market analyses, news media, and company websites – to see which, if any, of the ISPs in the country it matches. In many cases, the mapping was straightforward. In other cases, additional information was needed – for example, in case of ASs named after an ISP that had since been acquired by another ISP. In those cases, we mapped the AS to its current owner. In most cases, the relationship between an AS and ISP is one-to-one, but this is not always the case. When a large ISP (e.g. AT&T) owns multiple ASes, we group those ASes together. The opposite is also possible, where a multi-national ISP (e.g. UPC Group) shares an AS across several countries and companies. In these cases, we map each AS/CC part separately.

In the end, we mapped 2,260 ASes; of these, 681 belonged to one of the 262 broadband ISPs.

Aggregating IP Counts

We counted each ISP's unique number of IP addresses over a particular time period as a security metric for each ISP. IP addresses have a well-known weakness when used as proxies for machines, as dynamic IP address allocation policies can make the same infected machine appear with multiple IP addresses—the so-called *DHCP* (Dynamic Host Configuration Protocol) *churn* (Stone-Gross, Cova, et al. 2009; Rajab et al. 2007). What's more, these policies vary substantially across ISPs. We mitigated this problem by counting unique IP addresses in much shorter time frames (per day for the spam data and per hour for the Conficker data) and averaging these counts over a year to get the yearly metric. These aggregates—especially the hourly count—underestimate the total number of infected machines at any one point in time. However, this is not important as we sought to compare ISPs rather than determine the absolute number of infections.

Calculating Infection Rates

The final step toward acquiring comparative metrics across ISPs was to account for their size differences. ISPs with more subscribers are likely to have more bots simply due to their larger size (see Figure 3.1). Infection levels are a function of ISP subscribers, which necessitates using normalized metrics or rates. For this purpose, we divided the counts of each ISP's infected machines by its number of subscribers according to the GlobalComms dataset. The resulting dataset provides a longitudinal and cross-sectional view on botnet infection rates in ISPs worldwide.

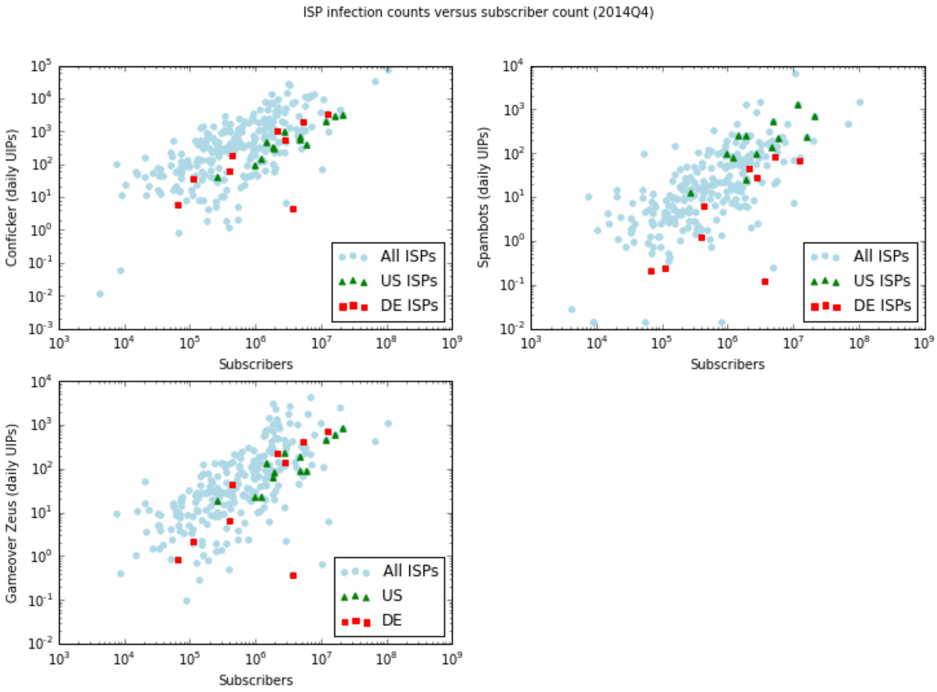


Figure 3.1. ISP infection counts versus subscriber count (2014, Q4)

3.4 Do ISPs Make a Difference?

Do legitimate ISPs in jurisdictions that care about botnets control the bulk of the infected population? The answer might seem trivial, but it isn't. ISPs can identify the customer behind an IP address and, as such, are uniquely positioned to contact and quarantine infected customers. However, this doesn't mean that they can control the bulk of the botnet problem. What portion of the infected population resides in ISP networks as opposed to, say, large corporate, educational, or even cloud networks? Furthermore, are the bots located in the networks of legitimate ISPs that are amenable to codes of conduct or regulatory efforts? Or are they in the networks of shady ISPs operators in jurisdictions with less mature governance structures, outside the reach of industry and the governments pursuing anti-botnet initiatives?

Figure 3.2 shows the proportion of all spam and Conficker bots located in the networks of 262 ISPs, for various years. We can see a relatively concentrated pattern: more than half of all infected machines are located in only 50 large ISPs. (The pattern holds for all years, except for spam in 2014. As overall spam levels have decreased, a larger proportion of the remaining spam-sending machines reside in non-ISP networks, especially hosting providers.) To put these findings into perspective, estimates of the total number of ISPs on the Internet run anywhere from 3,000 to 30,000. The top 50 are large firms that operate leading brands and are well-known to the regulators in their respective countries.

From a policy perspective, this provides an optimistic lesson: getting a limited number of large players to improve mitigation substantially affects the infection rate.

This brings us to a second question: Do the infection rates of these ISPs substantially differ, or are market incentives dictating a certain level of mitigation across ISPs? Earlier work has suggested that ISPs aren't incentivized by the market to undertake mitigation and thus avoid its additional cost (House of Lords 2007). If this is true, we should expect similar performance levels, especially among ISPs operating in the same price-competitive market.

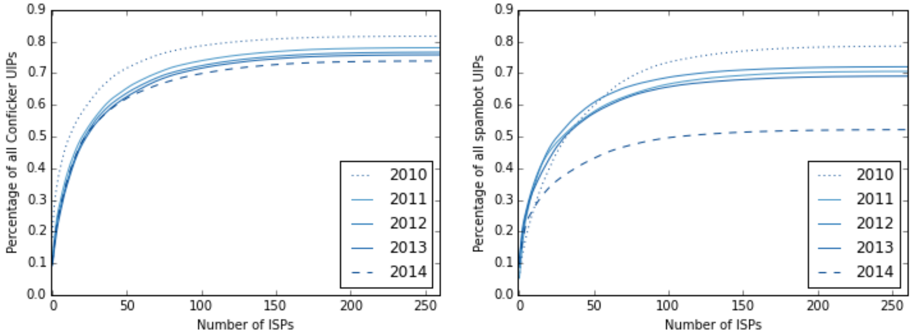


Figure 3.2. Cumulative percentage of infected machines at top ISPs[5]

As we can see in Figure 3.1, infection levels are a function of ISP size: more subscribers means more infections (note that both axes are plotted on a logarithmic scale). However, empirical evidence also shows dramatic variations in infection levels. Similarly sized ISPs can have up to two orders of magnitude difference in terms of numbers of infections. Even ISPs in the same country—under the same competitive pressures and regulatory framework—show differences of more than one order of magnitude, as illustrated by US and German ISPs in the figure. The pattern is consistent across all datasets and stable over time. Statistically, the *coefficient of variation*—a standardized measure of distribution dispersion— is 1.7 for Conficker infection rates and 2.7 for spambot infection rates, putting them both in the high-variance range. The correlation between infection rates in consecutive years is 0.7 for spambot and 0.9 for Conficker, indicating these differences are systematic and not driven by bad luck or transient circumstances.

The main lesson from this finding is that ISPs can and do make a difference. Whether a result of their policies, country policies, or just good luck in their share of Internet users, ISPs are critical control points and have discretion to undertake mitigation at higher levels. This finding is good news for regulators and enough to engage the ISPs. By determining

[5] More than half of all infected machines are located in only 50 large ISPs. The pattern holds for all years, except for spam in 2014: as overall spam levels have decreased, a larger proportion of the remaining spam-sending machines reside in non-ISP networks, especially hosting providers.

what the better-performing ISPs are doing right, we can teach others how to improve their performance.

3.5 Why Do Some ISPs Perform Better?

How can we explain the fact that some ISPs have infection rates that are orders of magnitude worse than those of their peers? In principle, this difference can be due to the ISPs' policies, guided by their incentives, or to their different customer bases. ISP incentives and customer behavior are both shaped by institutional factors, for instance the regulatory framework, education level, or the prevalence of unlicensed software. We use proxies to explore some of these relations in a regression model. This analysis is not a full institutional analysis and is limited to a number of factors for which data was available to us.

We captured regulatory efforts in two proxy variables. The first, *lap_regulator*, indicates whether a country's regulator has joined the London Action Plan (LAP), a consortium that supports the development of anti-spam and anti-botnet policies. LAP has no commitment power over its members and can't establish binding policies. We interpret membership as a proxy for regulatory attention to the issues of spam and botnets. Earlier reports found that LAP membership is correlated with lower infection rates (Kleiner, Nicholas, and Sullivan 2014). Of the 60 countries in our set, 24 had joined LAP. The second variable, *anti_botnet*, indicates whether a country has a national anti-botnet center. Since 2010, seven countries have had one: Australia, Finland, Germany, Ireland, Japan, Korea, and the Netherlands (OECD 2012; Rains 2012). Except for Germany, all these countries are also LAP members.

To control for relevant differences in ISP subscriber populations, we used the unlicensed software rate as a proxy for differences among user populations and a general environment control. Previously known as the piracy rate, this statistic is collected and reported by the Business Software Alliance and indicates the percentage of software installed without a valid license. It reflects user attitudes and is correlated with software-patching practices—higher rates of unlicensed software means more infections. It's also correlated with population properties such as education and wealth.

We used broadband prices (US dollars for a 1-Mbps connection) and broadband speeds as controls for the market conditions under which the ISP operates. The International Telecommunication Union gathers and reports these country averages. We hypothesized that lower prices reflect price pressure on ISPs, leaving less room for security expenditure. Higher broadband speeds might have an effect in both directions: as an enabler of malware spreading and as an indicator of a more mature and better managed infrastructure. We left out several other typical country-level variables, such as information and communications technology (ICT) development, to avoid problems of multicollinearity.

We include the log of the number of an ISP's subscribers as a proxy for its size. There are many reasons to include this variable as it relates to botnet mitigation. First, large ISPs are thought to react differently to regulatory pressure and peer pressure with regard to cleaning up their networks. Second, because of the scale of their operations, large ISPs are likely to have higher levels of automation in abuse handling and cleanup. This might reduce the cost per mitigation action.

We used fixed effect dummies as intercepts for each year. We wanted to control for the large variation in botnet activity across years driven by global attacker and defender behavior, beyond ISPs. Using fixed effects, we created a baseline level for each year against which we could then further distinguish ISP differences.

All these parameter estimates are partial effects under the assumption that all other factors remain unchanged. The variation among ISPs partially reflects differences among subscriber populations. Increased unlicensed software use correlates with higher ISP infection rates. Differences in our proxies for market forces had no impact. Broadband price and speed coefficient were close to zero and had no effect.

Table 3.1. Generalized linear models (GLMs) for ISP infection rates

Variable	**Mean (sd)**	**DV: isp_conficker_rate (c_uips_h offset by subs) GLM n.binom., log-link**			**DV: isp_spambot_rate (s_uips_d offset by subs) GLM n.binom., log-link**		
		Coefficient	Std error	P>|z|	Coefficient	Std error	P>|z|
LAP regulator	0.47 (0.50)	0.033	0.059	0.580	–0.163	0.096	0.091
anti_botnet	0.16 (0.36)	–0.202	0.076	0.008	–0.276	0.134	0.049
unlicensed sw	45.3 (19.9)	0.047	0.002	0.000	0.043	0.003	0.000
broadband price	24.4 (9.6)	–0.016	0.003	0.000	0.000	0.005	0.933
broadband speed	3.9 (6.4)	0.019	0.004	0.000	–0.001	0.006	0.875
isp_subs_l	5.6 (0.7)	–0.239	0.034	0.000	–0.264	0.052	0.000
FE_intercepts		for all years P>|Z| is 0.000			for all years P>|Z| is 0.000		
Deviance		model: 1,056/null: 2,562			model: 1,727/null: 4,694		

Note: 1,285 observations, 262 ISPs, 5 years

Large ISPs have, on average, fewer infections per customer than smaller ISPs. This is in line with qualitative data from interviews with European and US ISPs about how they handle infected customers: large ISPs are more likely to have automated key parts of their botnet and abuse response process (Van Eeten et al. 2011). Using automation helps reduce the cost of identifying, notifying, and mitigating infected customers, thus making it more economically efficient to mitigate on a larger scale.

In terms of policies, we found support that having a national anti-botnet center correlates with lower ISP infection rates (negative and significant). An active regulator seems to have significant impact.

An interaction between the policy variables and unlicensed software complicates our interpretation of the regression coefficients: countries that have an anti-botnet center also have considerably lower unlicensed software use. An intuitive way to disentangle such effects is to plot the regression predictor for different variable combinations (see Figure 3.3). Each curve shows the regression prediction given various combinations of regulatory activity and unlicensed software use. Although the presence of anti-botnet initiatives shifts the curves downward, the effect was relatively small compared to unlicensed software use in the country, which we know also correlate negatively with indexes of wealth and ICT development.

We should note that both regression models have unexplained variance because current models didn't capture many ISP-level differences. This is an area for further research, for instance, looking at actual network management policies (J. Zhang et al. 2014). The unexplained variance can also account for the differences among the spam_rate and conficker_rate models for the lap_regulator coefficient where they differ.

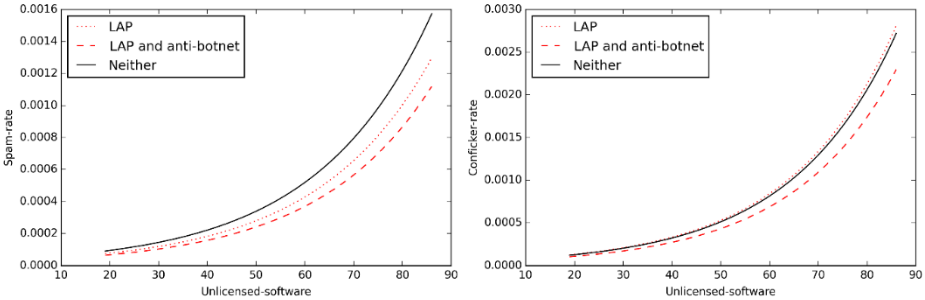


Figure 3.3. Reg. predictions for policies and unlicensed software[6]

3.6 Which Policies Are Effective?

Our analysis suggests that ISP incentives partially drive infection levels and that these, in turn, can be influenced by policy efforts. In the model, we included two explicit policy factors: LAP membership—as a proxy for regulatory involvement—and presence of a national anti-botnet initiative. Only the latter was significant. However, it's important to realize that the variables overlap: all countries that have a national initiative are also LAP members, except for Germany. So the impact of the anti-botnet variable is really a combined effect of LAP plus the initiatives. LAP members without a national initiative are probably less proactive.

[6] Each curve shows the regression prediction given different combinations of regulatory activity and unlicensed software use. The London Action Plan (LAP) curve indicates countries that are only part of the LAP (lap_regulator is set to one and anti_botnet set to zero), LAP and anti_botnet indicates countries that are part of the LAP and have an anti-botnet center (lap_regulator and anti_botnet both one), and neither indicates countries with neither policy (lap_regulator and anti_botnet both zero). All other variables are set at their mean.

National initiatives change ISP incentives in several ways. First, a national initiative demonstrates government involvement, which puts more pressure on ISPs to invest in security. Second, a national center reduces mitigation cost for ISPs, enabling them to increase their impact with the same resources. For example, the Netherlands' centralized clearinghouse, called AbuseHUB, is partially government funded. It sets up relationships with suppliers of abuse data, such as the ShadowServer Foundation and Microsoft. It has also automated the parsing of this incoming data and feeds it directly into member ISPs' automated abuse incident response processes. All this reduces ISP costs and scales up mitigation. Anti-botnet centers in other countries, such as Korea and Germany, provide actual customer support via a publicly funded call center. This shifts some of the mitigation cost to the tax payer, reducing the burden on ISPs.

In short, policies that incentivize ISPs appear effective, particularly when they take the form of national anti-botnet initiatives. However, the centers' impact shouldn't be overestimated. The extent to which ISPs respond to these reduced costs will differ. In an evaluation of the Dutch initiative, we found that, even though large ISPs received the same data feeds, if and when they acted on this data differed among providers, as evidenced by the fact that their relative infection rates continued to differ by a factor of three to five. We see similar variation in other countries with a national initiative. In the end, anti-botnet initiatives seem to nudge provider policies in the right direction but don't dictate them.

We also see that policy impact is modest when compared to contextual factors such as the rate of unlicensed software use. Of course, policy can also try to influence piracy rates—and, in many countries, it does, as part of their intellectual property protections. This raises an interesting policy option for botnet mitigation: focusing on the ICT infrastructure's general health might be the most effective way to reduce the societal burden of botnets.

3.7 Conclusion

The botnet battle hasn't been lost. Infection rates have been be relatively stable for several years. At a minimum, the dire predictions have continually been thwarted by the facts. That being said, the economic damage associated with botnets still runs into tens of billions of dollars per year.

In the search for more effective mitigation, the focus has shifted from end users to Internet intermediaries, most notably the ISPs. We empirically tested whether the assumptions behind this more recent strategy hold over time. They do. The problem of botnets isn't located in the networks of shady ISPs in countries with poor governance structures. The well-known and well-established ISPs in relatively well-governed jurisdictions control the bulk of the problem.

Within the ISP population, infection rates differ dramatically—more than two orders of magnitude. Even in the same country, infection rates can differ by more than one order of magnitude. This suggests that ISPs have discretion to enhance mitigation. Their economic incentives aren't dictated by the need to operate in markets that are primarily driven by price competition.

The differences among ISPs' infection rates can be understood from other incentives, most notably the cost of mitigation and the pressure of regulatory involvement. Large ISPs have lower infection rates, pointing to the benefits of automation in handling infection incidents, which lowers the cost per cleanup and allows ISPs to better scale up their mitigation. Regulatory involvement—that is, "soft regulation"—not only incentivizes ISPs to exert more effort but has also led to public–private initiatives, such as national anti-botnet centers, that reduce mitigation costs.

One sobering finding is that external factors, such as the level of software piracy in a country, might overwhelm the effects of anti-botnet policies. That said, some of these factors might also be the focus of more general cybersecurity policies. Such an approach might be more economically efficient, suggesting that we shouldn't focus our efforts too myopically on the botnets themselves.

Chapter 4: Conficker Botnet Cleanup After Six Years[1]

4.1 Introduction

For years, researchers have been working on methods to take over or disrupt the command-and-control (C&C) infrastructure of botnets (e.g., Holz et al. 2008; Stone-Gross, Cova, et al. 2009; Nadji et al. 2013). Their successes have been answered by the attackers with ever more sophisticated C&C mechanisms that are increasingly resilient against takeover attempts (Rossow et al. 2013).

In pale contrast to this wealth of work stands the limited research into the other side of botnet mitigation: cleanup of the infected machines of end users. After a botnet is successfully sinkholed, the bots or zombies basically remain waiting for the attackers to find a way to reconnect to them, update their binaries, and move the machines out of the sinkhole. This happens with some regularity. The recent sinkholing attempt of GameoverZeus (Shadowserver 2014), for example, is more a tug of war between attackers and defenders, rather than definitive takedown action. The bots that remain after a takedown of C&C infrastructure may also attract other attackers, as these machines remain vulnerable and hence can be re-compromised.

[1] This chapter has been peer reviewed and published as: Asghari, Hadi, Michael Ciere, Michel J.G. van Eeten, 2015. "Post-Mortem of a Zombie: Conficker Cleanup After Six Years". Proceedings of the 24th USENIX Security Symposium (Security '15). https://goo.gl/LnguCn.

Acknowledgements. The authors would like to explicitly thank Chris Lee, Paul Vixie and Eric Ziegast for providing us with access to the Conficker sinkhole and supporting our research. We also thank Ning An, Ben Edwards, Dina Hadziosmanovic, Stephanie Forest, Jan Philip Koenders, Rene Mahieu, Hooshang Motarjem, Piet van Mieghem, Julie Ryan, as well as the participants of Microsoft DCC 2015 and USENIX reviewers for contributing ideas and providing feedback at various stages.

To some extent, cleanup of bots is an automated process, driven by antivirus software, software patches, and tools like Microsoft's Malicious Software Removal Tool, which is included in Windows' automatic update cycle. These automated actions are deemed insufficient, however. In recent years, wide support has been established for the idea that Internet Service Providers (ISPs) should contact affected customers and help them remediate their compromised machines (Van Eeten et al. 2011; Livingood, Mody, and O'Reirdan 2012). This shift has been accompanied by proposals to treat large-scale infections as a public health issue (Clayton 2011; Sullivan 2012). As part of this public health approach, we have seen the emergence of large-scale cleanup campaigns, most notably in the form of national anti-botnet initiatives. Public and private stakeholders, especially ISPs, collaborate to notify infected end users and help them clean their machines. Examples include Germany's Anti-Botnet Advisory Center (BotFrei), Australia's Internet Industry Code of Practice (iCode), and Japan's Cyber Clean Center (superseded by ACTIVE) (OECD 2012).

Setting up large-scale cleanup mechanisms is cumbersome and costly. This underlines the need to measure whether these efforts are effective. The central question of this paper is: What factors drive cleanup rates of infected machines? We explore whether the leading national anti-botnet initiatives have increased the speed of cleanup.

We answer this question via longitudinal data from the sinkhole of Conficker, one the largest botnets ever seen. Conficker provides us with a unique opportunity to study the impact of national initiatives. It has been six years since the vulnerability was patched and the botnet was sinkholed. The attackers have basically abandoned it years ago, which means that infection rates are driven by cleanup rather than the attacker countermeasures. Still, nearly a million machines remain infected (see Figure 4.1). The Conficker Working Group, the collective industry effort against the botnet, concluded in 2010 that remediation has been a failure (Rendon Group 2011, iii).

Before one can draw lessons from sinkhole data, or from most other data sources on infected machines, several methodological problems have to be overcome. This paper is the first to systematically work through these issues, transforming noisy sinkhole data into comparative infection metrics and normalized estimates of cleanup rates.

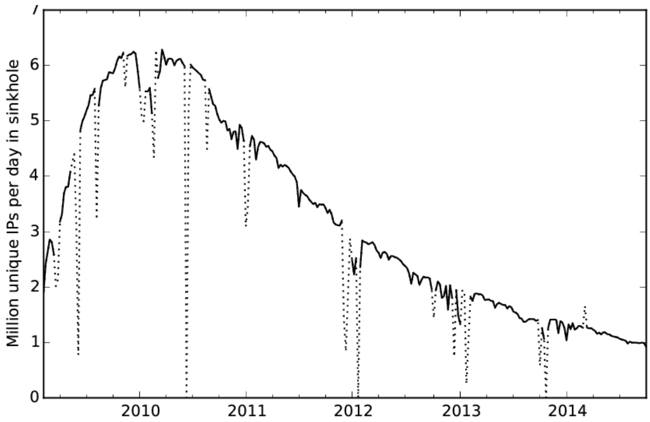


Figure 4.1. Conficker bots worldwide

For this research, we were generously given access to the Conficker sinkhole logs, which provide a unique long-term view into the life of the botnet. The dataset runs from February 2009 until September 2014, and covers all countries—241 ISO codes—and 34,000 autonomous systems. It records millions of unique IP addresses each year—for instance, 223 million in 2009, and 120 million in 2013. For this paper, we focus on bots located in 62 countries. In sum, the contributions of this paper are as follows:

1. We develop a systematic approach to transform noisy sinkhole data into comparative infection metrics and normalized estimates of cleanup rates.
2. We present the first long-term study on botnet remediation.
3. We provide the first empirical test of the best practice exemplified by the leading national anti-botnet initiatives.
4. We identify several factors that influence cleanup rates.

4.2 Background

Conficker Timeline and Variants

In this section, we will provide a brief background on the history of the Conficker worm, its spreading and defense mechanisms, and some milestones in the activities of the Conficker Working Group.

The Conficker worm, also known as Downadup, was first detected in November 2008. The worm spread by exploiting vulnerability MS08-067 in

Microsoft Windows, which had just been announced and patched. The vulnerability affected all versions of Microsoft Windows at the time, including server versions. A detailed technical analysis is available in (Porras, Saidi, and Yegneswaran 2009). Briefly put, infected machines scanned the IP space for vulnerable machines and infected them in a number steps. To be vulnerable, a machine needed to be unpatched and online with its NetBIOS ports open and not behind a firewall. Remarkably, a third of all machines had still not installed the patch by January 2009, a few months after its availability (Goodin 2009). Consequently, the worm spread at an explosive rate. The malware authors released an update on December 29, 2008, which was named Conficker-B. The update added new methods of spreading, including via infected USB devices and shared network folders with weak passwords. This made the worm propagate even faster (Rendon Group 2011).

Infected machines communicated with the attackers via an innovative, centralized system. Every day, the bots attempted to connect to 250 new pseudo-randomly generated domains under eight different top-level domains. The attackers needed to register only one of these domains to reach the bots and update their instructions and binaries. Defenders, on the other hand, needed to block all these domains, every day, to disrupt the C&C. Another aspect of Conficker was the use of intelligent defense mechanisms that made the worm harder to remove. It disabled Windows updates, popular anti-virus products, and several Windows security services. It also blocked access to popular security websites (Porras, Saidi, and Yegneswaran 2009; Rendon Group 2011).

Conficker continued to grow, causing alarm in the cybersecurity community about the potential scale of attacks, even though the botnet had not yet been very active at that point. In late January, the community—including Microsoft, ICANN, domain registries, anti-virus vendors, and academic researchers—responded by forming the Conficker Working Group (Rendon Group 2011; Schmidt 2014). The most important task of the working group was to coordinate and register or block all the domains the bots would use to communicate, staying ahead of the Conficker authors. The group was mostly successful in neutralizing the botnet and disconnecting it from its owners; however, small errors were made on two occasions in March, allowing the attackers to gain access to part of the botnet population and update them to the C variant.

The Conficker-C variant had two key new features: the number of pseudo-randomly generated domains was increased to 50,000 per day, distributed over a hundred different TLDs, and a P2P update protocol was added. These features complicated the work of the working group. On April 9, 2009, Conficker-C bots upgraded to a new variant that included a scareware program that sold fake anti-virus at prices between $50–$100. The fake anti-virus program, probably a pay-per-install contract, was purchased by close to a million unwitting users, as was later discovered. This use of the botnet prompted law enforcement agencies to increase their efforts to pursue the authors of Conficker.[2] Eventually, in 2011, the U.S. Federal Bureau of Investigation, in collaboration with police in several other countries, arrested several individuals associated with this $72-million scareware ring (Krebs 2011; Kirk 2011).

National Anti-Botnet Centers

Despite the successes of the cybersecurity community in neutralizing Conficker, a large number of infected machines remained. This painful fact was recognized early on; in its 'Lessons Learned' document from 2010, the Conficker Working Group reported remediation as its top failure (Rendon Group 2011, iii). Despite being inactive, Conficker remains one of the largest botnets. As recent as June 2014, it was listed as the #6 botnet in the world by anti-virus vendor ESET (2014). This underlines the idea that neutralizing the C&C infrastructure in combination with automated cleanup tools will not eradicate the infected machines; some organized form of cleanup is necessary.

During the past years, industry and regulatory guidelines have been calling for increased participation of ISPs in cleanup efforts. For instance, the European Network and Information Security Agency (Plohmann, Gerhards-Padilla, and Leder 2011), the Internet Engineering Task Force (Livingood, Mody, and O'Reirdan 2012), the Federal Communications Commission (2012), and the Organization for Economic Cooperation and Development (2012) have all called upon ISPs to contact infected customers and help them clean up their compromised machines.

The main reason for this shift is that ISPs can identify and contact the owners of the infected machines, and provide direct support to end users.

[2] Microsoft also set a $250,000 bounty for information leading to arrests.

They can also quarantine machines that are not cleaned up. Earlier work has found evidence that ISP mitigation can significantly impact end user security (Van Eeten et al. 2010).

Along with this shift of responsibility towards ISPs, some countries have established national anti-botnet initiatives to support the ISPs and end users in cleanup efforts. The setup is different in each country, but typically it involves the collection of data on infected machines (from botnet sinkholes, honeypots, spamtraps, and other sources); notifying ISPs of infections within their networks; and providing support for end users, via a website and sometimes a call-center.

A number of countries have been running such centers, often as part of a public-private partnership. Table 4.1 lists the countries with active initiatives in late 2011, according to an OECD report (2012). The report also mentions the U.S. & U.K. as developing such initiatives. The Netherlands is listed as having 'ISP-specific' programs, for at that time, KPN and Ziggo—the two largest ISPs—were heading such programs voluntarily (Van Eeten et al. 2011).[3] Finland, though not listed, has been a leader with consistently low infection rates for years. It has had a notification and cleanup mechanism in place since 2005, as part of a collaboration between the national CERT, the telco regulator, and main ISPs (Koivunen 2012; Rains 2012). At the time of writing, other countries are starting anti-botnet centers as well. In the EU alone, seven new national centers have been announced (Advanced Cyber Defence Centre 2014). These will obviously not impact the past cleanup rates of Conficker, but they do underwrite the importance of empirically testing the efficacy of this mitigation strategy.

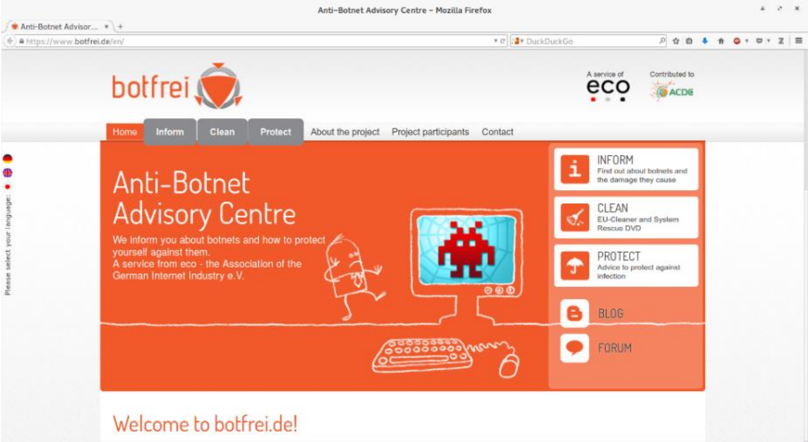
Table 4.1. List of countries with anti-botnet initiatives (OECD 2012)

Country	Initiative
Australia	Internet Industry Code of Practice (iCode)
Germany	German Anti-Botnet Initiative (BotFrei)
Ireland	Irish Anti-Botnet Initiative
Japan	Cyber Clean Center / ACTIVE
Korea	KrCERT/CC Anti-Botnet Initiative
Netherlands	Dutch Anti-Botnet Initiative (Abuse-Hub)

[3] It has now been replaced by a wider initiative involving all main providers and covering the bulk of the broadband market.

Figure 4.2 shows the website of the German anti-botnet advisory center, *botfrei*. The center was launched in 2010 by eco, the German Internet industry association, and is partially funded by the German government. The center does three things. First, it identifies users with infected PCs. Second, they inform the infected customers via their ISPs. Third, they offer cleanup support, through a website—with free removal tools and a forum—and a call center (Karge 2010). The center covers a wide range of malware, including Conficker. We should mention that eco staff told us that much of the German Conficker response took place before the center was launched. In their own evaluations, the center reports successes in terms of the number of users visiting its website, the number of cleanup actions performed, and overall reductions in malware rates in Germany. Interestingly enough, a large number of users visit botfrei.de directly, without being prompted by their ISP. This highlights the impact of media attention, as well as the demand for proactive steps among part of the user population.

We only highlight Germany's botfrei program as an example. In short, one would expect that countries running similar anti-botnet initiatives to have higher cleanup rates of Conficker bots. This, we shall evaluate.



Anti-Botnet Advisory Centre

We inform you about botnets and how to protect yourself against them.
A service from eco - the Association of the German Internet Industry e.V.

Find out about botnets and the damage they cause

EU-Cleaner and System Rescue DVD

Advice to protect against infection

Welcome to botfrei.de!

Figure 4.2. The German Anti-Botnet Advisory Center website

Related Work

Similar to other botnets, much of the work on the Conficker worm has focused predominantly on technical analysis (e.g., Porras, Saidi, and

Yegneswaran 2009). Other research has studied the worm's outbreak and modeled its infection patterns (e.g., C. Zhang, Zhou, and Chain 2015; Irwin 2012; Shin et al. 2012; Weaver 2010). There have also been a few studies looking into the functioning of the Working Group (e.g., Schmidt 2014). None of this work looks specifically at the issue of remediation. Although Shin et al. (2012) uses the same dataset as this paper to model the spread of the worm, their results are skewed by the fact that they ignore DHCP churn, which is known to cause errors in infection rates of up to one order of magnitude for some countries Stone-Gross, Cova, et al. (2009).

This paper also connects to the literature on botnet mitigation, specifically to cleanup efforts. This includes the industry guidelines we discussed earlier (e.g., Plohmann, Gerhards-Padilla, and Leder 2011; OECD 2012; Federal Communications Commission 2012; Livingood, Mody, and O'Reirdan 2012); as well as academic work that tries to model different mitigation strategies (e.g., Clayton 2011; Sullivan 2012; Hofmeyr et al. 2013; Khattak et al. 2014). We contribute to this discussion by bringing longitudinal data to bear on the problem and empirically evaluating one of the key proposals to emanate from this literature. This expands some of our earlier work.

In a broader context, a large body of research focuses on other forms of botnet mitigation (e.g., Holz et al. 2008; Stone-Gross, Cova, et al. 2009; Nadji et al. 2013; Rossow et al. 2013), modeling worm infections (e.g., Staniford, Paxson, and Weaver 2002; Zou, Gong, and Towsley 2002; Zou et al. 2003; Pastor-Satorras et al. 2014), and challenges in longitudinal cybersecurity studies. For the sake of brevity, we will not cite more works in these areas here (—except for works used in other sections).

4.3 Methodology

Answering the central research question requires a number of steps. First, we set out to derive reliable estimates of the number of Conficker bots in each country over time. This involves processing and cleaning the noisy sinkhole data, as well as handling several measurement issues. Later, we use the estimates to compare infection trends in various countries, identify patterns, and specifically see if countries with anti-botnet initiatives have done any better. We do this by fitting a descriptive model to each country's time-series of infection rates. This provides us with a specific set of parameters, namely the growth rate, the peak infection level, and the decay rate. We explore a few alternative models and opt for a two-piece model that accurately captures these characteristics. Lastly, to answer the central question, we explore the relationship between the estimated parameters and a set of explanatory variables.

The Conficker Dataset

The Conficker dataset has four characteristics that make it uniquely suited for studying large-scale cleanup efforts. First, it contains the complete record of one sinkholed botnet, making it less convoluted than for example spam data, and with far fewer false positives. Second, it logs most of the population on a daily basis, avoiding limitations from seeing only a sample of the botnet. Third, the dataset is longitudinal and tracks a period of almost six years. Many sinkholes used in scientific research typically cover weeks rather than months, let alone six years. Fourth, most infection data reflects a mix of attacker and defender behavior, as well as different levels (global & local). This makes it hard to determine what drives a trend – is it the result of attacker behavior, defender innovation, or just randomness? Conficker, however, was neutralized early on, with the attackers losing control and abandoning the botnet. Most other global defensive actions (e.g. patching and sinkholing) were also done in early 2009. Hence, the infection levels in our dataset predominantly reflect cleanup efforts. These combined attributes make the Conficker dataset excellent for studying the policy effects we are interested in.

Raw Data. Our raw data comes from the Conficker sinkhole logs. As explained in the background section, Conficker bots used an innovative centralized command and control infrastructure. The bots seek to connect to a number of pseudo-random domains every day, and ask for updated instructions or binaries from their masters. The algorithm that generates this domain list was reverse engineered early on, and various teams, including the Conficker Working Group, seized legal control of these domains. The domains were then 'sinkholed': servers were set up to listen and log every attempt to access the domains. The resulting logs include the IP address of each machine making such an attempt, timestamps, and a few other bits of information.

Processing Sinkhole Logs. The raw logs were originally stored in plain text, before adoption of the *nmsg* binary format in late 2010. The logs are huge; a typical hour of logs in January 2013 is around half a gigabyte, which adds up to tens of terabytes per year. From the raw logs, we extract the IP address, which in the majority of cases will be a Conficker A, B, or C bot (the sinkholed domains were not typically used for other purposes). Then, using the MaxMind GeoIP database (MaxMind 2015) and an IP-to-ASN database based on Routeviews BGP data (Asghari and Noroozian 2014), we determine the country and Autonomous System that this IP address belonged to at that moment in time. We lastly count the number of unique IP addresses in each region per hour. With some exceptions, we capture most Conficker bots worldwide. The limitations are due to sinkholes downtime; logs for some sinkholed domains not being handed over to the working group (Rendon Group 2011); and bots being behind an egress firewall, blocking their access to the sinkhole. None of these issues however creates a systematic bias, so we may treat them as noise.

After processing the logs, we have a dataset spanning from February 2009 to September 2014, covering 241 ISO country codes and 34,000 autonomous systems. The dataset contains approximately 178 million unique IP addresses per year. In this paper we focus on bots located in 62 countries, which were selected as follows. We started with the 34 members of the Organization for Economic Cooperation and Development (OECD), and 7 additional members of the European Union, which are not part of the OECD. These countries have a common development baseline, and good data is available on their policies, making comparison easier. We add to this list 23 countries that rank high in terms of Conficker or spam bots—cumulatively covering 80 percent of all such bots worldwide. These countries are interesting from a cybersecurity perspective. Finally, two countries were removed due to severe measurement issues affecting their bot counts, which we will describe later. The full list of countries can be seen in Figure 4.12 and Figure 4.13.

Counting Bots from IP Addresses

The Conficker dataset suffers from a limitation that is common among most sinkhole data and other data on infected machines, such as spam traps, firewall logs, and passive DNS records: one has to use IP addresses as a proxy for infected machines. Earlier research has established that IP addresses are coarse unique identifiers and they can be off by one order of magnitude in a matter of days (Stone-Gross, Cova, et al. 2009), because of differences in the dynamic IP address allocation policies of providers (so-called *DHCP churn*). Simply put, because of dynamic addresses, the same infected machine can appear in the logs under multiple IP addresses. The higher the churn rate, the more over-counting.

Figure 4.3 visualizes this problem. It shows the count of unique Conficker IP addresses in February 2011 over various time periods—3 hours, 12 hours, one day, up to a week. We see an interesting growth curve, non-linear at the start, then linear. Not all computers are powered on at every point in time, so it makes sense to see more IP addresses in the sinkhole over longer time periods. However, between the 6th and 7th day, we have most likely seen most infected machines already. The new IP addresses are unlikely to be new infections, as the daily count is stable over the period. The difference is thus driven by infected machines reappearing with a new IP address.

The figure shows IP address counts for the Netherlands and Germany. From qualitative reports we know that IP churn is relatively low in the Netherlands—an Internet subscriber can retain the same IP address for months—while in Germany the address typically changes every 24 hours. This is reflected in the figure: the slope for Germany is much steeper. Should one ignore the differences in churn rates among countries, and simply count unique IP addresses over a week, then a severe bias will be introduced against countries such as Germany. Using shorter time periods, though leading to under-counting, decreases this bias.[4] We settle for this simple solution: counting the average number of unique IPs *per hour*, thereby eliminating the churn factor. This hourly count will be a fraction of the total bot count, but that is not a problem when we make comparisons based on scale-invariant measures, such as cleanup rates.

[4] Ideally, we would calculate a churn rate — the average number of IPs per bot per day — and use that to generate a good estimate of the actual number of bots. That is not an easy task, and requires making quite a number of assumptions.

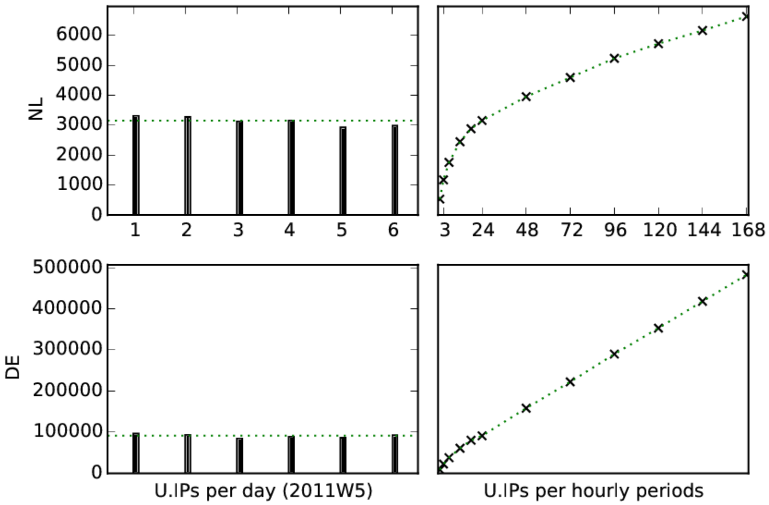


Figure 4.3. Unique IP counts over various time-periods

Network Address Translation (NAT) and the use of HTTP proxies can also cause under-counting. This is particularly problematic if it happens at the ISP level, leading to large biases when comparing cleanup policies. After comparing subscriber numbers with IP address space size in our selection of countries, we concluded that ISP-level NAT is widely practiced in India. As we have no clear way of correcting such cases, we chose to exclude India from our analysis.

Missing Measurements

The Conficker dataset has another problem that is also common: missing measurements. Looking back at Figure 4.1, we see several sudden drops in bot counts, which we highlighted with dotted lines. These drops are primarily caused by sinkhole infrastructure downtime—typically for a few hours, but at one point even several weeks. These measurement errors are a serious issue, as they only occur in one direction and may skew analysis. We considered several approaches to deal with them. One is to model the measurement process explicitly. Another is to try and minimize the impact of aberrant observations by using robust curve-fitting methods. This adds complexity and is not very intuitive. A third option is to pre-process the data using curve smoothing techniques; e.g., taking the exponentially weighted rolling average or applying the Hodrick-Prescott filter. Although not necessarily wrong, this adds its own biases as it changes data. The fourth approach, and the one that we use, is to detect and remove the outliers heuristically.

For this purpose, we calculate the distance between each weekly value in the global graph with the rolling median of its surrounding two months, and throw out the top 10%. This works because most bots log in about once a day, so the IP counts of adjacent periods are not independent. The IP count may increase, decrease, or slightly fluctuate, but a sudden decrease in infected machines followed by a sudden return of infections to the previous level is highly unlikely. The interested reader is referred to the appendix to see the individual graphs for all the countries with the outliers removed.[5]

Normalizing Bot Counts by Country Size

Countries with more Internet users are likely to have more Conficker bots, regardless of remediation efforts. Figure 4.4 illustrates this. It thus makes sense to normalize the unique IP counts by a measure of country size; in particular if one is to compare peak infection rates. One such measure is the size of a country's IP space, but IP address usage practices vary considerably between countries. A more appropriate denominator and the one we use is the number of Internet broadband subscribers. This is available from a number of sources, including the Worldbank Development Indicators.

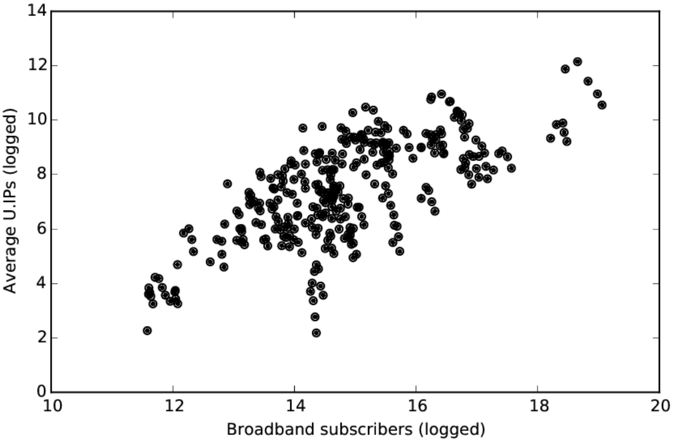


Figure 4.4. Conficker bots versus broadband subscribers

[5] An extreme case was Malaysia, where the length of the drops and fluctuations spanned several months. This most likely indicates country-level egress filtering, prompting us to also exclude Malaysia from the analysis.

4.4 Modeling Infections

Descriptive Analysis

Figure 4.5 shows the Conficker infection trends for Germany, United States, France, and Russia. The x-axis is time; the y-axis is the average number of unique IP addresses seen per day in the sinkhole logs, corrected for churn. We observe a similar pattern: a period of rapid growth; a plateau period, where the number of infected machines peaks and remains somewhat stable for a short or longer amount of time; and finally, a period of gradual decline.

What explains these similar trends among countries, and in particular, the points in time where the changes occur on the graphs? At first glance, one might think that the decline is set off by some event—for instance, the arrest of the bot-masters, or a release of a patch. However, this is not the case. As previously explained, all patches for Conficker were released by early 2009, while the worm continued spreading after that. This is because most computers that get infected with Conficker are "unprotected"—that is, they are either unpatched or without security software, in case the worm spreads via weak passwords on networks shares, USB drives, or domain controllers. The peak in 2010 – 2011 is thus the worm reaching some form of saturation where all vulnerable computers are infected. In the case of business networks, administrators may have finally gotten the worm's re-infection mechanisms under control (Microsoft 2012a).

Like the growth phase and the peak, the decline can also not be directly explained by external attacker behavior. Arrests related to Conficker occurred mid-2011, while the decline started earlier. In addition, most of the botnet was already out of the control of the attackers. What we are seeing appears to be a 'natural' process of the botnet. Infections may have spread faster in some countries, and cleanups may have been faster in others, but the overall patterns are similar across all countries.

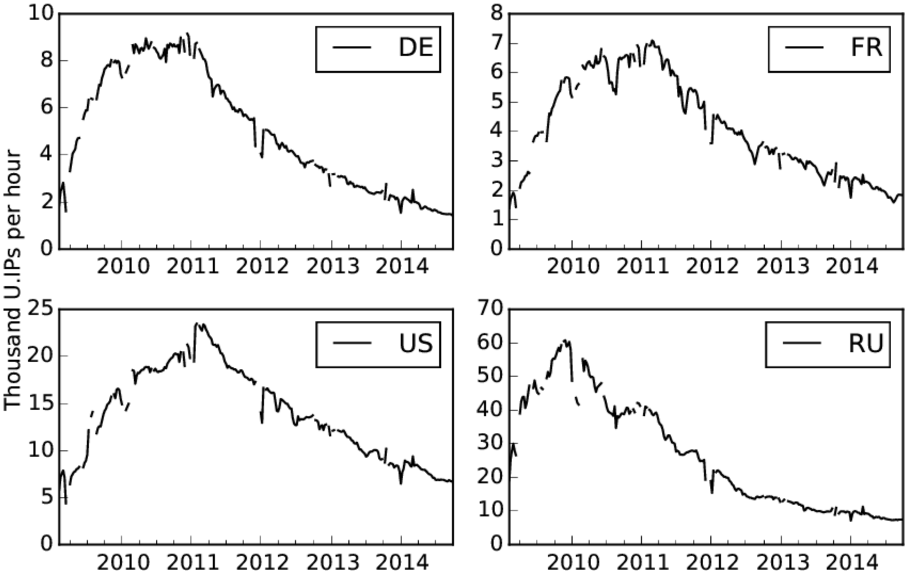


Figure 4.5. Conficker trends for four countries

Epidemic Models

It is often proposed in the security literature to model malware infections similarly as epidemics of infectious diseases (Pastor-Satorras et al. 2014, e.g., Zou, Gong, and Towsley 2002). The analog is that vulnerable hosts get infected, and start infecting other hosts in their vicinity; at some later point they are recovered or removed (cleaned, patched, upgraded or replaced).

This leads to multiple phases, similar to what we see for Conficker: in the beginning, each new infection increases the pressure on vulnerable hosts, leading to an explosive growth. Over time, fewer and fewer vulnerable hosts remain to be infected. This leads to a phase where the force of new infections and the force of recovery are locked in dynamic equilibrium. The size of the infected population reaches a plateau. In the final phase, the force of recovery takes over, and slowly the number of infections declines towards zero.

Early on in our modeling efforts we experimented with a number of epidemic models, but eventually decided against them. Epidemic models involve a set of latent compartments and a set of differential equations that govern the transitions between them—see Heesterbeek (2000) for an extensive overview. Most models make a number of assumptions about the underlying structure of the population and the propagation mechanism of the disease.

The basic models for instance assume constant transition rates over time. Such assumptions might hold to an acceptable degree in short time spans, but not over six years. The early works applying these models to the Code Red and Slammer worms (Zou, Gong, and Towsley 2002; Zou et al. 2003) used data spanning just a few weeks. One can still use the models even when the assumptions are not met, but the parameters cannot be then easily interpreted. To illustrate: the basic Kermack-McKendrick SIR model fits our data to a reasonable degree. However, we know that this model assumes no reinfections, while Conficker reinfections were a major problem for some companies (Microsoft 2012a).

More complex models reduce assumptions by adding additional latent variables. This creates a new problem: often when solved numerically, different combinations of the parameters fit the data equally well. We observed this for some countries with even the basic SIR model. Such estimates are not a problem when the aim is to predict an outbreak. But they are showstoppers when the aim is to compare and interpret the parameters and make inferences about policies.

Our Model

For the outlined reasons, we opted for a simple descriptive model. The model follows the characteristic trend of infection rates, provides just enough flexibility to capture the differences between countries, and makes no assumptions about the underlying behavior of Conficker. It merely describes the observed trends in a small set of parameters.

The model consists of two parts: a logistic growth that ends in a plateau; followed by an exponential decay. Logistic growth is a basic model of self-limiting population growth, where first the rate of growth is proportional to the size of the existing population, and then declines as the natural limit is approached (—the seminal work of Staniford et al. (2002) also used logistic growth). In our case, this natural limit is the number of vulnerable hosts.

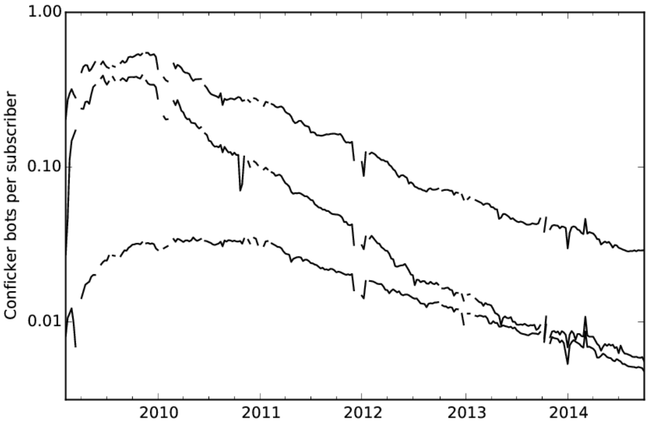


Figure 4.6. Conficker bots per sub. on log-scale for (top to bottom) Russia, Belarus, and Germany

Exponential decay corresponds to a daily decrease of the number of Conficker bots by a fixed percentage. Figure 4.6 shows the number of infections per subscriber over time for three countries on a logarithm scale. We see a downward-sloping straight line in the last phase that corresponds to an exponential decay: the botnet shrank by a more or less a constant percentage each day. We do not claim that the assumptions underpinning the logistic growth and the exponential decay models are fully satisfied, but in the absence of knowledge of the exact dynamics, their simplicity seems the most reasonable approach.

The model allows us to reduce the time series data for each country to these parameters: (1) the infection rate in the growth phase, (2) the peak number of infections, (3) the time at which this peak occurred, and (4) the exponential decay rate in the declining phase. We will fit our model on the time series for all countries, and then compare the estimates of these parameters.

Mathematically, our model is formulated as follows:

$$bots(t) = \begin{cases} \dfrac{K}{1 + e^{-r(t-t_0)}}, & if\ t < t_P \\ He^{-\gamma(t-t_P)}, & if\ t \geq\ t_P \end{cases}$$

where *bots*(t) is the number of bots at time t, t_P is the time of the peak (where the logistic growth transitions to exponential decay), and H the height of the peak. The logistic growth phase has growth rate r, asymptote K, and midpoint t_0. The parameter γ is the exponential decay rate. The height of the peak is identified by the other parameters:

$$H = \frac{K}{1 + e^{-r(t_P - t_0)}}$$

Inspection of Model Fit

We fit the curves using the Levenberg-Marquardt least squares algorithm with the aid of the *lmfit* Python module. The results are point estimates; standard errors were computed by *lmfit* by approximating the Hessian matrix at the point estimates. With these standard errors, we computed Wald-type confidence intervals (point estimate ± 2 s.e.) for all parameters. These intervals have no exact interpretation in this case, but provide some idea of the precision of the point estimates.

The reader can find plots of the fitted curves for all 62 countries at the end of the chapter (Figure 4.12 and Figure 4.13). The fits are good, with R-square values all between 0.95 and 1. Our model is especially effective for countries with sharp peaks, that is, the abrupt transitions from growth to decay that can be seen in Hungary and South Africa, for example. For some countries, such as Pakistan and Ukraine, we have very little data on the growth phase, as they reached their peak infection rate around the time sinkholing started. For these countries, we will ignore the growth estimates in further analysis. By virtue of our two-phase model, the estimates of the decay rates are unaffected by this issue. We note that our model is deterministic rather than stochastic; that is, it does not account for one-time shocks in cleanup that lead to a lasting drop in infection rates. Nevertheless, we see that the data follows the fitted exponential decay curves quite closely, which indicates that bots get cleaned up at a constant rate and non-simultaneously.[6]

Alternative Models. We tried fitting models from epidemiology (e.g. the SIR model) and reliability engineering (e.g. the Weibull curve), but they did not do well in such cases, and adjusted R-square values were lower

[6] The exception is China: near the end of 2010, we see a massive drop in Conficker infections. After some investigation, we found clues that this drop might be associated by a sudden spur in the adoption of IPv6 addresses, which are not directly observable to the sinkhole.

for almost all countries. Additionally, for a number of countries, the parameter estimates were unstable. Figure 4.7 illustrates why: our model's two phases capture the peak and exponential decay more accurately.

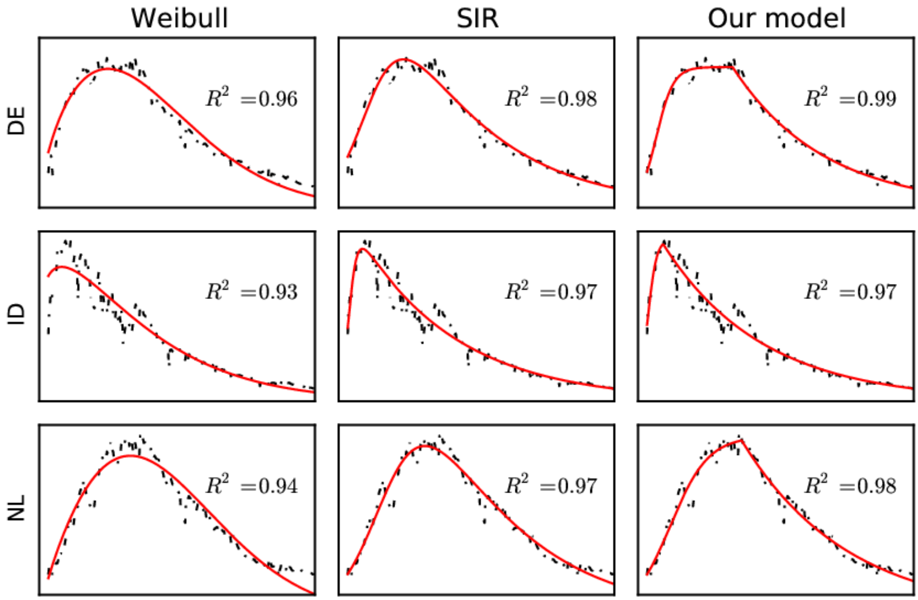


Figure 4.7. Comparison of alternative models

4.5 Findings

Country Parameter Estimates

Figure 4.8 shows the parameter estimates and their precision for each of the 62 countries: the growth rate, peak height, time of the peak, and the decay rate.

The variance in the peak number of infections is striking: between as little as 0.01% to over 1% of Internet broadband subscribers. The median is .1%. It appears that countries with high peaks tend to also have high growth rates, though we have to keep in mind that the growth rate estimates are less precise, because the data does not fully cover that phase. Looking at the peak height, it seems that this is not associated with low cleanup rates. For example, Belarus (BY) has the highest decay rate, but a peak height well above the median.

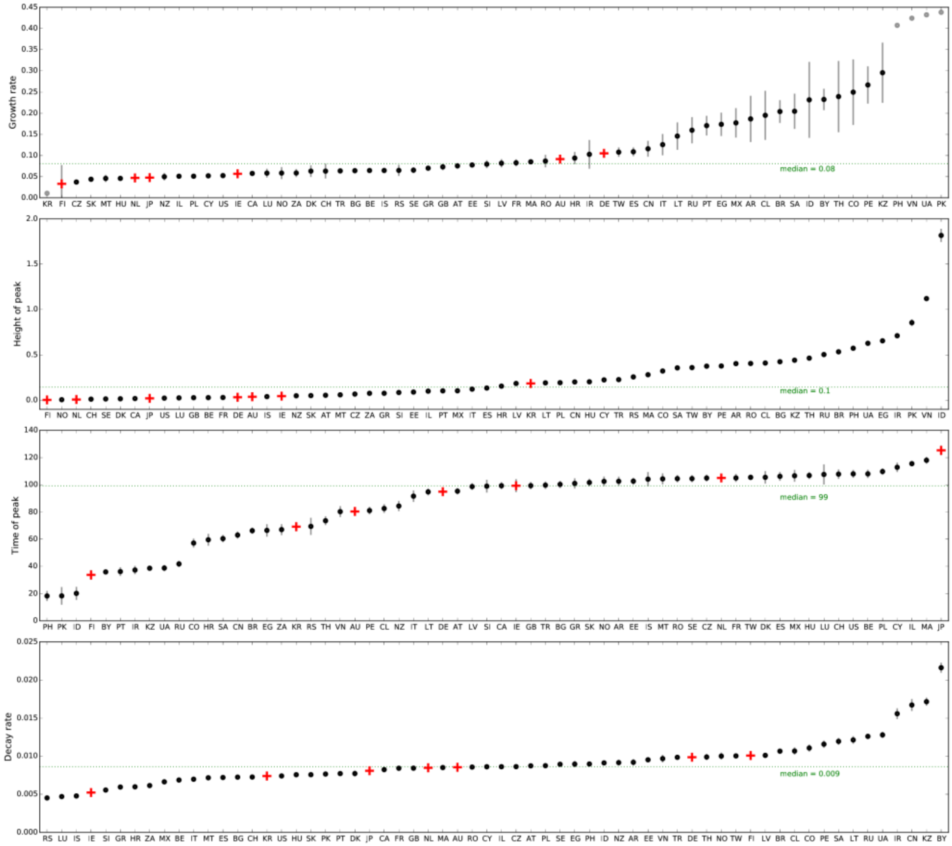


Figure 4.8. Parameter estimates and confidence intervals

The timing of the peaks is distributed around the last weeks of 2010. Countries with earlier peaks are mostly countries with higher growth rates. This suggests that the time of the peak is simply a matter of when Conficker ran out of vulnerable machines to infect; a faster growth means this happens sooner. Hence, it seems unlikely that early peaks indicate successful remediation.

The median decay rate estimate is .009, which corresponds to a 37% decline per year $(100 \cdot (1 - e^{-.009 \cdot 52}))$. In countries with low decay rates (around .005), the botnet shrank by 23% per year, versus over 50% per year on the high end.

National Anti-Botnet Initiatives

We are now in a position to address the paper's central question and to explore the effects of the leading national anti-botnet initiatives (ABIs).

In Figure 4.8, we have highlighted the countries with such initiatives as crosses. One would expect that these countries have slower botnet growth, a lower peak height, and especially a faster cleanup rate. There is no clear evidence for any of this; the countries with ABIs are all over the place. We do see some clustering on the lower end of the peak height graphs; however, this position is shared with a number of other countries that are institutionally similar (in terms of wealth for example) but not running such initiatives.

We can formally test if the population median is equal for the two groups using the Wilcoxon ranksum test. The p-value of the test when comparing the Conficker decay rate among the two sets of countries is 0.54, which is too large to conclude that the ABIs had a meaningful effect. It is somewhat surprising, and disappointing, to see no evidence for the impact of the leading remediation efforts on bot cleanup.

We briefly look at three possible explanations. The first one is that country trends might be driven by infections in other networks than those of the ISPs, as we know that the ABIs focus mostly on ISPs. This explanation fails, however, as can be seen in Table 4.2. The majority of the Conficker bots were located in the networks of the retail ISPs in these countries, compared to educational, corporate, or governmental networks. This pattern held in 2010, the year of peak infections, and 2013, the decay phase, with one minor deviation: in the Netherlands, cleanup in ISP networks was faster than in other networks.

A second explanation might be that the ABIs did not include Conficker in their notification and cleanup efforts. In two countries, Germany and the Netherlands, we were able to contact participants of the ABI. They claimed that Conficker sinkhole feeds were included and sent to the ISPs. Perhaps the ISPs did not act on the data—or at least not at a scale that would impact the decay rate; they might have judged Conficker infections to be of low risk, since the botnet had been neutralized. This explanation might be correct, but it also reinforces our earlier conclusion that the ABIs did not have a significant impact. After all, this explanation implies that the ABIs have failed to get the ISPs and their customers to undertake cleanup at a larger scale.

Table 4.2. Conficker bots located in retail ISPs

Country	ISP % 2010	ISP % 2013
AU	77%	74%
DE	89%	82%
FI	73%	69%
IE	72%	74%
JP	64%	67%
KR	83%	87%
NL	72%	37%
Others	81%	75%

Given that cleanup incurs cost for the ISP, one could understand that they might decide to ignore sinkholed and neutralized botnets. On closer inspection, this decision seems misguided, however. If a machine is infected with Conficker, it means it is in a vulnerable—and perhaps infected—state for other malware as well. Since we had access to the global logs of the sinkhole for GameoverZeus—a more recent and serious threat—we ran a cross comparison of the two botnet populations. We found that based on common IP addresses, a surprising 15% of all GameoverZeus bots are also infected with Conficker. During six weeks at the end of 2014, the GameoverZeus sinkhole saw close to 1.9 million unique IP addresses; the Conficker sinkhole saw 12 million unique IP addresses; around 284 thousand addresses appear in both lists. Given that both malware types only infected a small percentage of the total population of broadband subscribers, this overlap is surprisingly large.[7] It stands in stark contrast to the findings of a recent study that systematically determined the overlap among 85 blacklists and found that most entries were unique to one list, and that overlap between independent lists was typically less than one percent (Metcalf and Spring 2014). In other words, Conficker bots should be considered worthwhile targets for cleanup.

Institutional Factors

Given that anti-botnet initiatives cannot explain the variation among the country parameters shown in Figure 4.8, we turn our attention to several national factors, external to the ISP, that are often associated with mal-

[7] The calculated overlap in terms of bots might be inflated as a result of both NAT and DHCP churn. Churn can in this case have both an over-counting and under-counting effect. Under-counting will occur if one bot appears in the two sinkholes with different IP addresses, as a result of different connection times to the sinkholes. Doing the IP comparisons at a daily level yields a 6% overlap, which is still considerable.

ware infection rates (e.g., see Van Eeten et al. 2010). These are broadband access, unlicensed software use, and ICT development on a national level. In addition, given the spreading mechanism of Conficker, we also look at Operating System market shares, as well as PC upgrade cycles. We correlate these factors with the relevant parameters.

Growth Rate and Broadband Access. Broadband access is often mentioned as a technological enabler of malware; in particular, since Conficker was a worm that spread initially by scanning for hosts to infect, one could expect its growth in countries with higher broadband speeds to be faster. Holding other factors constant, most epidemiological models would also predict this faster growth with increased network speeds. This turns out not to be the case. The Spearman correlation coefficient between average national broadband speeds, as reported by the International Telecommunication Union (http://www.itu.int/en/ITU-D/Statistics), and Conficker growth rate is in fact negative: -0.30. This is most probably due to other factors confounding with higher broadband speeds, e.g. national wealth. In any case, the effects of broadband access and speeds are negligible compared to other factors, and we will not pursue this further.

Height of Peak and Operating System Market Shares. Since Conficker only infects machines running Windows 2000, XP, Vista, or Server 2003/2008, some variation in peak height may be explained by differences in use of these operating systems (versus Windows 7 or non-Windows systems). We use data from StatCounter Global Stats (http://statcounter.org), which is based on page view analytics of some three million websites. Figure 4.9 shows the peak height against the combined Windows XP and Vista market shares in January 2010 (other vulnerable OS versions were negligible). We see a strong correlation—with a Pearson correlation coefficient of 0.55. This in itself is perhaps not surprising.

Dividing the peak heights by the XP/Vista market shares gives us estimates of the *peak number of infections per vulnerable user*; we shall call this metric *hp*. This metric allows for fairer comparisons between countries, as one would expect countries with higher market shares of vulnerable OS's to harbor more infections regardless of other factors. Interestingly, there is still considerable variation in this metric – the coefficient of variance is 1.2. We investigate two institutional factors that may explain this variation.

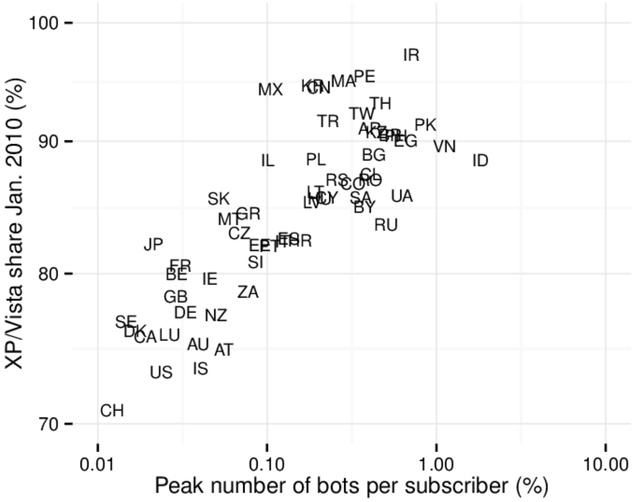


Figure 4.9. Bots versus XP & Vista use

Height of Peak and ICT Development Index. This an index published by the ITU based on a number of well-established ICT indicators. It allows for benchmarking and measuring the digital divide and ICT development among countries—based on ICT readiness and infrastructure, ICT intensity and use, ICT skills and literacy (http://www.itu.int/en/ITU-D/Statistic). This is obviously a broad indicator, and can indicate the ability to manage cybersecurity risks, including botnet cleanups, among both citizens and firms. Figure 4.10 shows this metric against *hp*, and interestingly enough we see a strong correlation.

Height of Peak and Unlicensed Software Use. Unlicensed software use or piracy rates are another oft-mentioned factor influencing malware infection rates. In addition to the fact that pirated software might include malware itself, users running pirated OS's often turn off automatic updates, for fear of updates disabling their unlicensed software—even though Microsoft consistently states that it will also ship security updates to unlicensed versions of Windows (Yam 2009). Disabling automatic updates leaves a machine open to vulnerabilities, and stops automated cleanups. We use the unlicensed software rates calculated by the Software Alliance (http://globalstudy.bsa.org/2013/). This factor also turns out to be strongly correlated with *hp*, as shown in Figure 4.10.

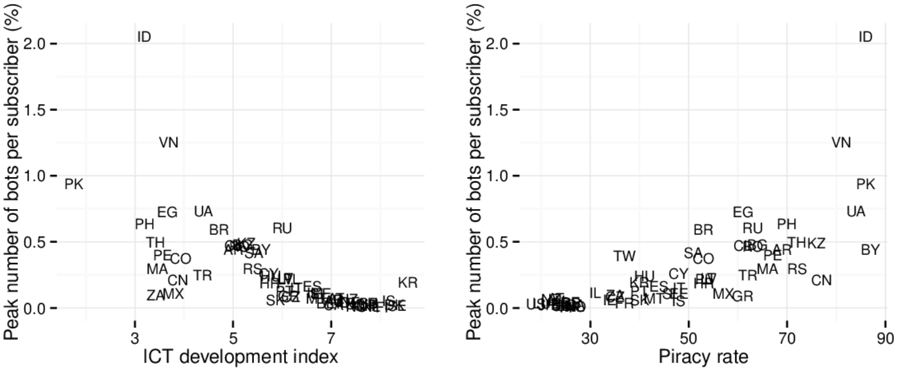


Figure 4.10. Height of peak versus ICT development & piracy

Since ICT development and piracy rates are themselves correlated, we use the following simple linear regression to explore their joint association with peak Conficker infection rates:

$$\log(hp) = \alpha + \beta_1 \cdot ictdev + \beta_2 \cdot piracy + \varepsilon$$

where both regressors were standardized by subtracting the mean and dividing by two standard deviations. We use the logarithm of *hp* as it is a proportion. The least squares estimates (standard errors) are $\hat{\beta}_1 = -0.78\ (0.27), p < 0.01$, and $\hat{\beta}_2 = 1.7\ (0.27), p < 0.001$. These coefficients can be interpreted as follows: everything else kept equal, countries with low (one sd below the mean) ICT development have $e^{0.78} = 2.2$ times more Conficker bots per XP/Vista user at the peak than countries with high ICT development (one sd above the mean), and, similarly, countries with high piracy rates (one sd above the mean) have an $e^{1.7} = 5.5$ times higher peak than countries with low piracy rates (one sd below the mean). The R^2 of this regression is 0.78, which indicates that ICT development and piracy rates explain most of the variation in Conficker peak height.

Decay Rate and Market Share of Windows XP/Vista. Although decay rates are less dispersed than peak heights, there are still noticeable differences among countries. Given the rather slow cleanup rates—the median of 0.009 translates to a 37% decrease in the number of bots after one year—one hypothesis that comes to mind is that perhaps some of the cleanup is being driven by users upgrading their OS's (to say Windows 7), or buying a new computer and disposing of the old fully. For each country, we estimated the *decay rate of the market share of Windows XP* *and Vista* from January 2011 to June 2013 using the StatCounter GlobalStats data. Figure 4.11 shows these decay rates versus Conficker decay rates. There is a weak correlation among the two, with a Spearman correlation coefficient of 0.26.

But more interesting and somewhat surprising is that in many countries, the Conficker botnet shrank at a slower pace than the market share of Windows XP / Vista (all countries below and to the right of the dashed line). Basically, this means that the users infected with Conficker are less likely to upgrade their computers then the average consumer.[8]

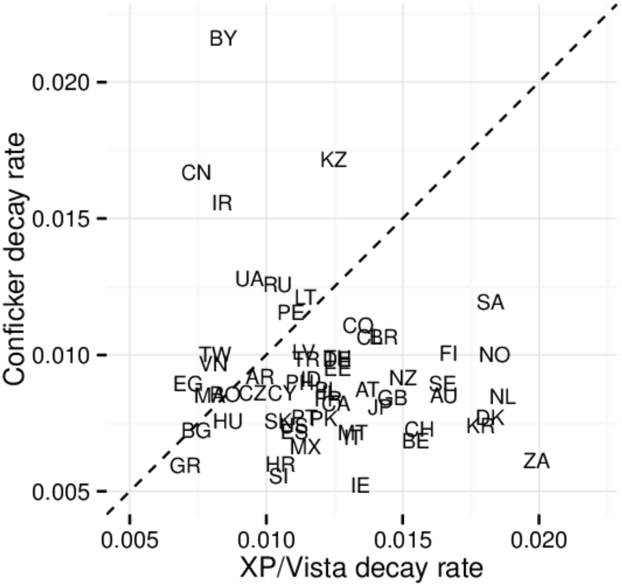


Figure 4.11. Conficker decay vs. XP/Vista decay

4.6 Discussion

We found that the large-scale national anti-botnet initiatives had no observable impact on the growth, peak height, or decay of the Conficker botnet. This is surprising and unfortunate, as one would expect Conficker bots to be among those targeted for cleanup by such initiatives. We

[8] This difference between users who remain infected with Conficker and the average user might be more extreme in countries with a higher level of ICT development. This can be observed in the graph.

checked that the majority of bots were indeed located among the networks of ISPs, and also observed that some of these machines have multiple infections. Turning away from the initiatives and to other factors that could explain the differences among countries, we observed that the ICT development index and piracy rates can explain 78% of the variation in peak height, even after correcting for OS market shares. We also found that the Conficker cleanup rate is less than the average PC upgrade rate.

Perhaps not all security experts are surprised by these findings. They are nevertheless important in forming effective anti-botnet policies. We presented the research to an audience of industry practitioners active in botnet cleanup. Two North American ISPs commented that they informed their customers about Conficker infections—as part of the ISP's own policy, not a country-level initiative. They stated that some customers repeatedly ignored notifications, while others got re-infected soon after cleanup. Another difficulty was licensing issues requiring ISPs to point users to a variety of cleanup tool websites (e.g. on microsoft.com) instead of directly distributing a tool, which complicates the process for some users. Interestingly enough both ISPs ranked well with regards to Conficker peak, showing that their efforts did have a positive impact. Their challenges suggests areas for improvement.

Future Work. Can take several directions. One is to test the various parameters against other independent variables—e.g. the number of CERTs, privacy regulation, and other governance indicators. A second avenue is to explore Conficker infection rates at the ISP level versus the country level. A random-effects regression could reveal to what extent ISPs in the same country follow similar patterns. We might see whether particular ISPs differ widely from their country baseline, which would be interesting from an anti-botnet perspective. Third, it might be fruitful to contact a number of users still infected with Conficker in a qualitative survey, to see why they remain unaware or unworried about running infected machines. This can help develop new mitigation strategies for the most vulnerable part of the population. Perhaps some infections are forgotten embedded systems, not end users. Forth and more broadly is to conduct research on the challenges identified by the ISPs: notification mechanisms and simplifying cleanup.

4.7 Conclusion

In this paper, we tackled the often-ignored side of botnet mitigation: large-scale cleanup efforts. We explored the impact of the emerging best practice of setting up national anti-botnet initiatives with ISPs. Did these initiatives accelerate cleanup?

The longitudinal data from the Conficker botnet provided us with a unique opportunity to explore this question. We proposed a systematic approach to transform noisy sinkhole data into comparative infection metrics and normalized estimates of cleanup rates. After removing outliers, and by using the hourly Conficker IP address count per subscriber to compensate for a variety of known measurement issues, we modeled the infection trends using a two-part model. We thereby condensed the dataset to three key parameters for each country, and compared the growth, peak, and decay of Conficker, which we compared across countries.

The main findings were that institutional factors such as ICT development and unlicensed software use have influenced the spread and cleanup of Conficker more than the leading large-scale anti-botnet initiatives. Cleanup seems even slower than the replacement of machines running Windows XP, and thus infected users appear outside the reach of remediation practices. At first glance, these findings seem rather gloomy. The Conficker Working Group, a collective effort against botnets, had noted remediation to be their largest failure (Rendon Group 2011). We have now found that the most promising emerging practice to overcome that failure suffers similar problems.

So what can be done? Our findings lead us to identify several implications. First of all, the fact that peak infection levels strongly correlate with ICT development and software piracy, suggests that botnet mitigation can go hand in hand with economic development and capacity building. Helping countries develop their ICT capabilities can lower the global impact of infections over the long run. In addition, the strong correlation with software piracy suggests that automatic updates and unattended cleanups are some of the strongest tools in our arsenal. It support policies to enable security updates to install by default, and delivering them to all machines, including those running unlicensed copies (R. Anderson et al. 2008). Some of these points were also echoed by the ISPs mentioned in section 4.6 .

Second, the fact that long-living bots appear in a reliable dataset—that is, one with few false positives—suggests that future anti-botnet initiatives need to commit ISPs to take action on such data sources, even if the sinkholed botnet is no longer a direct threat. These machines are vulnerable and likely to harbor other threats as well. Tracking these infections will be an important way to measure ISP compliance with these commitments, as well as incentivize cleanup for those users outside the reach of automated cleanup tools.

Third, given that cleanup is a long-term effort, future anti-botnet initiatives should support, and perhaps fund, the long-term sustainability of sinkholes. This is a necessity if we want ISPs to act on this data.

A long-term view is rare in the area of cybersecurity, which tends to focus on the most recent advances and threats. In contrast to C&C takedown, bot remediation needs the mindset of a marathon runner, not a sprinter. To conclude on a more optimistic note, Finland has been in the marathon for a longer time than all other countries. It pays off: they have been enjoying consistently low infection rates for years now. In other words, a long-term view is not only needed, but possible.

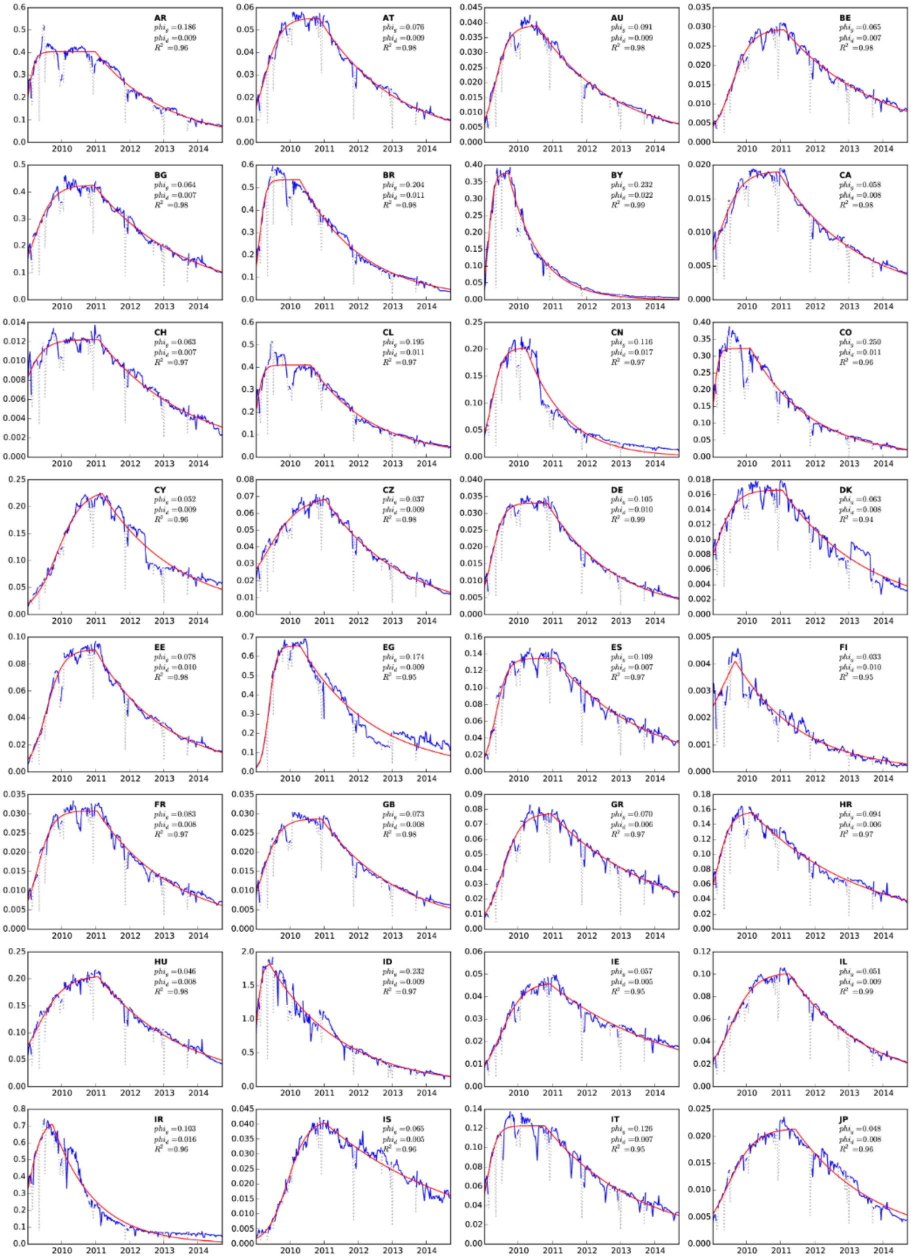


Figure 4.12. Conficker trend and model fit for countries (AR to JP)

Trends of relative Conficker bots (unique Conficker IP addresses per hour divided by broadband subscribers). Solid (blue) indicates measurement; dotted (gray) removed-outliers; smooth-solid (red) fitted-model. The model growth and decay parameters are given on the graph; height and time of peak infections are deducible from the axes.

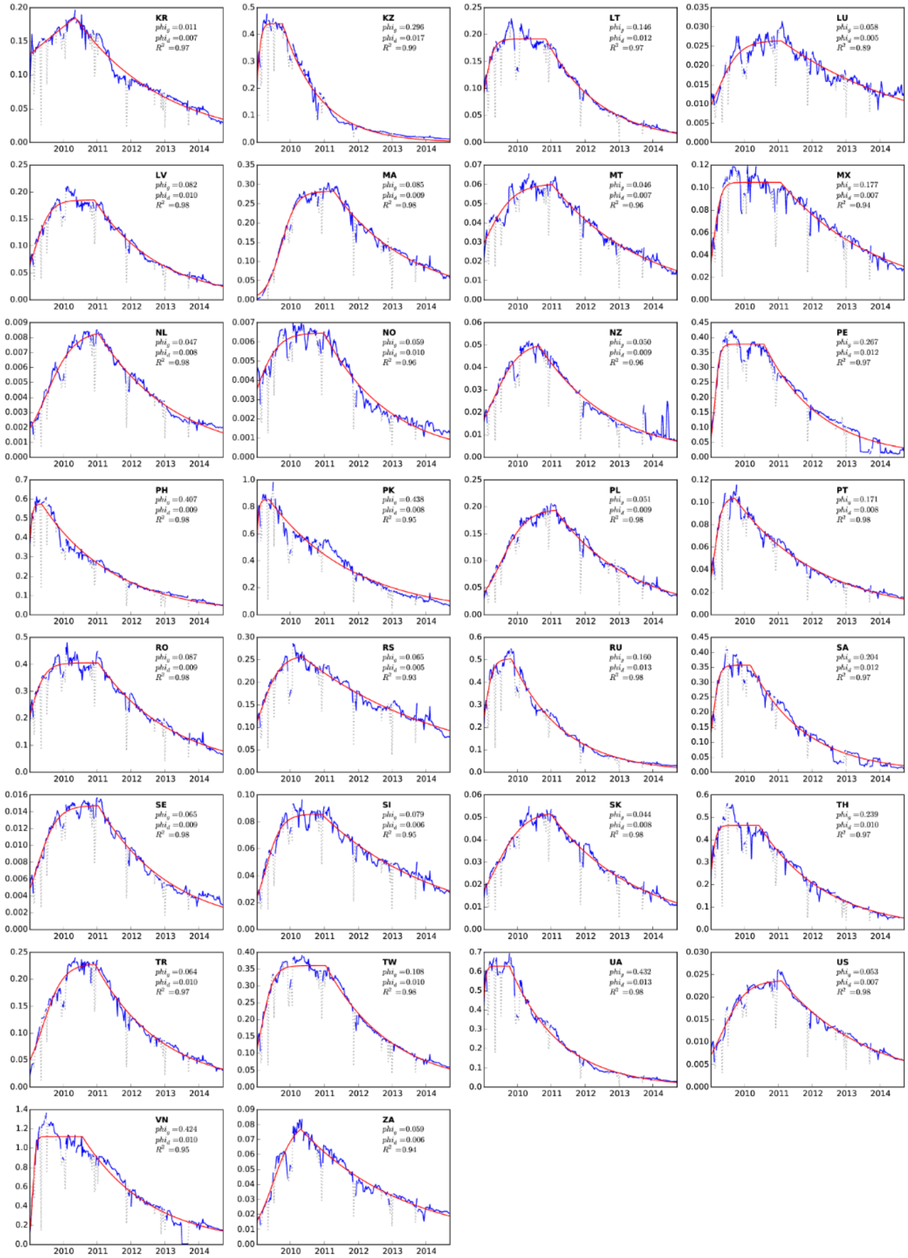


Figure 4.13. Conficker trend and model fit for countries (KR to ZA)

Chapter 5:Security Economics of Certificate Authorities[1]

5.1 Introduction

HTTPS (Hypertext Transfer Protocol Secure) has evolved into the de facto standard for secure Web browsing. Through the certificate-based authentication protocol, Web services and Internet users first authenticate one another ("shake hands") using a TLS/SSL certificate, encrypt Web communications end-to-end, and show a padlock in the browser to signal that a communication is secure. In recent years, HTTPS has become an essential technology to protect social, political, and economic activities online.

At the same time, widely reported security incidents—such as DigiNotar's breach, Apple's #gotofail, and OpenSSL's Heartbleed—have exposed systemic security vulnerabilities of HTTPS to a global audience. The Edward Snowden revelations—notably around operation BULLRUN,

[1] Parts of this chapter have been published as: Arnbak, Axel, Hadi Asghari, Michel J.G. van Eeten, Nico van Eijk. 2014. "Security Collapse in the HTTPS Market". *Communications of the ACM*, 57 (10): 47-55. © 2014 Association for Computing Machinery, Inc. Reprinted by permission. doi:10.1145/2660574.

Sections 5.3, 5.4, and 5.5 of the chapter have been extended with parts of an earlier work: Asghari, Hadi, Michel J.G. van Eeten, Axel Arnbak, Nico Van Eijk. 2013. "Security Economics in the HTTPS Value Chain". Paper presented at the 12th Workshop for the Economics of Information Security, June 11-13, Washington, DC. doi:10.2139/ssrn.2277806.

Acknowledgements. For inspiration and comments, the authors would like to thank: Bernhard Amann, Ian Brown, Peter Eckersley, Edward Felten, Sharon Goldberg, Joris van Hoboken, Ralph Holz, Chris Hoofnagle, Kees Keuzenkamp, Samad Khatibi, Arman Noroozian, Bruce Schneier, Stephen Schultze, Christopher Soghoian, Sid Stamm, Marcelo Thompson, and participants of TPRC 2012, WEIS 2013, two workshops at the Berkman Center in Spring 2014, 29c3, a UC Berkeley TRUST Seminar Jan. 2013, and an HKU Law & Tech Talk, Feb. 2013. The authors are solely responsible for this article.

MUSCULAR, and the lesser-known FLYING PIG program to query certificate metadata on a dragnet scale—have driven the point home that HTTPS is both a major target of government hacking and eavesdropping, as well as an effective measure against dragnet content surveillance when Internet traffic traverses global networks. HTTPS, in short, is an absolutely critical but fundamentally flawed cybersecurity technology.

While the Heartbleed incident illuminated severe flaws in a widely used crypto-library of HTTPS (OpenSSL), the focus here is on the systemic security vulnerabilities in the HTTPS authentication model that precedes end-to-end encryption. Although some of these vulnerabilities have been known for years, the 2011 security breach at the small Dutch CA (certificate authority) known as DigiNotar was a watershed moment, demonstrating these theoretical man-in-the-middle vulnerabilities in the wild. Meanwhile, large CAs such as Comodo and Verisign have experienced breaches as well but didn't suffer similar consequences as DigiNotar. In fact, some large CAs actually *benefited* from the increased sense of HTTPS insecurity.

Policymakers and technologists are increasingly advocating various solutions to address the security collapse of HTTPS. The European Union is halfway through adopting the first comprehensive legislation on HTTPS in the world. It will acquire immediate binding force in the legal systems of 28 European member states. As most large CAs operate (also) under E.U. jurisdiction, the legislation will impact HTTPS governance globally. In the U.S., on the other hand, attention has focused on technological solutions and industry self-regulation.

To evaluate both legal and technological solutions, an understanding of the economic incentives of the stakeholders in the HTTPS ecosystem, most notably the CAs, is essential. This article outlines the systemic vulnerabilities of HTTPS, maps the thriving market for certificates, and analyzes the suggested regulatory and technological solutions on both sides of the Atlantic. The findings show existing yet surprising market patterns and perverse incentives: not unlike the financial sector, the HTTPS market is full of information asymmetries and negative externalities, as a handful of CAs dominate the market and have become "too big to fail." Unfortunately, the proposed E.U. legislation will reinforce systemic vulnerabilities, and the proposed technological solutions are far from being adopted at scale. The systemic vulnerabilities in this crucial technology are likely to persist for years to come.

5.2 Systemic Vulnerabilities in the HTTPS Model

Essentially, HTTPS is a two-step process. First, a trust relationship (a handshake) is established between a Web site and an end user's browser. This is done with the help of a TLS/SSL (Transport Layer Security/Secure Sockets Layer) certificate containing basic information for authentication purposes. If the Web browser trusts the certificate and the issuing CA, then this authentication handshake succeeds. Second, successful authentication leads to a TLS/SSL-encrypted channel between the Web site and browser, called a *tunnel* (R. Anderson 2008, 670)*.* Thus, the handshake authentication serves as the stepping-stone for the confidentiality and integrity that HTTPS seeks to deliver. If the handshake succeeds, then the browser informs the user by, for example, depicting a padlock or a green address bar. If the TLS/SSL certificate or the issuing CA cannot be trusted, then the browser will show a security warning to the end user. The described data flows are shown in Figure 5.1.

A Web site that wants to provide HTTPS communications to users, needs to obtain a TLS/SSL certificate from a CA. Basically, these certificates are small computer files that contain information on hostname (Web site), certificate owner (Web-site owner), certificate issuer (CA), validity period, and public key (R. Anderson 2008, 672). The method for verification of the identity of a Web-site owner, among others, drives the costs of a certificate and is the key difference between DV (domain validated), OV (organization validated), and EV (extended validation) certificates (Arnbak and Van Eijk 2012, sec. 2).

The Stakeholders

The HTTPS market involves four central stakeholders, as depicted in figure 1: Web-site owners; certificate authorities; Web browsers; and end users.

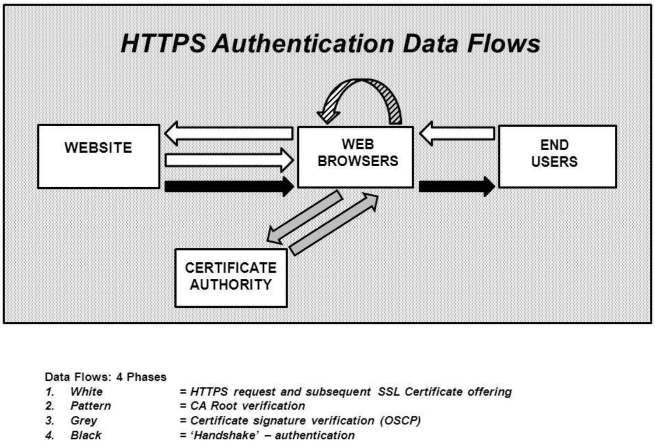

HTTPS Authentication Data Flows
WEBSITE
WEB BROWSERS
END USERS
CERTIFICATE AUTHORITY
Data Flows: 4 Phases
1. White = HTTPS request and subsequent SSL Certificate offering
2. Pattern = CA Root verification
3. Grey = Certificate signature verification (OSCP)
4. Black = 'Handshake' – authentication

Figure 5.1. HTTPS authentication data flows

Web-Site Owners. Web-site owners decide whether to deploy HTTPS or not, and how securely to implement it on their servers. Deployment is a binary affair from the point of view of the end user. An outdated implementation, as long as the browser accepts it, appears similar to the state-of-the-art implementation. If embedded content from third-party Web sites (e.g. behavioral tracking across Web sites for advertising) is a part of the revenue model of a Web-site owner, then that operator has a strong incentive not to deploy HTTPS at all. Both deployment and secure implementation vary widely (Trustworthy Internet Movement 2014).

Certificate Authorities. CAs sell TLS/SSL certificates, which come in three categories: root, intermediate/subordinate, and untrusted. *Root CAs* are trusted by default by browsers, after they have solicited for such a status with the browsers and complied with the varying browser CA trust policies. *Intermediate/Subordinate CAs* are either directly verified by one root CA or they are part of a chain of trust of several intermediate CAs that ultimately ends with one root CA. Certificates of *untrusted CAs* are not issued by a CA linked to a root CA but are mostly self-signed by the owner of a Web site. Self-signed certificates evoke the "untrusted connection" security warning when served by a Web site to browsers. CAs are owned by such varying entities as multinational corporations, nation-states, universities, and hacker communities—anyone can start a CA operation relatively easily.

Web-Browser Vendors. These vendors play a key role in the HTTPS ecosystem. For example, they decide whether to trust a CA inherently, how to respond to a (suspected) CA compromise, and how to implement related trust revocation protocols such as the OCSP (Online Certificate Status Protocol). Over the years, various browser have developed different certificate policies, leading to varying numbers of root and intermediate CAs inherently trusted per browser (Asghari et al. 2013; Durumeric et al. 2013).

End Users. Because their communications and valuable information are on the line, end users have an interest in seeking HTTPS communications with Web sites, but they depend to a large degree on security decisions made by the other stakeholders and can exert very little control over HTTPS (Bakos, Marotta-Wurgler, and Trossen 2009; ENISA 2011).

Known CA Breaches

DigiNotar. On Friday, September 2, 2011, a nocturnal press conference of the Dutch Minister of Internal Affairs marked the beginning of the DigiNotar affair. It was triggered by unauthorized access, reportedly by a hacker sympathizing with the government of Iran in mid-July 2011, to the root CA capacity of DigiNotar. When the breach became public three months later, it emerged that in this long period of obscurity 531 false certificates had been created for widely used and highly sensitive domain names such as *.google.com, *.facebook.com, update.windows.com, and *.cia.gov (Prins 2011). A small player in the global market with a strong presence in the niche for Dutch e-government services, DigiNotar had root status with all major browser vendors, leading those browsers to trust, by default, corrupt certificates for months.

According to the forensic report, 30 critical updates had not been performed, logging was insufficient, and no antivirus protection was in place at the time of the intrusion (Fox-IT 2012). The damage was probably enormous but cannot be determined with certainty because of the unreliability of the log files. ENISA (European Network and Information Security Agency) speaks of breached communications of "millions of citizens," particularly connected to the *.google.com certificate, and notes that some experts believe that the lives of Iranian activists have been put at risk (ENISA 2011). Upon publication of the breach, the trust in the entire range of DigiNotar activities was revoked by all the major browsers.

Comodo. The range of breaches at market-leading CA Comodo also received considerable media attention, notably the breach affecting its 'UTN-USERFirst-Hardware' certificate (InfoSecurity 2011).[2] According to the EFF (Electronic Frontier Foundation) SSL Observatory, 85,440 public HTTPS certificates were signed directly by UTN-USERFirst-Hardware, and indirectly, the certificate had delegated authority to 50 more intermediate CAs (Eckersley 2011).

Verisign. Another dominant CA, Verisign, was hacked in 2010. The breach was not discovered until February 2012, after new SEC (Security and Exchange Commission) regulations mandated companies to notify investors of intrusions. In reporting its discovery, news agency Reuters quoted a former CTO who said Verisign "probably can't draw an accurate assessment" of the damage, given the time elapsed since the attack and the vague language in the SEC filing (Menn 2012).

Trustwave. Trustwave used its root CA status to enable third parties to issue SSL server certificates for the purpose of monitoring employees. While providing man-in-the-middle capabilities to private entities via sub-CAs does not technically breach the HTTPS trust model, it undermines it. This is especially true when end users are not informed of the monitoring. Trustwave claims that this is common practice among root CAs (Constantin 2012). This illustrates the "compelled-CA attack" in real life: CAs are in a unique position to enable surveillance of end users (Soghoian and Stamm 2012).

Roosa and Schultze (2010) report on several other breaches, including GlobalSign, KPN/Getronics, StartSSL, and TurkTRUST. From the known CA breaches, several patterns emerge.

Systemic Vulnerabilities of the HTTPS Authentication Model

The term *systemic vulnerabilities* refers to those vulnerabilities inherent in the HTTPS ecosystem, as opposed to incidental vulnerabilities that have occurred at a particular stakeholder during an isolated incident.

[2] This sentence has been slightly revised to make it factually correct. Originally it read, "The best documented breach was the compromise of Comodo's UTN-USERFirst-Hardware certificate". We were informed by Comodo (on May 6, 2015) that two Registration Authority accounts where compromised, not the CA certificate. This still allowed signing of fraudulent certificates, so the rest of the text reads correctly.

Many security experts agree that the security of the HTTPS authentication model and thus the HTTPS ecosystem is systemically flawed as a result of these vulnerabilities.

Weakest Link. A crucial technical property of the HTTPS authentication model is that any CA can sign certificates for any domain name. In other words, literally *anyone* can request a certificate for a Google domain at any CA anywhere in the world, even when Google itself has contracted one particular CA to sign its certificate. CAs have certain institutional limits to issuing certificates (e.g. validation procedures) but no technical ones. If this second google.com certificate is obtained from one of the hundreds of intermediate CAs that link to root CAs trusted by browsers, users will get the familiar HTTPS notification (signaling all is OK).

While this ability to sign for any domain name has spurred a flourishing global market for certificates, it has profound implications for the security of the HTTPS ecosystem, commonly referred to as the *weakest-link* problem: if one CA suffers a breach, the entire ecosystem is under attack (ENISA 2011; Roosa and Schultze 2010). The scenarios for failure are manifold, from CA compromise, misconfiguration, and malpractice to state compulsion (Soghoian and Stamm 2012).

Information Asymmetry and Ineffective Auditing Schemes. The recurring information asymmetries are a striking systemic vulnerability, making it very hard for other stakeholders to know about the security of CAs. The current regulatory regime in the E.U. and auditing obligations worldwide have proven ineffective. The qualified certificate practices of DigiNotar were regulated and passed the periodic audits based upon internationally recognized industry standards. The regulatory and auditing schemes deliver perceived security and enable liability dumping (Roosa and Schultze 2010).

Liability Dumping. Web sites, browsers, and CAs push damages from security breaches downstream toward end users. CAs, for example, disclaim all liability for losses suffered via inappropriately issued certificates (Roosa and Schultze 2010; Vratonjic et al. 2013). Because of the negative externalities at play, liability dumping is a common practice, and it is widely criticized for providing wrong incentives or actual security provision (Winn 2009). End users bear the burden of these security vulnerabilities and breaches, even though most users are probably unaware of this and cannot reasonably be held responsible for evaluating security practices in the HTTPS authentication model.

To understand these systemic flaws better, a thorough understanding of the market dynamics of HTTPS is essential. It is only in light of such data-driven findings that one can start to reflect on the need for legal and technical interventions in the current HTTPS ecosystem.

5.3 Methodology

The empirical part of this study builds primarily upon two datasets of all publicly observable SSL certificates, and a manually gathered dataset of market prices for the different offerings of certificate authorities. The two datasets are the EFF SSL Observatory (from 2010) and the University of Michigan's HTTPS ecosystem scans (from 2012-2014).

Publicly Visible SSL Certificates

The SSL Observatory (https://www.eff.org/observatory) is a project that investigates the certificates used to secure all of the sites encrypted with HTTPS on the Web. The Observatory scanned the full IPv4 address space for publicly visible webservers running HTTPS, over a course of several weeks. All certificates returned by these servers were saved along with some metadata. This amounts to 4-6 million certificates, out of which only a portion is considered as valid by browsers, i.e. has a valid certificate chain, is not expired, etc. After filtering out the invalid, the Observatory dataset provides approximately 1.5 million SSL certificates. The dataset is very comprehensive, but is rather old. The version we accessed was the final public release of December 2010.

From the SSL Observatory data, we generated a list of certificate authorities using several standard queries (e.g. looking at *basicConstraints* or the *issuer* field). This results in approximately 1,100 CAs. The self-signed CAs on this list were matched using fingerprints to the Microsoft Root Certificate Program list (Microsoft 2012b) and to the Mozilla source file (http://www.mozilla.org/projects/security/certs/included) that has the roots in it. The matching allows us map the CAs to the owning organization information kept by the root stores. (Several fingerprints were not found, typically for new or retired roots; in some of these cases, we made inferences using the subject field.) Next, we identified certificate types.

EV certificates can be determined via the existence of certain policy object identifiers (OIDs) in the *Certificate Policies* field. These object identifiers (OIDs) are extracted from the Chromium browser source file. Distinguishing between DV & OV certificates is tricky and can turn into art - we adapted the heuristic algorithm suggested by Hurst (2012). The gist of the algorithm is to see whether the certificate *subject* field contains data that can identify an organization, using city and state fields as extra hints. The determined types were crosschecked by looking at the percentage of DV/OV/EV certificates each CA had issued, as a majority of owners issue only one type of certificate per CA.

We explored other available datasets in February 2013, at the writing of the original paper, to no avail. Other datasets were either as old, less comprehensive or not open. This included the SSL Landscape project at TU München (https://pki.net.in.tum.de/node/8), the Berkeley ICSI Certificate Notary (http://notary.icsi.berkeley.edu/), the NetCraft SSL Survey (http://www.netcraft.com/internet-data-mining/ssl-survey/) which is a recognized industry report, and a few others. The SSL Landscape dated back to March 2011. The Certificate Notary was not readily accessible due to privacy considerations, except in a highly aggregated graph, which we used for triangulation: it is based on certificates in active use in US networks monitored by the project, and so it has less certificates than the Observatory's full scan. The list of CAs and roots matched to a large degree, but not perfectly, possibly because they are from different points in time. The NetCraft Survey is not free. We compared their summary graph with the SSL data, and the results were consistent (no large discrepancies could be noted).

When writing the updated paper in May 2014, Durumeric et al. (2013) of Michigan University had released their *HTTPS Ecosystem Scans* (https://scans.io/study/umich-https), which is constantly being updated. This dataset had approximately 3 million trusted certificates, and we used for comparison with the EFF data. The difference mostly reflects a linear growth pattern over time in the number of certificates in use on the Web, and to a limited extent improved scanning methodology. There is a difference of 400,000 certificates if the growth trend in the ecosystem scan data is extrapolated back in time to the EFF data-collection period. Despite these differences, the other patterns are consistent across both datasets.

Market Prices

A dataset was built that maps each CA to its market name, product offerings and prices. The starting point was generating a list of all CAs that had issued more than 500 certificates[3]. The majority of these are subordinate CAs, for which we used web search to determine the owners. In most cases, this was straightforward. In some instances, we had to make an educated guess based on the results of web searches on CA and owner names.

Current product and price information were taken from the owner's website. A number of these vendors do not provide prices, and some only on request. To illustrate: the website of *Secure Business Services* (http://www.securebusinessservices.com), which has 3000 certificates in the dataset, gives neither prices nor an option to request a quote. The contact telephone provided on the site does not work either. We have skipped such vendors, accounting together for 2% of the market.

To make prices comparable, we standardized them to the extent possible as follows: (i) US dollar prices are used if available; if not, we convert using current rates; (ii) VAT is added when explicitly excluded; (iii) we only include prices of certificates with a one year validity period; (iv) all discounts including multi-year, bulk, as well as various bundled offerings, are ignored; (v) reseller pricing is ignored. Most SSL vendors have partner programs and theirs resellers often set lower prices – in one case, down to a fourth (€49 versus €12). It is not possible to tell from the certificates which ones have been bought via a reseller, so we cannot factor this in.

We considered wildcard and UCC certificates separately, and given the three DV/OV/EV types, this yields in total eight price categories (single-domain DV, multi-domain DV, wildcard DV, single-domain OV, multi-domain OV, wildcard OV, single-domain EV and finally multi-domain EV certificates. EV certificates do not support wildcards). Different brands of a vendor are also considered separately when the certificates can be technically distinguished, e.g. Symantec/Verisign, Symantec/Thawte, Symantec/GeoTrust and Symantec/RapidSSL. In the end, 98% of the SSL

[3] A number of smaller well-known brands that had issued less than 500 certificates were also checked to generate some insight in the long tail of CAs.

certificates in the dataset are mapped to a brand and prices are available for 96% of the certificates.

Limitations. Three limitations need to be considered. The first is a matter of scope: our certificate datasets contain only certificates of publicly visible webservers. This fits with our analysis (focusing on HTTPS), and does not capture other use cases such as back-end systems and email certificates. One point of comparison comes from Verisign's annual report. In December 2009, they had a 1.2 million installed base of SSL certificates ('business authentication services'), and an unspecified number of 'user authentication services' certificates (Verisign 2010, 49). In the Observatory data, Verisign has approximately 663 thousand certificates, which is a significant proportion of all server certificates. The second limitation is the time mismatch between market shares and prices. Market shares were calculated from the Observatory data (December 2010), while prices gathered in February 2013. We had a brief look at historical prices using the Internet Archive (http://archive.org) where possible. The third limitation regards price accuracy. Resellers offer different prices; prices can also be lower due to discounts; or several times higher when charged extra for installing on multiple servers. We have aimed to standardize the prices as much as possible.

5.4 The Market for TLS/SSL Certificates

How Many Organizations Issue Certificates?

The question of how many organizations can issue certificates seems straightforward, but it has been the source of speculation and controversy. The X.509 standard specifics a structure composed of root certificate authorities, intermediate certificate authorities, and end entities (Cooper et al. 2005). Root CAs are trusted directly by the end applications; they typically certify intermediate CAs, also known as subordinate CAs, who in turn certify other intermediates or issue certificates for end entities. Browser and OS vendors have their own policies for determining which CAs to include in their root stores; such is the case with as those of Microsoft, Mozilla, and Apple (Apple 2013; Microsoft 2009; Mozilla 2013). Software can also use roots provided by the operating system.

In the Observatory data, we saw approximately 1,100 valid issuing CAs (the HTTPS Ecosystem Scans yields a higher number, closer to 2000 trusted CAs). A company or organization can own and operate multiple root and intermediate CAs – for operational reasons, redundancy, security, branding, or as a consequence of acquisitions.[4] We mapped root CAs to their owning entities by looking at the details provided on vendor root stores (who keep their lists up to date during audits); the result is shown Table 5.1. Microsoft supports more root CAs than Mozilla, especially among governmental owners. Determining the ownership of the intermediate CAs is more complicated, as a base list to compare against does not exist. A portion are owned by the root organizations; others are separate entities. We mapped this manually for all intermediate CAs that have at least 500 certificates in the dataset - 93 CAs were above the threshold. Searching the web, we connected these CA names to their owners and, in the case of firms with multiple brands, to each brand. Other CAs with similar names to these 93 were also identified, bringing the total mapped to 134. Finally, we separately tagged the 261 CA names from the DFN-Cert hierarchy.

Table 5.1. Microsoft & Mozilla root certs matched with Observatory

Root store	Root owners (organizations)	Percent governmental	Root CAs	CAs under hierarchy	Hierarchy level
Microsoft	116 (89 in dataset)	36%	333 (173 in dataset)	1096 in dataset	Median 1, Max 4
Mozilla	61 (56 in dataset)	20%	158 (130 in dataset)	907 in dataset	Median 1, Max 4

In summary, we can provide a reasonable estimate of the total number of organizations issuing certificates. There are over a hundred owners for the root CAs; intermediate CAs with the aforementioned criteria bring the total to 140. Our impression is that mapping the whole population of CAs using the Observatory data brings the total to somewhere between 200 and 300 trusted certificate-issuing organizations, located in 54 countries[5]. Using the HTTPS Ecosystem Scans, leads to an estimated 250 to 700 trusted certificate-issuing organizations, located in 57 countries worldwide.

[4] One interesting case is the DFN-PKI scheme, used by the academic network in Germany. In this scheme, each institution has its own signing CA, yielding more than 250 subordinate CAs. The private key for all of them is kept centrally at DFN, not at the institutions. In practical terms, all these CAs full under one organization.

[5] Based on the certs country; company headquarters gives slightly different count.

Heterogeneity is often good for an ecosystem, especially in terms of resilience. Because of the weakest-link nature of the HTTPS system, however, this also means many more single points of failure in case of CA compromise or misconfiguration. What is particularly troubling is that a number of the trusted CAs are run by authoritarian governments, among other less trustworthy institutions. Their CAs can issue a certificate for *any* Web site in the world, which will be accepted as trustworthy by all browsers.

HTTPS Market Concentration.

Shares of Certificate Types. Figure 5.2 shows the distribution of the different certificate types in the Observatory data. DV and OV each hold around half of the total. The figure also shows the number of domains each certificate was issued for: a single domain, multiple domains, or a wildcard. Table 5.2 shows the percentage of top sites (based on the Alexa ranking) that are using SSL certificates in general and EV certificates in particular. Higher-ranking sites had higher HTTPS adoption but did not differ significantly in terms of using EV over OV or DV, despite browsers providing more explicit trust signals with EV.

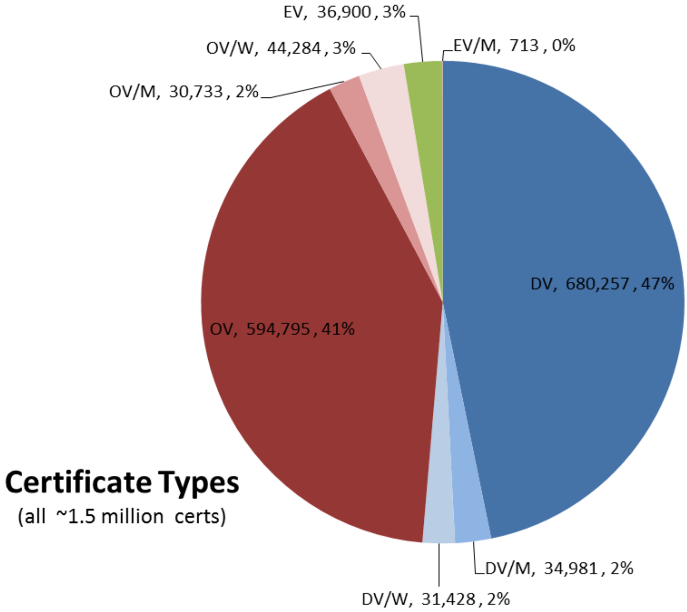


Figure 5.2. Global shares of SSL certificate by type (Dec 2010)

Table 5.2. Percentage of top sites running HTTPS (Dec 2010)

Top domains (Alexa ranking)	Percentage with a valid SSL certificate	Percentage of which is EV
Top 1000	35.3%	6.8%
Top 10k	25.2%	11.3%
Top 100k	15.2%	10.7%
Top 500k	5.0%	8.5%

Vendor Market Shares. We next mapped the market shares of the CA owners and brands, as shown in Figure 5.3 (for combined OV/DV/EV submarkets). Around 98% of all the certificates in the Observatory dataset are accounted for. The results indicate a highly concentrated market: three vendors – Symantec, GoDaddy and Comodo – hold more than three quarters of the market share. (Symantec, the largest commercial CA, owns multiple brands: Verisign, GeoTrust, Thawte, RapidSSL, and TC TrustCenter). The same pattern holds in HTTPS Ecosystem Scans. We also calculated the Herfindahl-Hirschman Index (HHI), to more formally assess the degree of market concentration This is presented in Table 5.3. The scores are above 2,500, indicating a highly concentrated market (Department of Justice and Federal Trade Commission 2010).

Figure 5.4 provides the distribution of certificates used by the top-thousand and top-hundred-thousand domains, to test whether higher-ranking websites chose particular vendors. Despite some differences, the concentration and overall pattern is the same as that for the total set of domains. (The Spearman rank coefficient rho is 0.75*** between total set of domains and the top-1k; rho is 0.94*** between total set of domains and the top-100k.) The largest difference is the FIRM-OWN-CA subgroup in the top-thousand domains, as companies such as Google, Facebook and Microsoft issue certificates from their own intermediate CAs.

Table 5.3. Market concentration for SSL certs by type (Dec. 2010)

	# Firms in Set	HHI-4
All certificate types	23+	2729
DV market	11+	3739
OV market	21+	2862
EV market	12+	5343

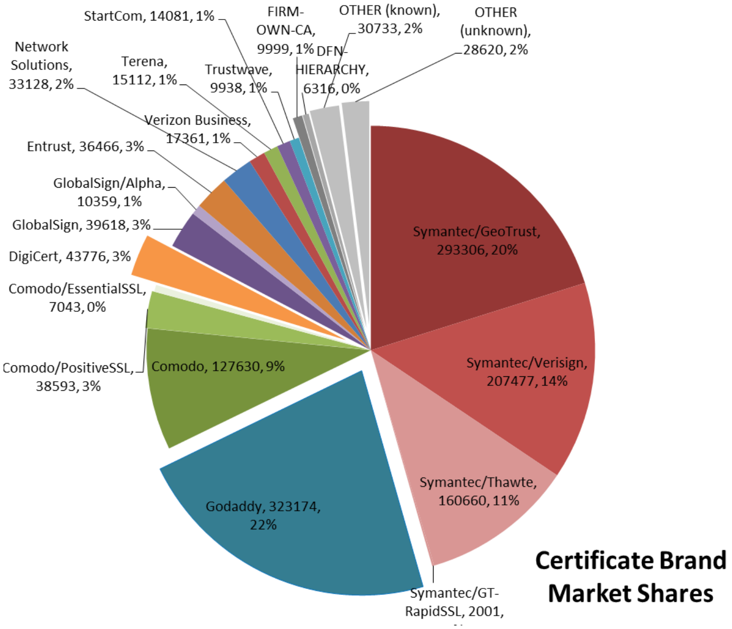


Figure 5.3. SSL vendor market shares for all certs (Dec. 2010)

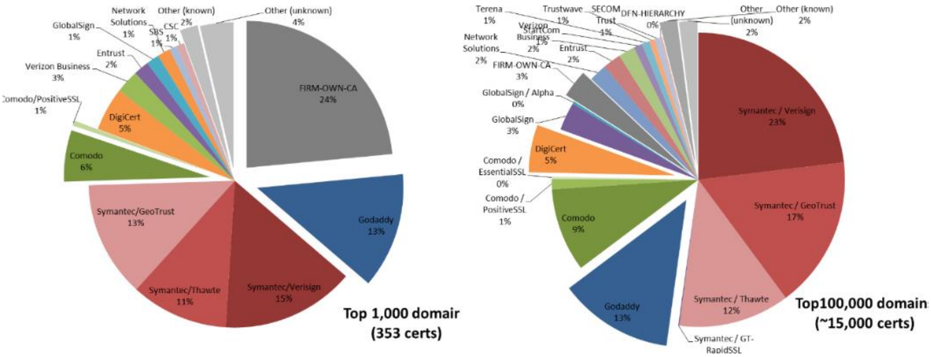


Figure 5.4. SSL vendors used by top websites (Dec. 2010)

In short, the market for SSL certificates is highly concentrated, despite the large number of issuers. In fact, both data sets find that around 75 percent of SSL certificates in use on the public Web have been issued by just three companies. The distribution is heavily skewed, with smaller CAs having little or no presence on the public Internet. Power-law distributions, although not surprising in Internet service markets, pose a major risk for the HTTPS ecosystem: if one of the large CAs is compromised, its root status cannot be revoked by browser vendors without massive collateral damage. One particular CA of GoDaddy had signed 26 percent of all valid HTTPS certificates in March 2013. That means if it were compromised, 26 percent of all Web sites that rely on HTTPS would need to be immediately issued new certificates (Durumeric et al. 2013). Otherwise, browsers ought to present certificate warnings or block access to those sites, posing an impossible tradeoff for the user between access and security. In other words, such large CAs are truly "too big to fail."

Price Competition

Mapping the prices for different certificate brands provides a sense of the degree to which the market is dominated by price competition. Figure 5.5 shows the price and market share for DV certificate offerings. Symantec/GeoTrust certificates (e.g. QuickSSL Premium) sell for $149 but have a much larger market share than Gandi SSL certificates selling at $16. OV and EV markets show similar dynamics, as showin in Figure 5.6, Figure 5.7, and Table 5.4. The situation is extreme in the EV market: the market leader, Verisign, sells certificates for approximately $1,000 and has a 63 percent market share. GoDaddy, offering certificates at a fraction of that price ($100), captures a mere 5 percent of the market. (As a reminder, the prices were as advertised by vendors in February 2013, while market shares were from the EFF 2010 data set. The HTTPS ecosystem scan data shows that similar market shares hold over time, with a slight shift of a few percentage points away from Symantec to cheaper providers.)

Table 5.4. Price ranges of different certificates

Certificate type	Min price	Max price	Average (sd)
DV	$0	$249	$81 (74)
OV	$38	$1172	$258 (244)
EV	$100	$1520	$622 (395)

Price competition has a comparable situation when we look at the long tail of market shares, or over time. In the long tail of the market, we mostly encounter small CAs with specific geographic markets. We compared prices of five brands in the long tail of the market, Etisalat, Netlock, RBC, TurkTrust, and, CERTUM, that have strong geographic presence. Their prices are in the same range as the market leader (e.g. $102-$326 for an OV certificate), seemingly focused on reaping profits from their local customers through a niche market strategy. For changes over time, we compared prices for twelve of the bigger brands in 2009 using the Internet archive. We found a mix of price increase and decrease for the various certificate types and brands, with no definitive trends, pointing to weak price competition.

The differences are intriguing, as certificates themselves are perfect substitutes (within each validation category). The differences might be explained by features bundled with the certificates, discussed in the next section. In sum: the SSL market shows few signs of intense price competition.

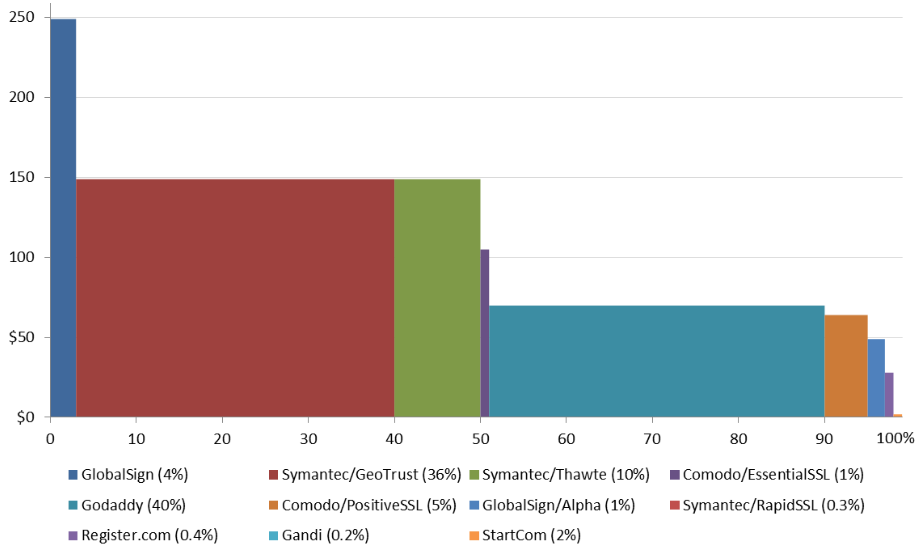


Figure 5.5. Price and market share of DV certs (Feb 2013, Dec 2010)

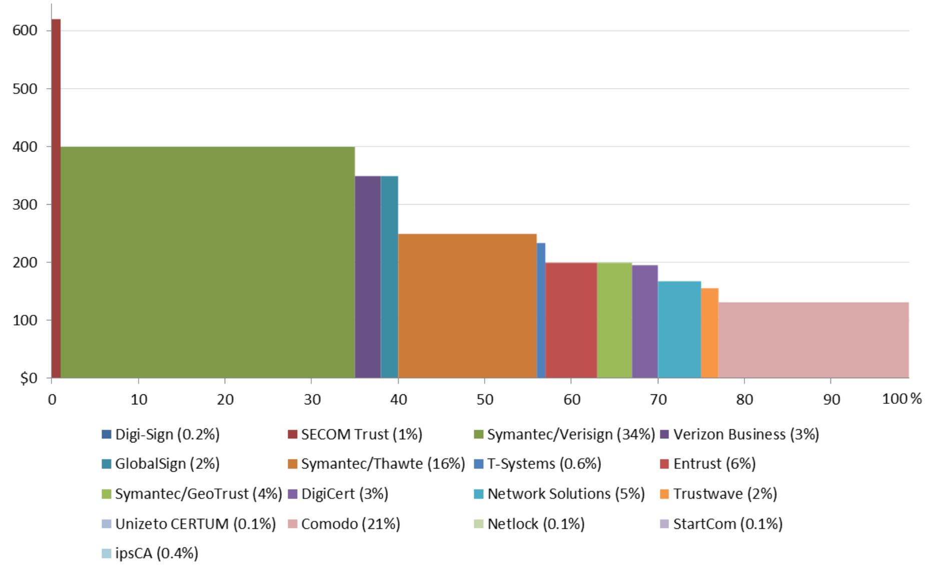


Figure 5.6. Price and market share of OV certs (Feb 2013, Dec 2010)

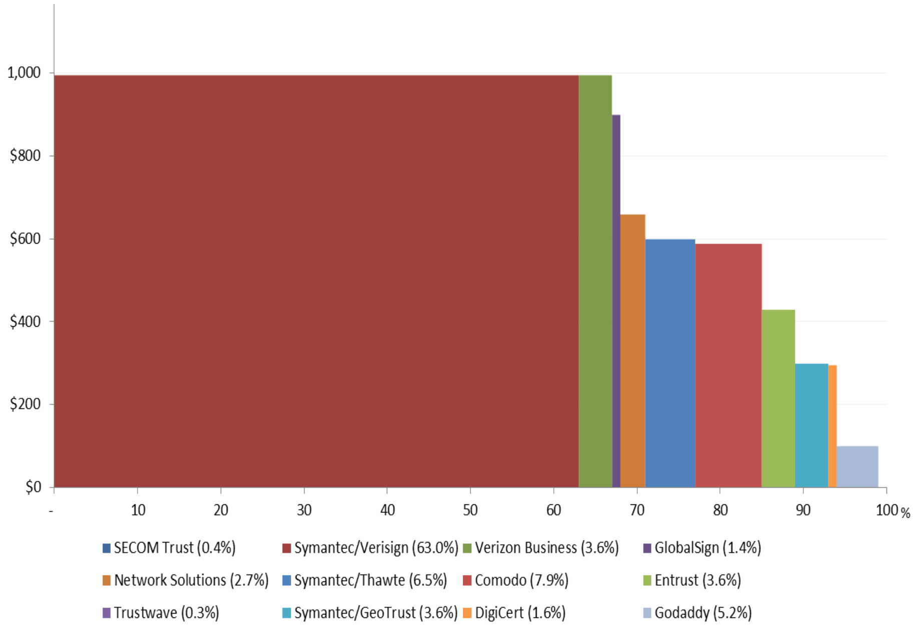


Figure 5.7. Price and market share of EV certs (Feb 2013, Dec 2010)

5.5 Analysis of HTTPS Market Incentives

The empirical data has revealed a pattern that requires an explanation: notwithstanding the fact that certificates of one type are technically perfect substitutes, each submarkets is highly concentrated, with very large price differences among suppliers and limited price competition. How can this be explained? In one sentence: because this market is not driven by the sale of the certificates themselves, but by the services and reputations signals bundled with the certificates.

No Race to the Bottom

Before we analyse the empirical pattern in more detail, we first want to highlight the fact that it falsifies a much-repeated claim about CAs, namely that they compete in a race to the bottom. Various researchers and industry observers have claimed that such a race exists in this market and some associate this with the poor security practices at DigiNotar and other compromised CAs (Kelkman 2013; Mills 2011; Roosa and Schultze 2010; Vratonjic et al. 2013).

At first glance, such a race is indeed what one would expect. The certificates of one type are perfect substitutes. This would suggest that the market is completely commoditized. Also, buyers can't meaningfully distinguish secure from less secure offerings. There are strong information asymmetries between the CAs and the buyers. More importantly, any CA can issue a certificate for any domain, which means that the security of SSL to prevent man-in-the-middle is determined by the weakest link in the market – i.e., the most insecure CA. In other words, buying from a supposedly more secure CA cannot protect the site owner against the threat of an attacker fraudulently signing his domain with a certificate from a compromised CA.

The combination of these two conditions – a completely commoditized market in which buyers have no way of telling which offering is more secure – should have produced a 'race to the bottom': a market dominated by fierce competition pushing prices towards marginal cost, with perverse incentives for security (R. Anderson 2008, 223; Shapiro and Varian 1998, 19–52).

The data, however, clearly suggests otherwise. We see market concentration, but not because dominant players leverage their increasing returns to scale to compete on price. There seems to be very little price pressure at work, in fact, especially in the market for EV certificates. The most expensive suppliers have large market shares, leaving only marginal shares for the cheapest ones. Even RapidSSL, the comparatively cheap 'fighter brand' of market leader Symantec, captures less than a 0.5% share of the DV certificate market.

One explanation for the lack of price competition could be the existence of entry barriers. It is unclear, however, what these barriers would entail exactly. It takes a substantial investment to get a root into the root stores of the leading browser and OS vendors. But there is a large group of CAs that are already present in those stores and that are cheaper than the dominant players. It does not seem to be a successful strategy. At the tail end of the market, where certificates are sometimes 5 to 10 times cheaper than those from the market leaders, we see that low prices have, by and large, only attracted minor market shares. There is one notable exception: GoDaddy, the hosting provider. Its cheaper DV certificates have captured 40% of the market, perhaps aided by the fact that they can bundle them with its huge hosting business. This stands in stark contrast to the market for EV certificates. Here GoDaddy's price is among the lowest prices in the market – and 10 times cheaper than the market leaders – and it has managed to capture only around 5% of the market. So the presence of entry barriers cannot really explain this pattern.

Rather than a market around a commoditized product competing on price and locked into a race to the bottom, the empirical pattern suggests that this is in fact a market with highly differentiated products that can be sold at dramatically different prices. In one sense, it is good news that the market is not driven by a race to the bottom, given the perverse security incentives associated with such a race. It does beg the question of how sellers have managed to differentiate their products and what this tells us about the security incentives that operate in the market.

What is Being Sold in SSL Certificate Markets?

If the certificates themselves are perfect substitutes, then how are suppliers differentiating their products to allow for the large price differences? In short: by bundling them with additional services. This becomes visible when we look at the marketing tactics used in the retail channels for SSL certificates.

CAs go out of their way to suggest that their offerings are different from those of its competitors. This has resulted in a rather baroque set of selling points on which they try to differentiate their products. We will not attempt to discuss them all, but rather focus on the main ones and then conceptually summarize the main differentiation strategies.

Some selling points are straightforward, such as the percentage of all internet users whose browsers will accept the certificate. There is no real differentiation here, however. All brands included in our overview (Figure 5.5, Figure 5.6, and Figure 5.7) are included in the dominant trust stores and therefore have a near-complete browser coverage measured in terms of internet users. Another selling point is the speed with which the certificate will be issued. Faster is seen as better. Most CAs promise to hand over DV certificates in minutes and EV certificates in a matter of days or even hours. We did not find meaningful differences among the brands.

CAs and resellers also stress the security 'features' of their certificates, such as its key length and the encryption level it supports, even though these features are virtually the same across all CAs and the security problems with SSL have had nothing to with breaking the encryption. As with browser coverage and speed, these features do not really differentiate the products on offer.

Another security-related tactic is leveraging the reputation of a CA brand. The market leaders all offer the buyers a seal to put on their site, indicating to site visitors that the site is secured by that specific brand. There are significant differences among brand reputations, if only in terms of name recognition, so this feature can account for a part of the price differentiation.[6]

[6] That said, we also found rather forced attempts to differentiate. CAs stress the difference between static and dynamic seals – which says nothing more than whether the seal is a static picture or an animated one with a bit of dynamic information, such as the current date.

Some CAs also bundle security services with the certificate, such as monitoring whether the buyer's domain is hosting malware or phishing sites. Another bundled tool supposedly scans whether the buyer's site handles credit card data in compliance with PCI standards.

Arguably, the most incomprehensible differentiating tactic is the 'warranty' on which some CAs compete. The warranty is not for the buyer, but for the end users who suffer fraud when using a site that was secured by an SSL certificate from the CA that should not have been issued in the first place. It is a rather mindboggling exercise trying to understand in real world terms how this warranty would work and how it would benefit the buyer of the certificate. To illustrate: in the case of DigiNotar such a warranty seems to only come into play if DigiNotar had been the official supplier of certificates for Google and the Iranian victims would have suffered some sort of fraud. Unsurprisingly, as far as we can tell there are no cases were a CA actually paid damages to end users under this warranty. Still, the idea seems to be that it would function as a trust signal to third parties – i.e., the warranty provides the visitors of the buyer's site with extra assurance that it is safe to conduct business with the buyer, because they can hold the CA liable if it turns out that it is not really the site of the buyer. Of course, in reality end users have never heard of these warranties, the information about the warranty amounts is not available to them, let alone that they know which CAs offers higher warranty amounts. In fact, end users rarely know, or care about, what CA actually issued the certificate in the first place. This has not stopped the CAs from competing the warranty amounts, where higher amounts supposedly demonstrate more secure or trustworthy certificates.

In addition to these selling points marketed in retail channels, there are also strategies that specifically target enterprise customers. These are much less visible to outside observers and we currently only have some anecdotal evidence on this from conversations with enterprise buyers. We encountered three additional differentiating features, each of which help explain the price differentiation and the dominance of the current market leaders.

First, and perhaps foremost, is the provision of enterprise-level certificate management services. One IT security manager of a multi-national firm explained how valuable support services are for the management, billing and reporting related to certificates. They employ certificates in thousands of domains for tens of different legal entities across many countries. Each entity faces different requirements in terms of billing languages, methods and periods, tax rules, reporting processes and more. What set the market leaders apart is the extensive and integrated back-end support for meeting these requirements. Smaller suppliers offered no such services.

Second, they bought from the market leaders because the reputations of the main brands functioned as a sort of a liability shield towards their corporate leadership, shareholders, and regulators, in case something would go wrong. It is a variant on the old adage: 'Nobody ever got fired for buying IBM'.

The third benefit from buying from market leaders is less explicit and a bit counter-intuitive. Enterprise buyers understand that security in this market is a weakest-link problem. They also understand that three of the four market leaders were hacked in recent years and are therefore not immune to the threat that brought down DigiNotar. This all suggests that there might not be any real security benefits from buying from them. The attacks have also demonstrated something else, however: these CAs are less likely to be thrown out of the root stores.

To put it differently: the market leaders are, in a sense, too big to fail. Browser and OS vendors will be extremely reluctant to remove them from the root store. This can actually be a benefit to the CA's customers, because it provides them with better business continuity. The collapse of DigiNotar has underlined the value of this advantage. For the government and business customers of DigiNotar, the breach was in essence a crisis of availability (continuity), not of confidentiality or integrity. Tens of thousands of certificates had to be found and replaced in about a week. During that time, government representatives publicly acknowledged that they faced the threat of a large-scale 'blackout' of governmental services (NRC 2011). That scenario is unlikely for the customers of the too-big-too-fail market leaders. Of course, buyers can still switch away from those suppliers if they choose to, but under less time pressure.

So, to sum up, what are buyers actually buying in this market and how can this explain the pattern of high concentration and of high price differentiation? The certificates themselves are perfectly substitutable, but CAs differentiate via:

- Bundled security services, such as scans of the buyer's s site for malware or PCI compliance;
- Enterprise certificate management services, such as support for the management, billing, and reporting around large numbers of certificates;
- Brand reputation as a liability shield against the buyer's organizational superiors, shareholders, regulators or others who may hold the buyer accountable in the face of security issues;
- Trust or security signals aimed at third parties, most notably end users, such as brand reputation, site seals, warranty amounts and, in a sense, the high price of a certificate itself signals security;
- Higher continuity in case of security failures at the CA, because of the unlikelihood of its root status being revoked by browser and OS vendors.

The technical artefact of a certificate is a perfectly substitutable information good, but in light of these features, one could argue that what CAs sell in practice is a subscription-based service. Subscription services are less substitutable and can thus be more effectively differentiated in the market.

The fact that some of the 'security' features of these services do not really provide actual security, does not change this. Knowledgeable buyers probably understand that buying from the market leaders does not actually increase the security of their HTTPs service. After all, the security of HTTPs is a weakest-link problem and thus determined by the weakest CA. Moreover, the reputation of the market leaders does not necessary mean they are actually more secure, as the large CAs have also proven vulnerable to attack and have not always been transparent about this. Even when a buyer understands this, it still makes sense to buy from the market leaders rational. Enterprise support, a liability shield, security signals to third parties and better continuity insurance are all valuable.

The price differences among certificates are large in absolute terms, but they are modest when compared to other cost components. Saving several hundreds of dollars is a marginal gain in light of the cost of installation, perceived trustworthiness and better support. Furthermore, the price of a certificate will typically be amortized over millions or even billions of clicks. Even when compared to a company's own intermediate CA, which can issue free certificates, the price difference is that significant. In the words of the respondent, self-issued certificates are 'not as cheap as you would hope'. There are still substantial costs related to the need for dedicated and trained staff for certificate management and the time spent by other business units involved in billing and reporting.

All these considerations reinforce the choice to buy from the market leaders, i.e., they strengthen concentration in the market and differentiate them enough from competitors to charge substantially higher prices.

Incentives for Security

Now that we better understand what the market is actually selling, what does this tell us about the security incentives at work? Given that the market leaders successfully differentiate their products via, among other things, security-related features, there appears to be a significant willingness-to-pay for security among buyers. But does this willingness-to-pay translate into actual security incentives? In other words, can CAs attract more customers or charge higher prices by investing more in security? This is not at all clear. Two classic problems affect the proper alignment of incentives*: information asymmetry* and *externalities*.

The information asymmetry prevents buyers from knowing what CAs are really doing. Buyers are paying for the perception of security, for a liability shield and for trust signals to third parties. None of these correlates verifiably with actual security. Given that CA security is largely unobservable to buyers, their demand for security does not necessarily translate into strong security incentives for CAs.

The incentive problem is exacerbated by the negative externalities that are the result of the weakest-link security of the system. The failure of a single CA impacts the whole ecosystem, not just that CA's customers. All other things being equal, these interdependencies would undermine the incentives of CAs to invest, as the security of their customers also depends on the efforts of all other CAs.

The most powerful incentive for security seems to be reputation effects. Given that the market leaders leverage their reputation to charge higher prices and capture a larger market share, does this make them more sensitive to the reputation damage caused by breaches? Again, not necessarily. Yes, they have more of a reputation to lose compared to smaller, lesser-known brands. But they also are less threatened by the ultimate reputation effect: being removed from the root stores of browser and OS vendors and, as almost unavoidable consequence, going into bankruptcy. The fact that the market leaders are more or less too-big-to-fail provides a perverse incentive to browser and OS vendors to keep them in the root store even at high cost. To phrase it differently: those vendors have to trade off availability of a large portion of the web against the confidentiality and integrity of the communications of the specific domains that are attacked.

Ironically, the security problems that have plagued the HTTPS ecosystem over the past few years may in fact benefit the market leaders, even though they themselves were partially to blame for these problems. The breaches have increased the demand for security and this demand seems to latch onto whatever security signals are available, regardless of their relationship to actual security. It seems reasonable to assume that post DigiNotar, buyers felt the pressure to shift from smaller CAs towards the larger, more 'trusted' brands (– this would be an interesting hypothesis for future work). The security problems also appear to have led enterprise customers to strategies of redundancy – i.e., encrypting connections using two certificates from two suppliers instead of one – which, again, would benefit the market leaders.

All of this may impact the attempts to fix the systemic vulnerabilities of the system. The current incentive structures seems quite favorable for the dominant players, which might make them reluctant, or at least less eager, to push for adoption of one of the proposed technical solutions. This is not to suggest that they will act against them, but rather that the status quo works quite well for them – perhaps even more so because of recent breaches. We should keep this in mind during the last part of this paper, where we discuss possible improvements in HTTPS governance.

5.6 Improving HTTPS Governance

In the aftermath of these CA breaches, policymakers and technologists have suggested regulatory and technical solutions to the systemic vulnerabilities of HTTPS. Let us evaluate these solutions in light of the market-incentive analysis.

Regulatory Solutions

The HTTPS authentication model is by and large unregulated in both the U.S. and the E.U. This is bound to change in the near future. Each entity has opted for a completely different approach: the U.S. gives priority to technological solutions and lets industry self-regulate in the meantime. The European Commission (the executive branch of the E.U.), on the other hand, proposed the Electronic Identification and Trust Services Regulation in June 2012. Unlike the more common E.U. *directives* that require implementation in national law, *regulations* acquire direct binding force of law in all E.U. member states upon adoption in Brussels. In April 2014 the European Parliament adopted substantial amendments to the commission proposal, leaving the regulation only for the E.U. Council (national governments of the E.U.) to approve. This section outlines the scope, underlying values, security requirements, security breach notification, and liability regime of the E.U. proposal (European Parliament 2014), as well as the recent proposals by Mozilla for "chain of trust transparency".

Scope. The E.U. proposal regulates *trust service providers*, including CAs (art. 3 sub. 16b). All major CAs appear to fall within both U.S. and E.U. jurisdiction (Asghari et al. 2013, n. 26). While inherently local, regulation may therefore be an effective instrument to address the observed market failures and positively influence HTTPS security globally. Other critical stakeholders in the HTTPS ecosystem, however, such as browser vendors and Web-site operators, remain unregulated in the proposal. This limited scope impacts the proposed security measures considerably.

Underlying Values. The E.U. proposal focuses on availability interests to boost trust in e-commerce, neglecting confidentiality and integrity concerns connected to the systemic HTTPS vulnerabilities already outlined. Apart from failing to observe privacy and communications secrecy obligations under the E.U. Charter of Fundamental Rights, the proposal completely ignores the Snowden revelations. The BULLRUN and MUSCULAR disclosures have made clear that HTTPS significantly raises the costs of mass dragnet surveillance and has been a primary target of intelligence agency subversion. Large Internet companies have now started or accelerated efforts to encrypt communication paths both with users and within their own networks using TLS. The April 2014 parliament amendments not only ignore these developments, but also make explicit that the HTTPS provision is "entirely voluntary" for Web services (recital 67).

Security Requirements. The E.U. proposal introduces new obligations for CAs to adopt security requirements. Their details will be determined by the European Commission in a so-called implementing act. While such delegation to the executive branch provides some flexibility to adapt requirements to new technological developments, the E.U. proposal fails to specify regulatory priorities or underlying values. Moreover, the April 2014 parliament amendments literally state that "industry-led initiatives (e.g. CA/Browser Forum)" influence such requirements (recital 67). Naming a CA group as influential in a law that seeks to address failing security practices of CAs indicates control by dominant market players.

Security Breach Notification (SBN). In theory, SBNs help minimize the damage after a breach has occurred and provide incentives for organizations to invest in information security upfront. The E.U. proposal introduces an SBN regime stating that notification needs to occur "within 24 hours" to relevant authorities if the breach "has a significant impact," a concept that is not defined in the law. The general public is informed when a breach harms the "public interest" (also undefined). Again, the European Commission will determine those details, but the parliament proposal states that CAs should be subject to "light-touch and reactive ex-post supervisory activities" and that there exists "no general obligation to supervise non-qualified service providers" (i.e., CAs offering certificates for HTTPS).

Aforementioned information asymmetries and CA breaches render defensible a strict regime for notifications—which types of breaches should be made public by default, for example. Experiences with SBN legislation in the U.S., moreover, suggest that SBNs need to be complemented with punitive (e.g. sanction and liability regimes) and proactive enforcement (e.g. as part of annual reporting) to create real incentive to notify—and avoid noncompliance by less well-intentioned companies (Winn 2009; Thaw 2011). In addition, reputation losses might not affect major CAs that do not risk being thrown out of root stores for non-reporting. Reporting not only breaches, but also the vulnerabilities that led to them, would be a major step forward, as would a scheme of responsible disclosure. Such lessons are not included in the E.U. proposals or considerations. Moreover, the parliament has further weakened the SBN regime by mandating light-touch and ex-post supervision. Again, these amendments indicate capture of the regulatory process by dominant CAs.

Liability. As already observed, liability for security breaches is disclaimed across the HTTPS ecosystem and transferred through terms and conditions to end users. The 2012 European Commission proposal sought to address such liability dumping by imposing a strict liability regime on CAs for "any direct damage," with CAs bearing the burden of proving that they handled the situation non-negligently. The 2014 parliament amendments reverse this burden of proof; customers and users now have to prove malicious intent or negligence at CAs post-breach. Moreover, CAs are allowed to transfer liability in their terms and conditions to end users. Astonishingly, the parliament explicitly codifies liability dumping. Again, there are traces of regulatory capture at the European Parliament.

The weakest-link problem of HTTPS creates more fundamental problems with security through liability: small CAs will be unable to conduct business with large corporations processing vast amounts of sensitive data. Consider DigiNotar with its an annual budget of a few million U.S. dollars; it could never cover damages for the rogue certificates that were issued for Google, Facebook, Skype, cia.gov, etc. in the midst of its security breach. Smart CAs will thus circumvent liability by creating subsidiary special-purpose companies that bear full liability and can easily file for bankruptcy. Indeed, DigiNotar quickly went bankrupt post-breach, while its parent company Vasco has escaped unscathed.

Tackling fundamental issues with liability regimes requires carefully crafted policies or broad mandates for enforcement. Liability should be matched with security requirements and distributed among all stakeholders: domain owners should have incentives to protect their assets through HTTPS offering and implementation (Arnbak and Van Eijk 2012), while browsers should strengthen their CA policies (as discussed later). The European Commission failed to consider such fundamental drawbacks, and the parliament amendments make matters worse by codifying liability dumping and reversing the burden of proof.

Chain of Trust Transparency. Unrelated to the E.U. proposals, Mozilla has proposed the so-called "chain of trust transparency." As discussed earlier, one cannot assure that HTTPS communications are subject to systematic but unnoticed surveillance without transparency (Soghoian and Stamm 2012), but today it is only starting to emerge through various (research) projects such as the browser plug-in CertPatrol for Firefox.

In a recent amendment to its CA policy, Mozilla requires that subordinate CA certificates "either be technically constrained or be publicly disclosed and audited" (Mozilla 2013). Subordinate CAs, in other words, must either be constrained to issue certificates for only a (small set of) domain name(s)—on internal networks, for example—or their chain of trust must be publicly disclosed and audited. The aim is to hold subordinate CAs to similar standards as root CAs and make a root CA accountable for all the sub-certificates it signs. Existing subordinate CA certificates were given until May 15, 2014, to comply, so it is too early to observe how Mozilla enforces noncompliance. Nonetheless, chain of trust transparency warrants at least consideration and, from a theoretical perspective, encouragement throughout the HTTPS ecosystem (Roosa and Schultze 2013). So far, it has not been part of any regulatory proposal.

Technological Solutions

A host of technological solutions to the systemic vulnerabilities of the current system are being developed. Among the most prominent are Convergence (http://convergence.io/details.html), Perspectives (http://perspectives-project.org), DANE (Hoffman 2012), Sovereign Keys (https://www.eff.org/sovereign-keys), Certificate Transparency (http://www.certificate-transparency.org; Laurie, Langley, and Kasper 2013), Public Key Pinning (Evans, Palmer, and Sleevi 2012), and TACK (http://tack.io; Marlinspike 2013). From the perspective of governance, we can make several general observations:

- All proposals solve the weakest-link problem by introducing another authority to check whether the certificate that is validated through the normal HTTPS process is indeed the correct one.
- All proposals reduce information asymmetry of buyers and users, versus CAs, by systematically uncovering suspect certificates.
- All proposals can function on top of the current CA system, leaving it in place or depending on it; a subset can also replace it.
- All proposals can follow incremental adoption paths, albeit some more difficult than others, and all need support from browsers.

None of these solutions is close to large-scale adoption. That said, they do seem promising in terms of addressing the current weaknesses, especially the weakest-link problem, for which regulatory solutions appear ineffective. Therefore, in the long run they are preferable, and it's relevant to assess how they relate to the incentives of the HTTPS stakeholders. Some scholars predict multiple proposals will eventually be adopted (Bonneau 2014).

As argued earlier, the insecure status quo can be beneficial for market leaders. In light of this, one might assume that CAs are not particularly keen on actively helping any of these proposals along, especially the ones that theoretically could make them obsolete. In practice, however, some CAs are involved in developing potential solutions—for example, DigiCert and Comodo are experimenting with Certificate Transparency (Langley 2012). Other proposals require nontrivial activities on the side of the domain owner, which may be done by their CA as a complementary service to current business models. Furthermore, each proposal is intensely debated in relation to browser performance. Any form of large-scale adoption requires default support by browser vendors. Google and Mozilla have been particularly active in this area.

While none of these solutions is easy to scale, there are benefits for early adopters, a key requirement for any solution to take off. Whether the costs are worth it depends on the kinds of threats HTTPS stakeholders want to defend against. An average cybercriminal might not be interested in breaching a CA and manipulating network traffic already encrypted through HTTPS, as financially attractive information can be acquired through more cost-effective attacks (Langley 2013; Florêncio and Herley 2013b). From previous breaches, it appears that state-sponsored attackers and large corporations, rather than criminals, are more likely to engage in the complex man-in-the-middle attacks. For some user groups and domains, such adversaries make early adoption attractive.

5.7 Conclusion

Recent breaches at CAs have exposed several systemic vulnerabilities and market failures inherent in the current HTTPS authentication model: the security of the entire ecosystem suffers if any of the several hundreds of CAs is compromised (weakest link); browsers are unable to revoke trust in major CAs ("too big to fail"); CAs manage to conceal security incidents (information asymmetry); and ultimately customers and end users bear the liability and damages of security incidents (negative externalities). Understanding the market and value chain for HTTPS is essential to address these systemic vulnerabilities. The market is highly concentrated, with very large price differences among suppliers and limited price competition. Paradoxically, the current vulnerabilities benefit rather than hurt the dominant CAs, because among others, they are too big to fail.

In terms of solutions, the E.U. has opted for a regulatory response, while the preference in the U.S. is for industry self-regulation and technological solutions. In general, the technological solutions aim to solve the weakest-link security problem of the HTTPS ecosystem. Several proposals are promising, but none is near large-scale adoption. Industry self-regulation has only augmented market failures, rather than solve them. The proposed E.U. regulation does not consider the role of all stakeholders in the HTTPS ecosystem, thus reinforcing systemic vulnerabilities by creating new long-term institutional dependencies on market-leading CAs. The April 2014 European Parliament amendments make matters much worse, which seems to be the result of extensive lobbying efforts by part of the industry.

Regardless of major cybersecurity incidents such as CA breaches, and even the Snowden revelations, a sense of urgency to secure HTTPS seems nonexistent. As it stands, major CAs continue business as usual. For the foreseeable future, a fundamentally flawed authentication model underlies an absolutely critical technology used every second of every day by every Internet user.

Chapter 6: ISP Incentives to Deploy Deep Packet Inspection[1]

6.1 Introduction

Internet intermediaries such as ISPs are sometimes encouraged to take on security measures that present their own challenges and controversies. The use of Deep Packet Inspection (DPI) is one such example. DPI allows Internet traffic to be analyzed and dealt with in real-time; a capability which can be used to block malware and other network intrusions (Kim and Lee 2007). This capability however is often considered intrusive in terms of privacy. It also changes the traditional role of ISPs. ISPs used to be understood as "bit pipes" that routed network traffic without caring about content. Now they could manage their networks more effectively by filtering, prioritizing, or monetizing certain categories of traffic. DPI quickly touched upon multiple sensitive policy topics, such as network neutrality, control of copyrighted material, censorship, privacy, and intermediary liability (Bendrath and Mueller 2011; Mueller, Kuehn, and Santoso 2012; Wagner 2012).

[1] This chapter is a major revision of: Asghari, Hadi, Michel J.G. van Eeten, Johannes M. Bauer, and Milton L. Mueller. 2013. "Deep Packet Inspection: Effects of Regulation on Its Deployment by Internet Providers." Presented at the 41st Research Conference on Communication, Information, and Internet Policy (TPRC 2013), September 27-29, Arlington, VA.

Related Publication. Mueller, Milton L., and Hadi Asghari. 2012. "Deep Packet Inspection and Bandwidth Management: Battles over BitTorrent in Canada and the United States." *Telecommunications Policy* 36: 462–75. doi:10.1016/j.telpol.2012.04.003.

Acknowledgements. The authors wish to thank Marcel Dischinger, Tiziana Refice, Hao Qiu, Meredith Whittaker, Shahab Zehtabchi, as well as Measurement-Lab, Google, and New America for their help in accessing and processing Glasnost data. This research was partially funded by the Next Generation Infrastructures Foundation.

This paper investigates the extent to what DPI was deployed by ISPs under various regulatory conditions. This is interesting as ISPs face conflicting pressures. They have a commercial interest to deploy DPI for bandwidth management (BEREC 2012), while customers and regulators might not look favorably on the intrusive monitoring of customers' traffic (Kuehn and Mueller 2012). Regulatory attitudes have both deterred and encouraged DPI deployment. In an earlier work, we found that bandwidth scarcity, weak privacy safeguards, and Internet censorship were significantly correlated with DPI use for bandwidth management, but did not compare their relative strengths (Asghari, Van Eeten, and Mueller 2012). We extend this work here and ask which force is stronger in DPI deployment: commercial incentives of ISPs to manage bandwidth, or external regulatory and consumer concerns about privacy?

The DPI data comes from a crowd-sourced online test named Glasnost, developed by Dischinger et al. (2010). Glasnost is run by end-users worldwide to detect if their ISP uses DPI to throttle or block BitTorrent traffic—a specific but common application of DPI.

The paper continues with some more background on why DPI is contested; Section 6.3 explores the steps to convert 800,000 Glasnost test logs into a dataset of DPI use (by broadband ISPs for bandwidth management) across 46 countries and spanning 2009-2012. Section 6.3 and 6.4 present the DPI trends and multivariate model. Section 6.6 discusses the findings, followed by the conclusions.

6.2 Background

DPI is a label for a collection of technologies and applications that detect and shape live traffic on a network. They recognize patterns in and across network packets. The primary technical capability here is the ability to recognize; recognition enables packet manipulation and notification. Packet manipulation is the ability to act on the detection, by blocking, prioritizing or de-prioritizing, or otherwise regulating the flow of certain traffic. Notification concerns actions around the information that can be extracted from detection, such as generating reports, alarms or billing incidents (Mueller 2011).

Implementing DPI can have economic benefits for ISPs, or it might be necessary to meet other obligations. Bendrath and Mueller (2011) identified a number of use cases for DPI in the literature. Among them, bandwidth management and ad-injection potentially benefit the ISP, while malware detection, government surveillance, content regulation, and copyright enforcement can benefit other actors. We can add other use cases that benefit ISPs: network quality monitoring and per application billing. Deploying DPI entails costs, including equipment and software costs, operational costs, and legal and reputational risks.

Anecdotal evidence points to bandwidth management being the most important incentive for ISPs to deploy DPI. A study by the Body of European Regulators of Electronic Communications found that traffic management is the number one application of DPI for network operators (BEREC 2012). The chief technology officer of a mid-sized ISP told us that after deploying the DPI for traffic shaping, their ISP managed to service twice the number of subscribers with the same total upstream bandwidth, translating into a four to one return of investment in a year. Similar figures were reported to us by an industry consultant.

Customers however might not look very favorably on such uses. They might be upset when they face degraded download speeds or service quality; others might find it intrusive or unfair. Regulators might also look unfavorably at the use of DPI due to competition and privacy concerns. If the backlash is strong enough, ISPs might decide to abandon the practice. Kuehn and Mueller (2012) observe this pattern in multiple cases: typically, ISPs initially start using DPI secretly; at some point, the issue is discovered and subsequently followed by a public outcry and pursuit by the regulators, which in some cases results in the ISP abandoning the practice.

In an earlier work, we looked at seven economic and political drivers of DPI – extracted from the above use cases – and found upstream bandwidth scarcity, lack of competition, weak privacy safeguards, and presence of Internet censorship to be significantly correlated with DPI use (for bandwidth management) by ISPs (Asghari, Van Eeten, and Mueller 2012). That work did not however compare the relative strengths of these factors.

ISPs face conflicting pressures. Public and regulatory attitudes both deter and encourage ISPs to deploy DPI. In a few countries, policymakers and regulators have directly weighed in on the topic of DPI (e.g. Canada and the U.S., see Mueller and Asghari 2012). Existing regulation and norms regarding privacy and surveillance might act as a deterrent. Conversely, countries with systematic Internet censorship encourage ISPs to monitor and regulate content; ISPs might use this as an opportunity or obligation to deploy DPI. The question we ask is which force is stronger, the commercial incentives of ISPs to deploy DPI for bandwidth management, or the external regulatory and consumer privacy concerns? The answer to the question also implies the extent to which ISPs have agency and discretion over the deployment of technologies in their networks, given that they need to be attentive to the regulatory environment.

6.3 Methodology

To determine DPI use, one strategy might be to survey ISPs. This is quite problematic, however, as it is costly, response rates tend to be low, ISPs that do respond might be less likely to use DPI, introducing selection bias, and their answers cannot be verified. A different strategy was taken by Dischinger et al. (2010). They built a crowd-soured measurement tool named Glasnost. End users anywhere on the Internet can run Glasnost; it measures the speed of several upstream and downstream flows, and determines whether throttling is happening, and if so, is it done using deep packet inspection. Glasnost has been hosted on Measurement Lab (also known as M-Lab, http://www.measurementlab.net/) since early 2009. For this study, we used approximately 800,000 test logs, spanning 2009 to 2012 (Table 6.1).

Glasnost only detects one DPI use case, bandwidth management, and even there only in terms of blocking or throttling BitTorrent. This measurement limitation affects the paper’s findings, a point that we take into account in later sections. Nevertheless, BitTorrent throttling is a major DPI application. As mentioned earlier, ISPs named bandwidth management as a top reason they use DPI, and BitTorrent was a major bandwidth hog during the study period, although gradually losing ground to streaming websites (Sandvine 2012). Detecting if their ISPs throttles BitTorrent was a key motivation for many users to run the tool.

Table 6.1. Glasnost tests per year

Year	Glasnost test logs	# aborted or corrupt	# noisy tests	With verdicts (all countries)	With verdicts (select ISPs)
2009	355,685	180,350	21,983	153,352	115,118
2010	203,232	114,623	17,029	71,580	54,350
2011	78,403	29,514	9,943	38,946	28,977
2012	106,433	48,086	9,726	48,621	37,131
Total	**789,408**	**338,081**	**64,526**	**338,081**	**235,576**

Note: 46 countries (out of 207 in the data) are selected; this equals 578 ASNs (out of 8356) belonging to 215 ISPs

Turning Glasnost Logs to Verdicts. The M-Lab platform stores detailed logs and packet dumps, but unfortunately not the final verdict shown to users (DPI or not). This made it necessary to parse the logs to obtain this verdict. Glasnost works by recording and comparing the speeds of several network flows between the client and the server. Data is transferred using an application protocol and a random bitstream, and on an application-assigned port and a neutral port. If the application flow on a neutral port is significantly slower than the other flows, it can be concluded that the ISP is performing application-based throttling. However, matters are complicated because the Internet routes traffic on a best-effort basis and speed fluctuations are normal. The test developers came up with reliable thresholds for meaningful differences and for when to deem a connection too noisy for clear results. Further complications include a large number of aborted tests, and tests with results that do not make sense (e.g. the application flow is significantly faster than the controls). The combinations required understanding the detail workings of Glasnost to decide on verdicts for each combination.

Mapping Tests to ISPs. The test logs include the IP address of the user running the test, but not the country, AS, or ISP. We added this information by using MaxMind's GeoIP database (https://maxmind.com), pyasn for AS lookups (https://github.com/hadiasghari/pyasn), and our own AS-to-ISP mapping (explained elsewhere).

Calculating DPI Scores. We finally calculate the yearly percentage of tests indicating DPI for each ISP. We then classify ISPs with a DPI score of under 0.15 as not using DPI and above 0.15 as using DPI. This cut-off point is chosen because Glasnost tests can have measurement errors up to approximately 16% of the time (Dischinger et al. 2010; Dischinger and

Gummadi 2011), which we fine-tuned using qualitative data.[2] To reduce bias caused by false positive and negatives, we discarded ASes with too few tests (minimum five tests, from five different IPs, on five different days).

In the end, our dataset contains 774 observations: a DPI score for 215 broadband ISPs, per year between 2009-2012. (In 86 cases, there were not enough observations to determine a score for a year). Note that only broadband ISPs are included in the study, as mobile ISPs (and ASes) follow different patterns of DPI use. The ISPs are located across 46 countries for which we could collect the explanatory variables used in the multivariate model.

6.4 DPI Trends

More than half of the ISPs in our sample (122 out of 215 used DPI for bandwidth management in one or more years. This number is surprisingly high, given the public and regulatory unease towards it use, and given the fact that Glasnost detects only one use case of DPI. It appears that many ISPs viewed the benefits of DPI to outweigh its costs.

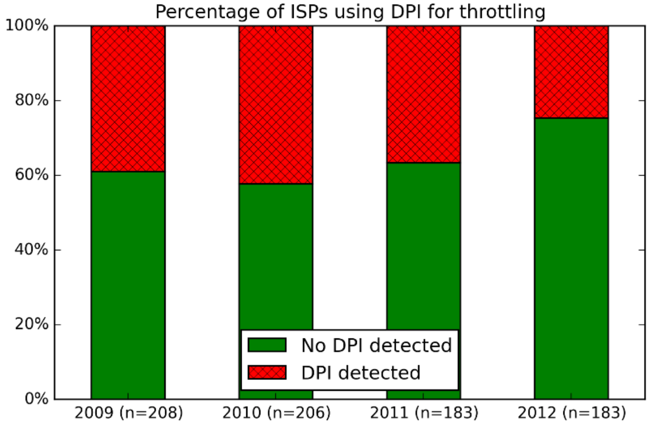


Figure 6.1. Percentage of ISPs using DPI for bandwidth management

Figure 6.1 shows the yearly breakdown of this statistic: around 40 percent of ISPs were found to be using DPI in 2009-2011, with 2010 being

[2] It is also possible to categorize ISPs, based on the DPI score, as persistently throttling, or only for certain customers or at certain times. The cutoff points are, however, hard to choose systematically.

slightly higher; the percentage drops to 25 in 2012. One explanation for the peak in 2010 is that mass diffusion occurred in that year, perhaps as DPI technology became more affordable. The subsequent drop could indicate negative pushback due to market forces or political pressure, or ISPs not finding the technology beneficial.

DPI-deploying ISPs are located in a wide variety of countries, as illustrated in Table 6.2. In 2009, ISPs in 29 countries (63 percent of all countries) were using DPI in a noticeable or pervasive manner; this gradually drops to 17 countries (36 percent) in 2012. This drop could indicate that ISPs shied away from using DPI for bandwidth management; it might also reflect that BitTorrent throttling was not the top concern anymore due to the increasing popularity of streaming websites (Sandvine 2012).

Table 6.2. DPI use (by ISPs for bandwidth management, 2009-2012)

Year	Negligible DPI Use (less than 15% of ISP market)	Noticeable DPI Use (15% to 50% of ISP market)	Pervasive DPI Use (more than 50% of ISP market)
2009	17	12	17
2010	19	9	18
2011	21	9	16
2012	29 (of which 2 no tests)	5	12

Individual ISP scores are shown in Figure 6.2. Each row represents all ISPs in a certain country, comparing 2010 and 2012. Within each row, there are bars representing the individual ISPs, with DPI scores written in them. The bars are sized to the market share of the ISPs.[3] Red (striped) means ISPs doing DPI, green (dark) means ISPs not doing DPI, and white indicates ISPs for which no Glasnost test were run or for which we had no market shares.

[3] ISP market data is from TeleGeography (https://telegeography.com/research-services)

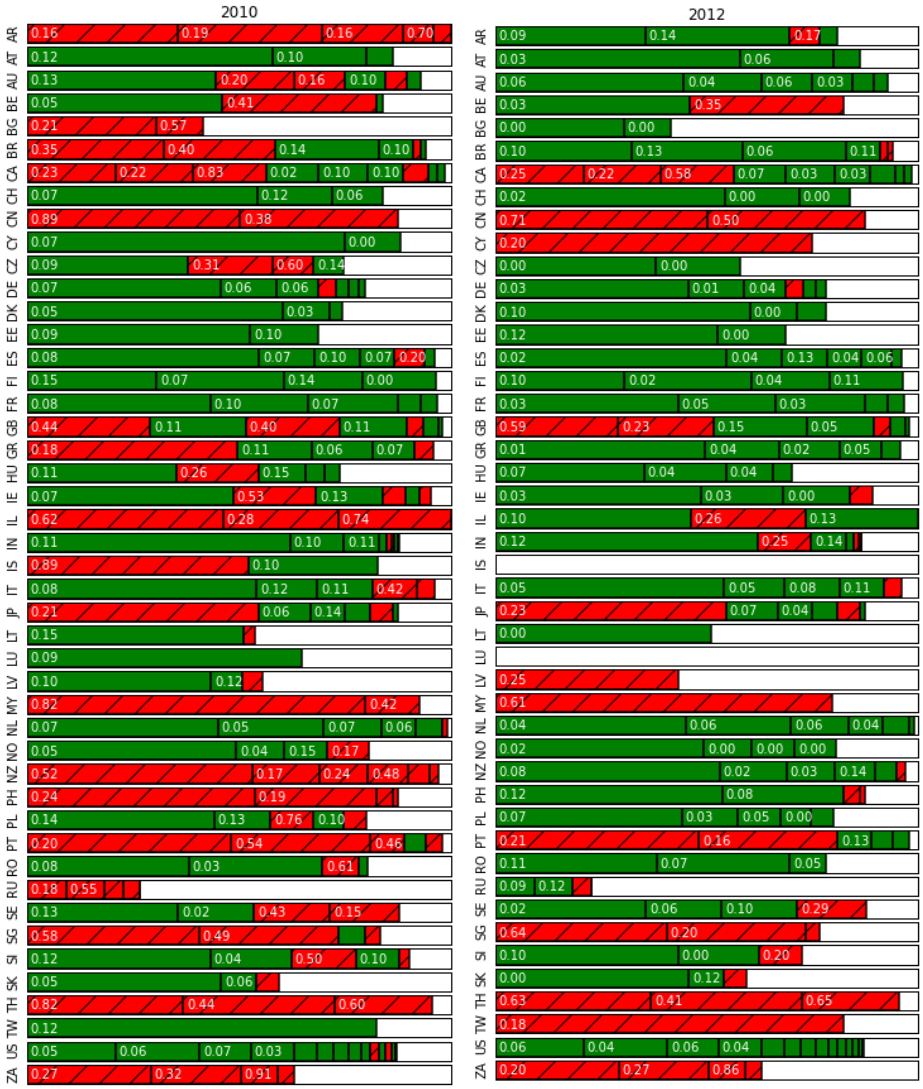


Figure 6.2. DPI score per ISP in various countries for 2010 and 2012

6.5 Multivariate Modeling

We construct a multivariate logistic regression model with DPI use by ISPs as the binary response variable and a number of explanatory and control variables.[4]

[4] Using ISP as the unit of analysis. An alternative is to calculate and use country DPI score as the independent variable; but that reduces the granularity of the model.

The explanatory variables are chosen from the DPI drivers previously found to be significant, that is bandwidth scarcity, privacy safeguards, and Internet filtering (Asghari et al 2012). The motivation for these drivers, as a reminder, were as follows: (i) upstream bandwidth scarcity means more pressure on ISPs to limit bandwidth hogging applications, the most direct application of DPI; (ii) strong privacy safeguards in a country increases the risk of public or regulatory backlash over packet inspection, deterring ISPs from deploying DPI; (iii) Internet censorship could lead to increased DPI for bandwidth management as well, as ISPs piggyback on the need for DPI equipment to comply with the government's requirement to monitor and regulate network content. After a review of indicators available in public datasets of sufficient quality, we choose those listed in Table 6.3 as proxies for these drivers.

We include two ISP level controls: ISP market power and size (also Table 6.3). Regulatory and public attention is often more on larger players, which could make them more cautious; on the other hand, their market power might give them maneuvering room with customers and regulators. Size is included because the deployment of DPI might be easier or harder at various scales. We do not assume a direction for either of these controls.

Finally, we add fixed effects for years, to account for the overall DPI trends. The motivation to include them is that several factors in the model lack any time-variability. Cross-country data collection studies are many times not repeated, due to costs and other challenges; e.g. Privacy International has not done a newer version of their privacy report. Since institutional and country-level factors change slowly, this is often acceptable. Regardless, the fixed effects for years allows us to control for the yearly trends.

Table 6.3. Independent variables in the multivariate DPI model

Variable	Operationalized Variable	Range (avg±std)	Source
Bandwidth scarcity	International bandwidth per Internet user[5], in kbps, natural log	1 – 6.3 (3.9 ± 1)	ITU World I. 2012 (http://itu.int/en/ITU-D/Statistics)
Privacy safeguards	Privacy index, composed of constitutional and statutory protections, privacy enforcement, and other safeguards.	1.3 – 3.1 (2.2 ± 0.5)	Privacy Int. Privacy Monitor 2007 (http://privacyinternational.org/reports)
Internet censorship	Internet filtering of socially sensitive topics (e.g. sexuality, gambling). Recoded as 0 (low f.) and 1 (high f.)[6]	0 – 1 (0.1 ± 0.3)	OpenNet Initative 2012 (http://opennet.net/research/data)
ISP size	ISP subscribers, log-10	3.6 – 8.0 (5.7 ± 0.7)	TeleGeography 2012 (footnote 3)
ISP market power	ISP market share, percentage	0 – 86 (19 ± 18)	TeleGeography 2012 (footnote 3)

The regression results are presented in Table 6.4. All the country-level and ISP-level factors have a significant effect; among the fixed-effect intercept, only 2012 is considerably different from the previous years. Coefficients in logit models can be interpreted as odds-ratios. Thus, after controlling for other factors:

- An approximate doubling of a country's bandwidth per user reduces odds of an ISP using DPI by 28% (odds ratio 0.82, confidence interval 0.70 - 0.95)
- A unit increase in a country's privacy index reduces odds of an ISP using DPI by 41% (odds ratio 0.59, confidence int. 0.42 – 0.83)
- Being in a country with Internet filtering increases odds of an ISP using DPI by 164% (odds ratio 2.64, confidence int. 1.62 - 4.31)

[5] Ideally, bandwidth scarcity would be measured per ISP—for future work.

[6] Only six countries in the sample filter social topics: China, India, Italy, Russia, Singapore, and Thailand. ONI lacks data for around half the countries in the sample. With the rationale that the ONI monitors most countries with high Internet filtering, and to avoid reducing sample size, we assume the missing countries to do little or no filtering (country codes: AR, AT, BE, BG, BR, CH, CY, CZ, EE, ES, GR, IE, IS, JP, LT, LU, NL, NZ, PL, PT, SI, SK, TW, ZA).

- A ten-fold increase in an ISP's subscribers reduces odds of it using DPI by 48% (odds ratio 0.52, confidence int. 0.40 - 0.68)
- An increase in an ISP's market share has no effect on the odds of it using DPI (confidence interval 1.01 - 1.02)

The signs of the three key country-level factors are in the hypothesized direction. The results indicate that privacy safeguards at a country level deter DPI use (for bandwidth management); Internet censorship and bandwidth scarcity lead to higher DPI use (for bandwidth management). The Internet censorship relation is perhaps the most interesting, which we shall return to in the discussions. Among the ISP-level controls, the relationship with size can be interpreted that at larger scales, deploying DPI becomes technologically cumbersome or economically inefficient (i.e., it is cheaper to get more bandwidth).

Comparing the strength of the factors involves comparing the changes in odds; however, it becomes tricky when interpreting what a one level change in privacy index means. This we shall return to in the discussions, where we interpret the results to answer the paper's research question.

Table 6.4. Multivariate (logit) regression model for DPI use by ISPs

```
                          Logit Regression Results
==============================================================================
Dep. Variable:                  dpi   No. Observations:                  774
Model:                        Logit   Df Residuals:                      765
Method:                         MLE   Df Model:                            8
                                      Pseudo R-squ.:                 0.07794
                                      Log-Likelihood:                -465.45
converged:                     True   LL-Null:                       -504.79
                                      LLR p-value:                 8.971e-14
=============================================================================
               coef    std err          z      P>|z|      [95.0% Conf. Int.]
-----------------------------------------------------------------------------
privacy_index -0.5287      0.175     -3.016      0.003        -0.872    -0.185
filtering      0.9688      0.250      3.868      0.000         0.478     1.460
bandw_pu_ln   -0.2043      0.080     -2.564      0.010        -0.360    -0.048
subs_log10    -0.6580      0.136     -4.821      0.000        -0.925    -0.391
market_share   0.0141      0.005      2.998      0.003         0.005     0.023
FE_2010        0.1153      0.211      0.546      0.585        -0.299     0.529
FE_2011       -0.0497      0.220     -0.226      0.822        -0.481     0.382
FE_2012       -0.6518      0.235     -2.777      0.005        -1.112    -0.192
intercept      4.8694      1.009      4.825      0.000         2.891     6.847
```

Effect of Individual Countries. We assessed the robustness of the results, and whether coefficients were driven by one particular country, using resampling. We removed remove all ISPs belonging to a specific country from the dataset, and calculated the regression coefficients, and compared the difference. The removal of no country caused any of the coefficient signs to flip; differences were minimal in most cases.

Model Fit. The model's log-likelihood ratio is highly significant, indicating that the model has explanatory power (compared to an intercept only model). The low pseudo-R square (0.08) however shows much unexplained variance and missing covariates. Reducing parameters to simplify the model does not yield in a better a Akaike Information Criterion score (a measure that penalizes for model complexity). The fit can be also visually assessed using a separation plot, as shown in Figure 6.3. There is some clustering of events on the right and non-events on the left; but there are event lines everywhere. A final check is using the model to predict DPI outcomes on our own dataset, and counting the number misclassified. This is shown in Figure 6.4. The area under the ROC curve (AUC score) adds to a combined sensitivity and specificity of 70 percent. This is better than chance but pretty inaccurate, highlighting the unexplained variance.

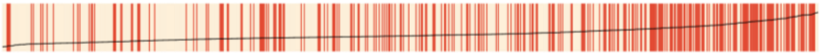


Figure 6.3. Logistic regression diagnostic with a separation plot

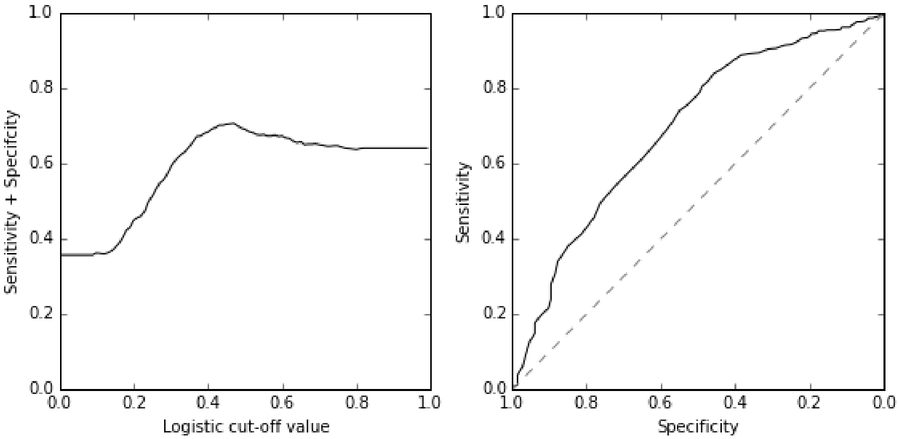


Figure 6.4. Logistic regression diagnostic with the ROC curve

6.6 Discussion

We found that more than two thirds of ISPs used DPI for bandwidth management at some point, including in many liberal democracies. This is surprisingly high, and suggests that for some ISPs the benefits of using DPI outweigh the risks of public or regulatory outcry. If we were to include other DPI applications, this number would be likely even higher.

From multivariate modelling we found that after controlling for other factors, DPI use was lower in countries with better privacy safeguards (constitutional and statutory protections, privacy enforcement, and other safeguards). This was expected. Privacy safeguards directly (by making DPI use explicitly illegal) or indirectly (by correlating with consumer preferences for privacy) deter ISPs from inspecting traffic contents openly.

We also found DPI use (for bandwidth management) to be higher in countries with Internet censorship practices. Internet censorship might be done with or without the aid of DPI. In either case, it does not make it automatic that the technology is also used for bandwidth management. The fact that censorship correlates with bandwidth management indicates that ISPs in these countries piggybacked on the norm of interfering with network traffic for their own agenda.

Concerning ISP incentives and cost savings related to using DPI for bandwidth management, we found that bandwidth scarcity at the country-level (lower international bandwidth per user) increases the odds of DPI. We also saw that larger ISPs on average use less DPI. This can be interpreted as the technology becoming more cumbersome to implement on large- scale; or economically inefficient, that is the larger ISPs simply have more bandwidth at their disposal; both interpretations point to the ISP's discretion. We can infer that ISPs have discretion based on the fact also that DPI use varies among ISPs operating in the same country, i.e., under similar market and regulatory conditions.

Regression diagnostics showed that although our model is decent, it leaves much unexplained variance, which could be linked to ISP discretion. It could also be explained by regulatory trajectories not captured in the model. An example is the net-neutrality battles in the United States and Canada, described by Mueller and Asghari (Mueller and Asghari

2012). In both countries, major ISPs deployed DPI to conserve bandwidth from early 2006 on; this was discovered and led to public protests, litigation and regulatory proceedings. The outcomes differed in a paradoxical way. The Canadian regulator upheld the traffic shaping practices. In the U.S., the FCC's authority to regulate ISPs' network management practices was successfully confronted; nevertheless, US ISPs dramatically changed their behavior due to the controversy. No privacy laws being changed, but the regulator encouraged or discouraged DPI in a lasting way. In 2012, DPI use remains pervasive in Canada and negligent in the U.S. (Figure 6.2).

We now answer turn to the question of which dominates, commercial ISP incentives to use DPI or the privacy concerns against it; the answer seems to be the former. The coefficients for bandwidth scarcity, and the fact that ISPs have discretion support the dominance of ISP incentives. Internet filtering as an external factor is also used by ISPs as an opportunity. This leaves privacy safeguards as the sole external deterrent. After controlling for other factors, we see that one standard deviation change in privacy safeguards reduces the odds of DPI less than one standard deviation change in bandwidth per user (20.5% versus 28%), further supporting the dominance of ISP incentives.

This analysis highlights an inconvenient reality. ISPs have sometimes avoided undertaking security countermeasures, citing privacy concerns and other regulatory constraints. However, once there is a direct commercial interest involved, those concerns appear to lose significance, constraints turn into considerations, and ISPs engage the activity even with the risk of an external pushback. They do not do anything illegal in either case; but the internal evaluation for the same technical measure seems to change from "let's not do this if there is any doubt" to "let's do this until it's explicitly forbidden". The general implication is that arguments referencing "constraints" in cybersecurity policy need to be engaged critically.

6.7 Conclusion

In this paper, we looked empirically at the use of DPI technologies by ISPs over four years, for bandwidth management. We constructed a dataset for this purpose from the logs of a crowd-sourced tool named Glasnost, yielding a DPI finding for 215 ISPs in 46 countries and for four years. DPI is a politically contested technology; regulators and Internet users in varying countries have resisted it. Yet we found that DPI is used on a large scale for bandwidth management. We then built a multivariate logistic regression to compare the effects of several factors previously found to be correlated with DPI use; namely privacy safeguards, Internet censorship, and bandwidth scarcity. We found that privacy safeguards reduce the odds of DPI use and Internet censorship increases it. We discussed the interactions of the factors. In short, the we found that that the commercial incentives of ISPs to manage bandwidth outweighed the external regulatory and consumer concerns about privacy. ISPs have agency and discretion over the deployment of technologies in their networks, even though they need to be attentive to the regulatory environment. With the discretion also comes the need for transparency and accountability.

Chapter 7: Security Measurements and Public Policy: Mind the Gap[1]

Measurement-sets need to have certain features to be usable for policy research. This chapter reflects on this issue in light of the earlier empirical studies and provides a complimentary perspective to the dissertation's central question. It argues that a systematic gap exists between how Internet measurement researchers think about collecting data, and how other disciplines think about using data. It proposes guidelines for measurement projects to reduce this gap and make them accessible and relevant to a wider audience. The chapter

7.1 Introduction

Policy researchers in areas such as cybersecurity, privacy protection or network neutrality, can benefit substantially from large-scale empirical data, as findings based on global and longitudinal evidence are more reliable and insightful than those based on secondary sources and anecdotes.

Luckily, there is a substantial number of projects that generate large dataset that could potentially inform policy development in these areas. However, in our experience, a gap or mismatch exists between what measurement engineers tend to record, and what the social scientists, economists, and policy researchers can typically consume. Consider packet dumps: for the measurement engineers they provide the ultimate accountability and flexibility to answer new questions in the future. For the policy researchers who typically answer questions around larger aggregates such as months or ASNs, the individual dumps are a big hurdle; they mandate downloading gigabytes to extract the few interesting

[1] This chapter has been peer-reviewed and published as: Asghari, Hadi, Michel J.G. van Eeten, and Milton L. Mueller. 2013. "Internet Measurements and Public Policy: Mind the Gap." In *Sixth USENIX Workshop on Cyber Security Experimentation and Test (CSET '13)*. doi:10.2139/ssrn.2294456.

pieces of information. One could judge this as merely a nuisance or lost machine time; but in practice, it might impose a serious barrier to further use of the data if a parsing tool has to be first written by the social scientists to extract and interpret those interesting bytes.

Social scientists also deal with problems of measurement error and statistical validity of samples in ways different from technical researchers.

This mismatch is not simply a matter of inconvenience for policy researchers; it directly undermines the potential policy impact of the measurement project. Computer scientists and engineers that build large-scale measurement tools often hope that their systems will impact Internet policy by increasing transparency in a particular realm. While this impact occasionally happens, more often than not valuable data never reaches the policy debate.

In this paper we shed light on this problem by briefly describing our team's efforts to estimate deep packet inspection deployment in ISPs worldwide using a measurement test called Glasnost (Dischinger et al. 2010; Dischinger and Gummadi 2011). Glasnost allows ordinary Internet users to detect whether their ISP is differentiating between flows of specific applications. We briefly discuss the challenges we faced while parsing, analyzing, and interpreting the logs as an illustration of a public dataset that can be very informative for the policy discourse. The challenges where not unique to this measurement set, however. We discuss several other large measurement efforts later in the paper.

The contribution of this paper is to provide guidelines on how Internet measurements *could* be stored, structured, and supported to make it easier to use for a wider range of researchers. The significance of this exercise is a two-way discussion; one that obviously benefits the policy researchers; but also increases the chances that many more measurement projects can create the policy impacts that their designers had in mind.

7.2 Accessible Measurements

The Gap between Measurement Experts and Policy Researchers

Internet measurement datasets can be an invaluable tool for policy research. They provide valuable empirical evidence to support the policy discussions in many areas, such as botnets, network neutrality, or SSL certificate use. That being said, it's important to note that developing the instruments and maintaining the infrastructure that runs and stores the measurements constitute only *half* the work required to use them for policy research.

The other half includes a mundane task of transforming the measurement logs into datasets that can be handled by common statistical packages; and finally, experimenting with models, adding independent variables, uncovering patterns, and validating and interpreting the results. Policy researchers would *prefer* to focus only on this last part, as that is where their main contribution lies. In practice however making sense of the raw data and the *transformation step* turns out to be extremely time-consuming. It is also this step that forms the gap between the two disciplines.

The gap is structural, rooted in the different requirements of computer scientists and policy researchers in the way they work and use data. For example, computer scientists often need to remain as close as possible to the raw data. This allows for accountability and validation. If an ISP denies deploying DPI, they can be presented with the packet dumps. It also makes it easier to mine the data in previously unthought-of ways in the future. In many cases, test results or interim reports are not even saved; the idea being that one could regenerate them from source at any point. In some measurement projects, historical data is not kept at all — you are offered the live feed and can decide to log it from now on.

As we shall see in the next section, the needs of policy researchers are different from these. Just to give some examples: researchers employing econometric techniques are interested in having a well-defined and consistent measurement approach as the starting point of their work; they prefer to work with observations spanning several years, and typically use organizations and companies as their unit of analysis (rather than individual machines). Robust, longitudinal, and aggregated, in contrast to flexible, real-time, and granular data.

Is it possible to have store and structure data in a fashion that addresses both sets of needs?

The "Ideal" Measurement Set

In this section, we elaborate the needs of policy research, based on our experience in working with large measurement datasets. We shall in later sections assess how several other datasets compare with this criterion. Implementing all these suggestions might be hard and perhaps impractical in certain cases. They are meant as guidelines for measurement projects that want to increase their potential policy impact by enabling the analyses of other researchers.

1. *Measurement sets ought to keep archives and will benefit from being up to date.* This should really be seen as an entry-level requirement, as policy research benefits most from looking at patterns over time.

2. *Providing spatially and temporally aggregated versions of the data is helpful.* Typical units of analysis in policy research include the organization and country level (versus individual IP addresses), and over periods of weeks, months, quarters and years (versus days). Making such aggregated versions of the data available for download will be very helpful, despite the drawbacks of duplication. Not only will it reduce download and processing times, but also resolve privacy issues with disclosing IP addresses, thus opening up the data for more researchers.[2]

3. *Measurements ought to have clear verdicts and interpretations.* If the meaning of a particular measurement is ambiguous, life will be very hard for other researchers. It is very hard to interpret the results of a test created by others, as it forces a researcher with a different background to understand all details of a system they have not implemented. Anomalies and corner cases, most notably false positives/negatives, make this process even harder. [3]

[2] With regards to spatial-aggregation, geo-location and IP-to-ASN data from the time of the measurement should be used. If this data is not already stored along with the measurements, historical lookup databases can be consulted.

[3] Please note that we are not advocating over-simplification and binary verdicts; measurements will many times be messy, like the real world. In practice, this recommendation means having good documentation regarding both typical and unusual cases; keeping interim verdicts and logs (the complete-trace); providing parsers. As a last resort, supporting researchers attempting to use the data, via a mailing list or other means, can be beneficial.

4. *Consistency of the measurement instrument over time is important.* This recommendation is as important as it is difficult to execute. The difficulty comes from the fact that measurement researchers often experiment with various parameters in their systems to see which creates the most accurate results. Unfortunately, this practice can be very harmful for econometric analysis, as one cannot simply pool the results derived from the different measuring instruments together. Keeping parallel versions of the tests running while experiments are conducted might be one solution; changes should be well documented in any case. Monitoring of the testing infrastructure and its storage can also be crucial to avoid gaps in recorded data.[4]

5. *Data collection should be organized in a manner that promotes sample validity.* The number of measurements, and its balanced distribution over ASNs, countries or use cases, is extremely important for statistical validity. Guaranteeing this is again understandably very hard; enlisting the aid of researchers from other disciplines, e.g. interaction designers, might be very fruitful in incentivizing different user groups to participate in measurements.

7.3 The Case of Analyzing Glasnost

Researching Deep Packet Inspection

We shall start by briefly describing the nature of our interest in using one of the datasets, Glasnost. Our research project involved the deployment and governance of deep packet inspection (DPI) technology. DPI can disrupt the Internet's end-to-end principle in both beneficial and controversial ways, e.g. thwarting spam and malware, rationing bandwidth, blocking access to censored content, and building user profiles for advertisers. With its dual potential, DPI use is contested politically (Mueller, Kuehn, and Santoso 2011). In broad terms, we wanted to find out what impact this new technological capability has on how states and companies govern the Internet.

[4] A commitment to maintain the tests over time might prove costly or infeasible for many projects. Deploying the tests on shared and open platforms such as M-Lab could be one way to reduce maintenance costs.

This leads to a set of sub-questions, such as which Internet providers are using DPI, to what extent, and how they respond to various regulations and laws aimed at privacy, network neutrality, and censorship.

How could we answer these questions? One way to get this information is to ask the operators, but as a research method that is quite problematic. It would be costly and time consuming to survey all Internet service providers, many of them will refrain from responding, and for the others we have to doubt the truthfulness of their answers. So an alternative strategy is for network users to run tests that reveal what is actually happening to their traffic. This is precisely what the *Glasnost* test does. Glasnost, developed by researchers at the Max Plank Institute, enables users to detect blocking or throttling of BitTorrent and other protocols by their access provider, and whether this is done using DPI or the TCP port (see Dischinger et al. 2010 for details). The M-Lab platform gave Glasnost a global reach, with the test being run thousands of times by users from 2009 to 2012. The test-logs are stored and made publicly available. All of this seems ideal for our research purposes.

Evaluating the Glasnost Dataset

In this section of the paper, we will describe the steps involved in processing the glasnost logs into the dataset suitable for our research. Our initial expectation was that this should be relatively straightforward, but this turned out to be far from the case. We compare Glasnost data against the guidelines laid out earlier. This is not meant to criticize the Glasnost project, but to better understand the issues that many projects seeking policy impact face.

Archives & ongoing logging

The Glasnost test has been on M-Lab platform (http://www.measurementlab.net/about) since early 2009, and it is still maintained and live.

Level of Aggregation

The Glasnost data is stored at the level of individual tests on Google Storage. For each test, a server log and a packet dump are stored, of which only the log is useful in our work. Furthermore, out of each log, only the header and a few summary lines at the end are needed. This means that much more data needs to be downloaded than is actually needed, even in the absence of spatially and temporally aggregate data. For example, for just February 2012, 115 GB of compressed data has to be downloaded. This take several hours to download on a campus gigabit connection due to the way Google storage functions. After extraction and removal of the packet-dumps, we are left with 33 GB of uncompressed data. Extracting the useful lines brings us down to 40 MB for per-test metrics, which is less than 0.1% of the downloaded data. Geo location and ASN information is also not stored with the data, making it necessary to use historical records for accuracy.

Turning Logs to Verdicts

We wished to have a verdict for each test run: does it indicate the presence of application based throttling or blocking (hence, DPI), or not? Although these results are shown to the user when they conduct the test, they are not stored in the logs. This made it necessary to parse and analyze the logs to re-calculate the result.

This turns out to be very involved. The test logs store details information about each measurement flow. The Max Plank researchers provided a parser that works on logs after May 2010; for the first batch of log files, we had to write our own parser by reverse engineering the Glasnost server code. The parsers took us only part of the way: it provides separate verdicts for upload, download, throttling and blocking, while we required *combining* them for a final verdict. Due to anomalies, corner cases and scarce documentation, this was not straightforward.

We will briefly explain these steps, but not bother the reader with all the complexities. In short, Glasnost works by recording and comparing the speeds of several network flows. Data is transferred between the client and server using different protocols (the application being tested versus a random bit-stream) and on different TCP ports (the application assigned port versus a neutral port), and detected interruptions are also recorded. If for instance the speed of the application flow is much slower than the control flow, it can be concluded that the ISP is performing application-based throttling. Since the Internet routes traffic on a best-effort basis, speed fluctuations are normal. The test developers came up with thresholds that could indicate speed differences reliably, and also determine if a connection is too *noisy* to make any inferences. The cases get more complicated when considering noisy flows, and *failed flows* (when zero bytes are transferred). Further complications include a large number of aborted tests, and tests with anomalous results, for instance where the BitTorrent flow is found to be significantly faster than the control flow, which does not make sense. These yield a large number of possible combinations that required us to decide on the verdict for each combination.

This got us involved in the details of the workings of the measurement tool, took over two months of full time work to accomplish, and was very far removed from the policy research we planned to conduct.

Consistency over Time

The Glasnost data has several discontinuities in the logs. First, the log formats changed three times. This change did not cause any major statistical problems, only extra parsing work. The second discontinuity was statistically relevant, however, and was caused by changes to the default parameters used by Glasnost, including the flow durations, repetitions, and directions. These were changed mid-2009 to find the optimal settings that yielded the fewest false results without making the test too long. These changes create very visible jumps in the results' percentages. (As Figure 7.1 shows, the number of false positives and negatives drops considerably after October 2009). The third discontinuity, also significant, was that for several periods in 2010 and 2011, the longest of which spans several weeks, no test logs exist. This was due to an unfortunate *rsync* problem between M-Lab and Google Storage, resulting in data loss.

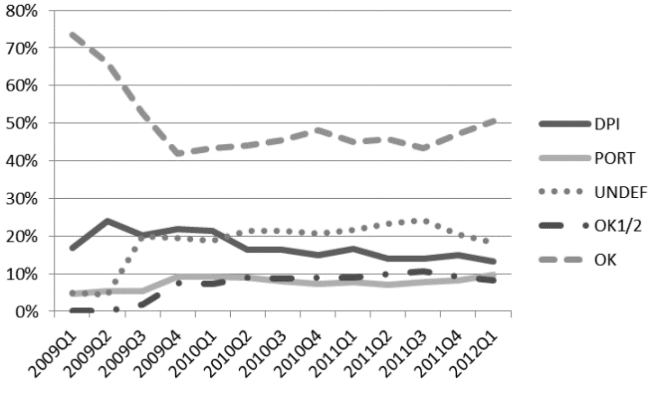


Figure 7.1. Test verdict percentages over time

Issues with Sample Size

One cannot blame a crowd-sourced project for inadequate sample size, but can think of remedies. Two specific problems of sample size exist in the Glasnost data. First, although the test has supported testing different protocols since May 2010, BitTorrent still makes up the vast majority of the tests, because it was set as the default choice on the test interface. The other issue is regarding ASNs with 10 or less tests over a period, where one false positive or negative can make a large difference in the results of that ASN. A future remedy for both situations would be that the M-Lab website recommends visitors to run Glasnost when the total number of tests from that visitor's ASN is low, and for it to set the default protocol similarly.

On the plus side, Google made good efforts to publicize the M-Lab initiative generally. The number of tests conducted directly responds to these publicity efforts. When those efforts dwindled, the number of users conducting tests goes down.

Support Infrastructure

Overall, the M-Lab team makes a strong effort to ease use of the Glasnost data. The support included an active mailing list, access to base parsing scripts. In terms of documentation, the original Glasnost paper provided a good starting point, but as mentioned, more was desirable. The test authors also clarified some issues at one or two points. Over time, the quality of support improved, indicating a learning process for all parties. This was in our opinion what enabled our project to eventually succeed.

At this point and after much work, we have our "cleaned" dataset – one that is ready for econometric analysis. In the ideal situation, this would have been our starting point.

7.4 Other Cases

We compare Glasnost to four other measurement projects in Table 7.1. These include a spam trap, the SANS DShield database, the EFF SSL-observatory and finally the Conficker sinkhole, all of which have provided valuable input to policy research.

These datasets benefit from being (mostly) longitudinal and enjoy a relatively good sample size. The aggregation level is unfitting in two of the five cases; the verdicts lack clarity in two of the five cases. The discontinuity problem exists in two of the five. The main take away message here is that the guidelines can be used to evaluate all these large datasets; the criteria are meaningful and of value in all the cases.

Table 7.1. Evaluating five measurement sets

	Time Period	**Aggregation & format**	**Logs to verdicts**	**Consistency**	**Sample size**
Glasnost	2009-now	(-) Individual test logs	(-) Parsing involves many steps	(-) Multiple discontinuities	(+/-) Mixed
Spam trap	2005-now	(+/-) Logs, daily. IP based.	(+) Relatively clear, excellent support	(+) Yes	(+) Good
DShield[5]	2006-now	(+/-) Logs, daily. IP & port.	(+/-) False positives still unclear	(+) Yes	(+) Good
SSL Observatory[6]	Only 2010	(+) SQL dump; Certificates	(+) Good documentation and support	N/A	(+/-) Full, but once
Conficker sinkhole[7]	2009-now	(-) Logs, hourly; per connect	(+) Relatively Clear	(-) Log format change	(+) Full

7.5 Discussion

A comment we received in an earlier draft was that the proposed guidelines do not consider costs of the measures. We have two responses to this comment. First, one could look at incurred costs as simply the costs of doing business. This of course depends on the aims of the measurement project owners: if they wish their work to have an impact on telecommunication policy and related fields, and to aid policymakers to make informed decisions based on data, which we suspect to be often the case, then bearing these costs will be simply a necessity. It is basic economics: lowering the costs involved in using your data means more

[5] http://www.dshield.org/about.html

[6] https://www.eff.org/observatory

[7] http://www.confickerworkinggroup.org/wiki/

researchers will use it, thus increasing the odds of it being impactful. Second, implementing the guidelines will not be as costly as one thinks: the objective is to lower the barriers to entry, not eradicate them. Simply thinking about the issues in the design and deployment phase of measurement projects will already accomplish much. *Hallway usability testing* (Spolsky 2000), championed as a common sense approach to software engineering, can also work here. A hallway usability test is where you grab the next person that passes by in the hallway and force them to try to use the code you just wrote. We could expand the idea as persuading the next econometrician passing through the department to use the measurement sets, and resolving the top issues faced. This should be neither formal nor costly; it might even turn out to be fun.

Related Work. The Internet measurement community already appreciates a number of strategies for what they call "*sound measurements*". Our guidelines are comparable in many points. For example, Paxson (2004) states the importance of keeping the complete audit-trial, tying this to the need for reinterpreting the data at a future time when the original rich research context is forgotten; now, compare this to our criteria of clear verdicts and interpretations. In this literature stream, our work simply reiterates and highlights some of the already known sound strategies that are important for interdisciplinary research. On a different note lies the benefits and hardships of *interdisciplinary research*. Thuraisingham (2009) talks specifically about reasons to pursue research projects between computer science and the social sciences and highlights a number of challenges along the way, e.g. that computer scientists need to be ready to develop new tools and avoid one-size-fits-all solutions. The National Academies (2005) book "Facilitating Interdisciplinary Research" provides a long list of key conditions for interdisciplinary work. Most of them are essentially linked to conversations, connections, and combinations among teams of different disciplines, which in our opinion is similar to the gap presented in this paper.

7.6 Conclusion

This paper presented the following guidelines for computer scientists designing large-scale measurements, so that their efforts are accessible and relevant to policy research:

1. Measurement sets ought to keep archives and will benefit from being up to date.
2. Providing spatially and temporally aggregated versions of the data is helpful.
3. Measurements ought to have clear verdicts and interpretations.
4. Consistency of the measurement instrument over time is important.
5. Data collection should be organized in a manner that promotes sample validity.

As a case study, we highlighted the challenges faced by our own team in using a number of datasets, including Glasnost. The dataset was invaluable, and provided us with empirical insights into deep packet inspection use that would otherwise remain unanswered. However, due to the way Glasnost logs are stored and structured, we were forced to spend considerable time upfront to process the logs into a suitable format. For many social scientist, this hurdle will be insurmountable not only because of time constraints, but because they lack access to the technical competencies that are needed to move forward. This creates a major distraction from policy research and in our opinion represents a structural dissonance between the different goals of computer scientists and policy researchers in using Internet measurements. Although data transformation is inevitable, the complexity and amount of time required to do so directly impacts the number of research teams willing to use a particular dataset. The proposed guidelines are an attempt to reduce this gap.

Chapter 8: Conclusions

In the concluding chapter, I shall review what we have learnt in the preceding chapters, and connect them to the dissertation's central question and objective. The dissertation focused on three themes for strengthening cybersecurity: the significance of incentives; the role of Internet intermediaries; and the use of security measurements to infer behavior and incentives. These were combined in the following question, which has been researched via a literature review, four empirical studies, and a reflection paper.

> *What can security measurements tell us about internet intermediary behavior? What incentives explain these behaviors, and how do firm characteristics, market forces, and regulatory conditions shape these incentives? What does this imply for cybersecurity policy?*

Each of the peer-reviewed studies answered this question in the context of a particular intermediary and security issue. In section 8.1 , I summarize the studies, including the measurement data that was analyzed and the findings about incentives. Next, I reflect on the commonalities and broader regularities among the studies and answer the question more generally. Section 8.2 reflects on the analysis of security measurements, and section 8.3 looks at policy implications. The findings and reflections constitute contributions to the field of economics of cybersecurity.

The studies received significant attention outside of academia, among industry and policy experts, illustrating the value of the dissertation's approach to inform policy via analysis of security measurements. The botnet mitigation studies were presented[1] at the Organization for Economic Cooperation and Development (OECD), the Dutch Ministry of Economic Affairs, the German Association of the Internet Industry (ECO), Microsoft Digital Crimes Consortium, and elsewhere. The CA study was presented to the European Commission. The DPI study led to interactions with the

[1] By myself and other coauthors (Table 1.1) in a collaborative effort.

Dutch telecom regulator (ACM), the Canadian telecom regulator, and the U.S. Federal Communications Committee (FCC). The studies were also all featured in the media and on technology sites, such as the BBC, MIT Technology Review, ArsTechnica, and Slashdot. This further shows that the approach, produces timely, relevant and innovative insights.

The chapter ends with limitations and future work.

8.1 Summary of the Empirical Findings

Chapter 3 examined at the role of ISPs in mitigating botnets. Mitigating botnets has turned out to be a decade long challenge. Different countermeasures have been proposed and tried with varying levels of success. Yet botnets remain a significant security threat and the platform for many forms of cybercrime. At the time I started my research in this field, there were proposals for ISPs to undertake botnet mitigation directly, partly because they were seen as natural control points. Our study assessed this claim empirically; and further asked whether ISPs differed in infection rates and mitigation efforts; and if so, what explains the difference?

The final version of the study used two global and longitudinal datasets of botnet activity (consisting of approximately 150 and 300 million unique IP addresses) to estimate infection rates for ISPs in sixty countries. We found that well-established ISPs in relatively well-governed jurisdictions control the bulk of the bots. There are dramatic differences in infection rates among the ISPs, suggesting they have discretion to enhance mitigation. Large ISPs have lower infection rates, pointing to the role of automation in handling infection reports and lowering the cost per cleanup. We also found evidence that regulatory involvement incentivizes ISPs to spend more efforts on mitigation.

In light of these findings, we advocated, along with several other academic and industry groups, for public-private initiatives to further reduce the cost of mitigation: "a centralized and shared clearinghouse might be an efficient way to improve the intelligence that ISPs are using to protect their networks and customers" (Van Eeten et al. 2011). Several countries have since launched new Anti-Botnet Initiatives, including AbuseHUB in Netherlands

Chapter 4 looked at the success of national ABIs in cleanup of Conficker bots. Conficker is one of the largest botnets ever seen, and despite successful efforts in reverse engineering its code, releasing software patches, and dismantling the attackers' command-and-control infrastructure, hundreds of thousands of bots remain infected. We transformed six years of noisy sinkhole data into parameters that capture infection trends across 62 countries; and determined whether countries with ABIs had different growth, peak, or decay rates. Our main finding was sobering: institutional factors seemed to overwhelm ABI efforts. The two institutional factors that we checked, namely the general level of ICT development and the prevalence of unlicensed software, influenced Conficker spread and mitigation more than ABIs.

Using ABIs as a solution to reduce infections turns out to be more complex than earlier thought: regulatory involvement and reducing mitigation costs helps, but the cleanup success hinges on a number of additional factors. ISPs participating in ABIs pointed out that some users infected with Conficker do not respond to notifications, and cleanup is hard for those that do. This suggests that improved notifications as well as simplified and automatic clean-up tools are an important area to expand research efforts. Additionally, the effects of institutional factors suggest cybersecurity capacity building is an important foundational policy.

Chapter 5 studied vulnerabilities in the Certificate Authority ecosystem and reflected on proposed technical and legal fixes. CAs sell the digital certificates used to encrypt Internet communications. In 2011, an extensive breach at the Dutch CA DigiNotar highlighted a systematic vulnerability. Attackers had successfully issued malicious certificates for websites such as Google, even though Google had no relationship with DigiNotar. A single breached CA can be used to compromise the security of any website in the world that relies on certificates for encrypted connections. In other words, the security of the entire ecosystem depends on the weakest link, i.e., the most vulnerable CA. This led us to examine the security incentives of CAs by analyzing two datasets that had collected all TLS/SSL certificates on the public web (approximately 1.5 and 3 million certificates).

We found many CAs and several hundred organizations that issue certificates trusted by browsers. Yet the market is highly concentrated, with three companies controlling 75% of the market globally. We collected certificate prices from websites. We found surprisingly large price differences for identically secure certificates, up to a factor of ten, with the more expensive brands having larger market shares. This indicates information asymmetries and perverse incentives at work, with the major CAs benefiting from the systemic vulnerabilities. Our analysis showed an interesting interplay between vulnerabilities inherent in the technology, incentives of the market players, and how regulation would potentially change the incentives. We concluded that without a technical fix, the incentives would not align, so regulation—such as the E.U. Regulation No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market—cannot alone improve certificate security. Some proposed technical fixes have higher chances of improving security, but adoption has so far stalled.

Chapter 6 studied the use of Deep Pack Inspection (DPI) by ISPs for bandwidth management. Intermediaries are sometimes encouraged to take on security measures that present their own challenges and controversies. The use of DPI is one such example. DPI gives ISPs the capability to block, slow down, or prioritize Internet traffic based on content. This is a major shift from traditional Internet routing; it enables ISPs to manage their network capacity better; it also allows blocking politically undesirable content. DPI has been controversial, tying directly into Internet governance issues such as network neutrality, intellectual property, censorship, privacy, and cybersecurity. We investigated the extent to which DPI was used, given this backdrop; what factors drove its adoption across 46 countries; and whether the commercial incentives of ISPs to manage bandwidth outweighed the regulatory and public concerns about privacy.

We processed logs of a crowd-sourced test that determines whether ISP's use DPI to restrict peer-to-peer file sharing (approximately 800,000 tests). We found that despite the public and regulatory unease, more than two thirds of the ISPs used DPI, at least for bandwidth management. Using multivariate modelling, we further found that DPI use was somewhat lower in countries with better privacy safeguards, and higher in countries with Internet filtering. The latter are however not causally linked. Internet filtering, even when done using DPI, does not necessitate bandwidth management. The fact that they are correlated suggests that some ISPs piggybacked on the norm of interfering with network traffic for their own agenda. We also observed that, similar to the botnet study, ISPs have considerable discretion. DPI varied significantly, even among ISPs that operate in the same country, i.e., under similar market and regulatory conditions.

8.2 Reflections on Analyzing Security Measurements

There is a wealth of literature on statistics and data science that serves as a starting point for any quantitative empirical research. Many resources teach how to store, process, or visualize data, as well as how to make inferences. But advanced tools are only the beginning. Given that all analysis contains assumptions and approximations, considerable rigor is required for the work to stand up to scrutiny by peers and industry practitioners with first-hand knowledge.

I reflect, as an answer to part one of the research question, on what I have learnt about analyzing security measurements during the PhD research.

First, on the Use of Secondary Data. Let me briefly weigh the pros and cons of using secondary data—that is measurements gathered by others, versus collecting one's own. Running measurements allows more freedom in what can be researched, and removes the need to make sense of the work of others. Using secondary data is however often more practical for policy research. For one, while doing Internet measurements correctly is hard and can be the sole subject of many dissertations, it is only the starting point of policy research. Another is that measurements starting today cannot answer longitudinal questions for a while, which is critical for many policy questions.

Measurement-sets also need to have certain features be usable for policy research. *Chapter 7* reflected on this issue and highlighted some challenges of using secondary data. It proposed five guidelines for measurement projects to be accessible to a wider range of researchers.

Second, on Understanding the Measurement and its Biases. Analyzing measurements start with understanding what it measures, what that represents, and what biases it holds. This requires initial processing of the raw measurement data into a format that can be visualized. Plotting distributions, time trends, and scatter plots helps reveal regions and times that are outliers, or have some other unusual pattern. One needs to understand what drives these in order to decide what to do about them. Very little is known beforehand about distributions, statistical properties, and other aspects of many measurements—in contrast with well-established datasets in more mature fields such as macroeconomics or psychometrics. Asking the measurement data owners and triangulating with other datasets can help reveal bias. Anomalies and differences invite further inspection, as all measurements have biases. It. The key question is how a bias affects findings. Sometimes, filtering data helps. Other times, answering a question through multiple datasets can help distinguish noise from robust patterns.

Understanding bias is an iterative process that needs to be repeated after other steps.

Third, on Mapping Technical Identifiers to Real World Entities. Most datasets require mapping measurements to the world of firms, markets and institutions. This step is where many unacceptable shortcuts are made. Initial database lookups are often used to aggregate technical identifiers to a higher level, e.g. IP addresses to ASes. These lookups ought to be done with historical data (from the time of the measurement) to ensure accuracy. Next is mapping technical identifiers to real world entities, e.g. ASes to companies. My experience is that this requires manual effort. Automated text matching or machine learning techniques fall short for two reasons. Human mistakes or negligence means databases such as WHOIS and the likes have inaccuracies. More importantly, due to historical trajectories, companies interpret and adopt network policies differently. ISPs for instance differ in whether they use a single AS or multiple smaller ones, and in how they fill registry data. Similarly, the German organization DFN is the only CA worldwide to have created a separate sub-CA for each participating university; they argue that others have misunderstood the standard. Intermediaries within a geographical proximity or at a similar scale are more likely to have similar policies. But there is no global well-defined behavior. Some researchers solve this issue by deferring to the literature on technical standards and RFCs. This is theoretically correct, but divorces the analysis from the necessary empirical accuracy—needed for policy research. Since manual mapping is time consuming, a selection strategy on entities to include might be needed. For instance, limiting the number of countries instead of using all ISO codes.

I developed two mapping tools in the course of this dissertation that are now used by other cybersecurity researchers. One is *pyasn,* a tool to determine which autonomous system historically owned an IP address (see Appendix A). The other is an *AS-to-ISP-map* that links these technical entities to legal entities.

Fourth, on Developing Comparative Metrics. Next, we typically develop a comparative metric (or dependent variable) for the entities under study. The simplest method is to count and normalize. This involves choices about the time window, aggregation level, and so forth— which need to match the research question. As an example, for the Conficker botnet, we counted *unique* IPs seen on *average* per *hour* over each *week*. This is very different from counting unique IPs over the week. Importantly, both numbers are inaccurate approximations of the number of Conficker bots; for our purpose only the first is acceptable (see chapter 4). Normalization plays a similarly important role in comparative metrics. A larger ISP will have more bots simply due to its larger number of customers. As obvious as it sounds, a surprising number of studies do not normalize, often due to lack of a good data for the denominator. At the end of this stage, we have a dataset ready for statistical analysis.

Fifth, on Common Statistical Mistakes. Despite being a well-known concept in statistics, predictive and explanatory models are often confused in modelling security measurements. Papers too often boast regression models with very high predictive power ($R^2{>}0.90$) obtained by including the kitchen sink as a predictor. For policy research, a model is *only* reasonable if the relations can be causally interpreted and the relationships hold over sufficiently long time periods. The bulk of the impressive predictive models in computer science concern very short time frames. Think of the well-known example of Google predicting the outbreak of a flu epidemic. The early detection predates existing CDC reports by only 1-2 weeks (Ginsberg et al. 2009). Some of these issues are similar to the correlation-versus-causation discussion, which has been reinvigorated by the emergence of so-called Big Data. Correlation is effective in its own right, even without a clear causal model. But for policy, we need to understand larger patterns that hold over longer time frames, and that can be understood as a causal process, where influencing causes leads in a comprehensible way to a desired effect. A factor contributing to bad explanatory models is the scarcity of independent variables to explain entities. Some country level indicators are available from established sources (e.g. Worldbank and ITU) as well as newer projects attempting to fill the void (e.g. the Web Index); I recommend again not shying away from manually encoding or extracting variables from other sources.

Other common statistical errors include ignoring the distribution of the dependent variable in regression analysis; and reporting point estimates and significance instead of confidence intervals.[2] Partially at fault is the outdated statistics education that many graduate students still receive. The reader is referred to Gill and Meier (2000), Gill (2000), Ziliak and McCloskey (2004), and Schrodt (2014) for discussions of these topics.

Sixth, on Inferences from Basic Patterns. Some of the most powerful insights in all my studies have come from descriptive statistics and basic patterns, as opposed to complex regression models. Basic patterns are easy to validate—whether a pattern is surprising or expected; robust or stochastic; or even indicative of an error. They are however often underappreciated, perhaps because they are methodologically unsexy – i.e., they require no sophistication modelling, let alone a new contribution to that field. Familiarity with the economics and governance literature are required to make inferences from basic patterns, e.g., what a concentration pattern or sample variance reveals.

Seventh, on Seeking Expert Feedback. Even though obtaining 100% certainty is not possible, academic peers and industry experts alike will be convinced if you can show that an analysis has been executed rigorously during all steps, and that it has revealed valuable insights. Presenting the findings to industry experts and asking for their feedback can act as an assessment. It can also reveal alternative explanations and new insights.

If some points seemed trivial, it is due to the multidisciplinary nature of cybersecurity research: applying well-established tools and ideas of one discipline in another. Social scientists wishing to use security measurements ought to learn the technical details as much as possible, including how to use many of the data analysis tools. Computer scientists wishing

[2] For a parody example, see xkcd: Significant (https://xkcd.com/882).

to do policy research ought to learn principles of quantitative social research.

8.3 Implications for Cybersecurity Policy

Each of the four studies answered the second part of the research question in its own way. The studies linked intermediary behavior to, among other things, specific public policies. In this section, I reflect on whether the findings support or refute policy options suggested in the literature, and what general lessons can be drawn for cybersecurity policy.

Policy Instruments from the Economics of Information Security Literature

As we saw in chapter 2, the economics of information security literature suggests a positive role for Internet intermediaries, based on arguments such as centrality, access to users, and technical competency. Our studies provide empirical support for this role: ISPs and CAs have significant influence (collectively) and discretion (individually) on cybersecurity outcomes, as evidenced by noticeable differences among them in similar markets. Influence and discretion are two necessary conditions for policy efforts to be effective. Next comes the question of what policies can incentivize the intermediaries to provide better security? The literature suggests seven generic policies to correct incentives that are misaligned due to *information asymmetries* and *externalities*. We review them here in light of the findings of the studies.

Security breach notification (SBN) aims to minimize the damage after a breach has occurred and to provide incentives for organizations to invest in information security upfront. The CA study discussed this option, and the DigiNotar case highlights the importance of informing the public for their protection. However, the scope of SBNs (and their siblings, data breach notifications) are typically narrow. They involve informing only regulators and directly affected customers. In this case, this would not include the victims of the fraudulent certificate attacks (Google and Gmail users). Solutions such as certificate transparency would work better than breach notification, as they can directly monitor and inform about the use of fraudulent certificates. In the botnet case, SBNs and DBNs might indirectly impact enterprise owners of infected machines, but they do not concern the ISPs doing notification. So, given their normal scope, SBN/DBN wouldn't help these challenges.

Responsible vulnerability disclosure encourages security research and incentivizes software and IT vendors to provide timely security patches for their software. Our empirical studies did not focus on software platform intermediaries. The intermediaries that we did study, that is ISPs and CAs, operate services rather than develop software. That being said, the Conficker study highlights an interesting point: the availability of patches (a key goal of responsible disclosure) is only half the story, and making sure the security patches are applied in timely manner is as critical. So, neither refuted or supported by our studies, we do observe that for this policy option to be effective, complimentary incentives need to be put in place towards other actors.

Certification schemes are used to reduce information asymmetry between producers and consumers and guarantee quality in many markets. Certifications however have limits when it comes to Internet security. In the CA study, we saw that DigiNotar was audited yearly, and despite this, failed miserably at security. This was because the audits focus on paperwork and compliance, rather than verifying the operational practices of security. So in short, not an effective policy option.

Publishing security reputation metrics found support in two of our studies. We presented detailed botnet infection rates to the Dutch ISPs as part of a study. One ISP had been consistently doing worse than others. In the quarter following the report, we observed this ISP improved considerably. The benchmarks seem to have incentivized security, possibly through self-awareness or peer-pressure (Tang et al. 2013). In the DPI study, publication of DPI scores led to regulatory and media attention to ISP behavior, and starting a dialogue that can lead to change. Making reliable metrics is however difficult, due to technical limitations (see 8.2) and the potential for strategic behavior. Nevertheless, it is a very promising avenue.

Cyber insurance has been suggested both as a way to reduce externalities (harms resulting from an attack), and to incentivize good security practices (to receive lower premiums). It seems unlikely insurance fits the security problems we have studied: insurers are understandably reluctant to cover the interdependent risk associated with a CA breach or malware outbreak. For example, consider harms to many Google's users from the DigiNotar breach, or the cascading harms that malware infected machines can do. Shetty et al. (2010) Böhme and Schwartz (2010) discuss cyber insurance in more depth; in short, it does not seem an effective policy option.

Liability assignment would have limited positive effects in the challenges studied. For CAs, as elaborated in section 5.6, strict enforcement will most possibly lead to liability shielding through subsidiary companies; moreover, the weakest-link problem means that the ecosystem remains at the mercy of the worst CA in any jurisdiction, so the gains would be modest at best. In the case of botnets, one could think of assigning liability to different actors, but none are satisfactory. The vendor of the exploited software could be liable if a timely patch is not released; the ISP could be made liable if bot infected customers aren't notified in time. But as the Conficker study showed, patches and notifications aren't enough, if end-users don't apply the patches. One could assign liability to end-users, but they are often victims, and enforcement at that level would be extremely difficult. Fryer et al. (2013) discuss intermediary liability more thoroughly. In short, not an effective policy option.

Law enforcement entails capturing those behind malware attacks or CA hacks. This disincentivize future criminals, and potentially benefits the ecosystem. In the case of Conficker, the botnet operators were arrested in 2012. This slowed the growth of the botnet, and made it effectively harmless. But the arrests did not cleanup infections, and unpatched machines became victims of GameoverZeus. In other words, while law enforcement is important, it does not affect the role of intermediaries.

In summary, the studies give strong support to one of the generic policies (publishing metrics); one policy (SBN) depends on the details; three policies (insurance, liability, and certifications) will not have a positive effect in the studied challenges; and two policies (law enforcement and vulnerability disclosure) do not directly apply. This list suggests that the literature is underdeveloped with regards to the policy options: although the concepts of information asymmetries and externalities are very powerful and generate relevant insights, the findings do not fit well with the generic policy proposals.

Policy Instruments from the Broader Governance Literature

What broader policy lessons can we draw from the incentive structures uncovered for cybersecurity governance?

First, intermediaries such as ISPs and CAs are control points for many cybersecurity challenges and are possible intervention targets. The literature predicts this based on arguments such as the intermediaries control over resources and access to millions of users. We found considerable market *concentration* in the studied markets—i.e. a limited number of key actors. And that actors have *discretion* over security outcomes.

Second, we see a positive business case for collective action in some cases. In particular, the strongest incentive for security action by intermediaries appears to be *protecting corporate reputation*—be it among peers, in front of the regulator, or for their customers. The reputation incentive can be invoked by the regulator via developing and publishing security and transparency metrics. Conversely, although reputation incentives firms to improve their security individually, it will not improve the ecosystem's security when there is a technological weakest-link problem (e.g. for CAs).

Third, the regulator and policymaker have a number of instruments to stimulate informal, decentralized enforcement by private parties. These include *regulatory guidance* (also known as the 'shadow of hierarchy'), invoking laws such as 'duty to care' for customers, and financial partnerships to absorb some of the costs of intermediary efforts. The details of the approach matters. For instance, in the botnet mitigation study, we found that regulatory attention (as captured by LAP membership) encourages ISPs to act; in the follow up study we found the effectiveness of ABIs depended on extra conditions not initially anticipated.

Fourth, the regulator and policymaker should *engage critically* with arguments referencing constraints against action. While some ISPs had raised privacy "constraints" for not implementing security countermeasures in the past, the majority of ISPs reinterpret such constraints as mere "considerations" when their commercial incentives align with the technology, as in the case of DPI-based bandwidth management. Another argument that needs to be reassessed is that, since cybersecurity issues are transnational in nature, national-level policies will not work. We have found that national regulators had considerable impact in both the botnets and DPI studies.

Using the conceptual framework of government tools defined by Hood and Margetts (2007), we can summarize the implications of our findings as follows: authority is a key tool, nodality and treasure play some role, and organization little. Authority gives the government the ability to determine what is expected and engage with intermediaries (as explained in #3 and #4). Understandably governments have been conservative in using this power with regards to the Internet, as they do not want to 'break' the Internet. A large risk is for the regulator to codify perverse incentives, unintentionally or due to capture, as was highlighted in the network-neutrality debates in the U.S. and Canada (section 6.6).

Nodality denotes the property of being in the middle of an information network and equips government with the ability dispense information, e.g. reputation metrics (#2). I state 'some' role however, as the intermediaries have more nodality than the government in the networked world. Treasure can reduce the cost of certain measures and incentivize scaling up efforts. But it's role is limited, as many intermediaries run profitable businesses with adequate margins. The organizational power of government is least useful, as the intermediaries often have much better technical capabilities and are apt at using IT automation for efficiency. The treasure and organization tools of government can come in handy in the long-run by helping train cybersecurity talent.

More generally speaking, there are many parallels between the governance of cybersecurity and other large-scale, globalized, socio-technical systems such as the environment or financial sectors. Many challenges, dilemmas, and questions are shared, including for instance the move from self-regulation to more hybrid forms of regulation (Groenleer et al. 2014). Such meta-connections are points for further research and fall out of the scope of this dissertation.

In conclusion, cybersecurity can be improved by understanding and aligning the economic incentives of Internet intermediaries. This is actionable for policymakers and regulators, and may be more effective than alternatives such as raising awareness among consumers and businesses, or mandating specific technical solutions. The mechanisms for alignment need not be law; softer mechanisms such as regulatory guidance, or facilitating positive or negative reputation effects may work better in some situations. In each case, measuring, analyzing, and understanding the properties of these markets and the incentives of its players is critical to developing effective cybersecurity policies.

8.4 Future Work

The dissertation consists of several standalone studies. The limitations of each study is discussed at length in its own chapter. This concerns both validity of measurements and the overall analysis (Van der Velde, Jansen, and Anderson 2004). Broadly stated, the studies can be extended in two ways. First is improve the quality of the data—both concerning measurements that capture the phenomena of interest, and the independent variables for intermediary characteristics and environment. This requires collaboration among scholars and experts from diverse fields. Second is to use other statistical instruments. During the PhD research, I gradually advanced towards more suited statistical instruments, e.g., from pooled OLS regressions to time-series and GLM regressions. There are other statistical instruments and empirical methods that could yield better results, in particular with regards to determining causality.

Analysis of behavior is a contested topic in economics. The approach undertaken in this dissertation has interestingly enough received criticisms from both sides of the spectrum. At least one neoclassical economist called it "great research, but not economics", due to lack of formal analysis; and at least one heterodox economist suggested that 'understanding' cannot be claimed without an in-depth case study and direct observation of behavior. While both criticisms in their own way outline the limitations of the undertaken approach, the case studies have demonstrated that novel and substantial insights about behavior of intermediaries can be derived from Internet measurements. This approach has its own strengths and weaknesses vis-a-vis the more established bodies of research in orthodox and heterodox economics.

Standalone studies have drawbacks regarding overall generalizability, notwithstanding the general issue of generalizability in social sciences (Little 1993; Bernstein et al. 2000). This dissertation looks at only two intermediaries and four cybersecurity challenges among many critical issues. Other intermediaries, such as hosting providers, registrars, cloud providers, payment service providers, and social network operators, seem eminently suitable for follow-up research along the path mapped out by this thesis.

A final area of expansion is researching the systematic design of cybersecurity policies, and the links between governance of cybersecurity and other large-scale, globalized, socio-technical systems.

References

Advanced Cyber Defence Centre. 2014. "Support Centers - Advanced Cyber Defence Centre (ACDC)." Accessed December 2, 2014. http://www.acdc-project.eu/?page_id=55.

Akerlof, George A. 1970. "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism." *The Quarterly Journal of Economics* 84 (3): 488–500.

Anderson, Jonathan, Joseph Bonneau, and Frank Stajano. 2010. "Inglorious Installers: Security in the Application Marketplace." Paper presented at the Ninth Workshop on the Economics of Information Security (WEIS 2010), June 7-8, Harvard University. http://www.econinfosec.org/archive/weis2010/papers/session3/weis2010_anderson_j.pdf.

Anderson, Ross. 2001. "Why Information Security Is Hard - an Economic Perspective." In *17th Annual Computer Security Applications Conference (ACSAC 2001)*, 358–65. doi:10.1109/ACSAC.2001.991552.

———. 2008. *Security Engineering: A Guide to Building Dependable Distributed Systems*. 2nd ed. Tokyo, New York: Wiley.

Anderson, Ross, Chris Barton, Rainer Böhme, Richard Clayton, Michel J.G. van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. 2013. "Measuring the Cost of Cybercrime." In *The Economics of Information Security and Privacy*, edited by Rainer Böhme, 265–300. Berlin and Heidelberg: Springer. doi:10.1007/978-3-642-39498-0_12.

Anderson, Ross, Rainer Böhme, Richard Clayton, and Tyler Moore. 2008. "Security Economics and the Internal Market." Study commissioned by the European Union Agency for Network and Information Security (ENISA). http://www.enisa.europa.eu/publications/archive/economics-sec.

Anderson, Ross, and Tyler Moore. 2006. "The Economics of Information Security." *Science* 314 (5799): 610–13. doi:10.1126/science.1130992.

Apple. 2013. "Apple - Root Certificate Program." Accessed February 1, 2013. http://www.apple.com/certificateauthority/ca_program.html.

Arnbak, Axel, Hadi Asghari, Michel J.G. Van Eeten, and Nico Van Eijk. 2014. "Security Collapse in the HTTPS Market." *Communications of the ACM* 57 (10): 47–55.

Arnbak, Axel, and Nico Van Eijk. 2012. "Certificate Authority Collapse: Regulating Systemic Vulnerabilities in the HTTPS Value Chain."

Paper presented at the 40th Research Conference on Communication, Information and Internet Policy (TPRC 2012), September 21-23. doi:10.2139/ssrn.2031409.

Arora, Ashish, Ramayya Krishnan, Rahul Telang, and Yubao Yang. 2010. "An Empirical Analysis of Software Vendors' Patch Release Behavior: Impact of Vulnerability Disclosure." *Information Systems Research* 21 (1): 115–32. doi:10.1287/isre.1080.0226.

Asghari, Hadi, and Arman Noroozian. 2014. *Python IP Address to Autonomous System Number Lookup Module.* (version 1.5). https://github.com/hadiasghari/pyasn.

Asghari, Hadi, Michel J.G. Van Eeten, Axel Arnbak, and Nico Van Eijk. 2013. "Security Economics in the HTTPS Value Chain." Paper presented at the Twelfth Workshop on the Economics of Information Security (WEIS 2013), June 11-13, Washington, DC. doi:10.2139/ssrn.2277806.

Asghari, Hadi, Michel J.G. Van Eeten, and Milton L. Mueller. 2012. "Unraveling the Economic and Political Drivers of Deep Packet Inspection." Paper presented at the GigaNet 7th Annual Symposium, November 5, Baku, Azerbaijan. doi:10.2139/ssrn.2294434.

August, Terrence, and Tunay I. Tunca. 2011. "Who Should Be Responsible for Software Security? A Comparative Analysis of Liability Policies in Network Environments." *Management Science* 57 (5): 934–59. doi:10.1287/mnsc.1100.1304.

Bakos, Yannis, Florencia Marotta-Wurgler, and David R. Trossen. 2009. "Does Anyone Read the Fine Print? Testing a Law and Economics Approach to Standard Form Contracts." Working Paper #09-04. NET Institute Working Papers Series. Fourth Annual Conference on Empirical Legal Studies. http://hdl.handle.net/2451/29503.

Bendrath, R., and M. L. Mueller. 2011. "Deep Packet Inspection and Internet Governance. The End of the Net as We Know It?" *New Media and Society* 13 (7): 1142–60. doi:10.2139/ssrn.1653259.

BEREC. 2012. "A View of Traffic Management and Other Practices Resulting in Restrictions to the Open Internet in Europe: Findings from BEREC's and the European Commission's Joint Investigation." BoR (12) 30. Body of European Regulators for Electronic Communications. http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=2039.

Bernstein, Steven, Richard Ned Lebow, Janice Gross Stein, and Steven Weber. 2000. "God Gave Physics the Easy Problems: Adapting Social Science to an Unpredictable World." *European Journal of International Relations* 6 (1): 43–76. doi:10.1177/1354066100006001003.

Bevir, Mark. 2012. *Governance: A Very Short Introduction*. Oxford: Oxford University Press.

Böhme, Rainer. 2005. "Cyber-Insurance Revisited." Paper presented at the Fourth Workshop on the Economics of Information Security

(WEIS 2005), Harvard University. http://infosecon.net/workshop/pdf/15.pdf.

———. 2010. "Security Metrics and Security Investment Models." In *Advances in Information and Computer Security*, 10–24. Springer. doi:10.1007/978-3-642-16825-3_2.

Böhme, Rainer, and Tyler Moore. 2009. "The Iterated Weakest Link - A Model of Adaptive Security Investment." Paper presented at the Eight Workshop on the Economics of Information Security (WEIS 2009), June 24-25, University College London. https://www.is.uni-muenster.de/security/publications/BM2009_IteratedWeakestLink_WEIS.pdf.

Böhme, Rainer, and Galina Schwartz. 2010. "Modeling Cyber-Insurance: Towards a Unifying Framework." presented at the Ninth Workshop on the Economics of Information Security (WEIS 2010), June 7-8, Harvard University. http://www.icsi.berkeley.edu/pubs/networking/modelingcyber10.pdf.

Bonneau, Joseph. 2014. "Fixing New Models for Distributing Transport Security Policy." Seminar presented at the Center for Information Technology Policy (CITP) at Princeton University. https://docs.google.com/presentation/d/dxWwKUOVjO1MnOJQkyxCS03VfFp_kmPeAmneJ9KLdM/edit?usp=sharing.

Bonneau, Joseph, Cormac Herley, Paul C Van Oorschot, and Frank Stajano. 2012. "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes." In *IEEE Symposium on Security and Privacy (SP) 2012*, 553–67. doi:10.1109/SP.2012.44.

Bradbury, Danny. 2014. "Testing the Defences of Bulletproof Hosting Companies." *Network Security* 2014 (6): 8–12.

Branscomb, Anne W. 1994. *Who Owns Information?: From Privacy to Public Access*. New York: Basic Books.

Bravo-Lillo, C., L.F. Cranor, J.S. Downs, and S. Komanduri. 2011. "Bridging the Gap in Computer Security Warnings: A Mental Model Approach." *IEEE Security and Privacy* 9 (2): 18–26. doi:10.1109/MSP.2010.198.

Brecht, Matthias, and Thomas Nowey. 2013. "A Closer Look at Information Security Costs." In *The Economics of Information Security and Privacy*, edited by Rainer Böhme, 3–24. Berlin and Heidelberg: Springer.

Brown, Ian, and Christopher T. Marsden. 2013. *Regulating Code: Good Governance and Better Regulation in the Information Age*. Cambridge, MA: MIT Press.

Camp, L Jean. 2013. "Beyond Usability: Security Interactions as Risk Perceptions." Paper presented at the Workshop on Risk Perception in IT Security and Privacy, Newcastle, UK. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.385.7530&rep=rep1&type=pdf.

Canali, Davide, Davide Balzarotti, and Aurélien Francillon. 2013. "The Role of Web Hosting Providers in Detecting Compromised Websites." In *Proceedings of the 22nd International Conference on World Wide Web (WWW'13)*, 177–88. http://dl.acm.org/citation.cfm?id=2488388.2488405.

Cavusoglu, Huseyin, Birendra Mishra, and Srinivasan Raghunathan. 2004. "A Model for Evaluating IT Security Investments." *Communications of the ACM* 47 (7): 87–92. doi:10.1145/1005817.1005828.

Chen, Min, Varghese S. Jacob, Suresh Radhakrishnan, and Young U. Ryu. 2012. "The Effect of Fraud Investigation Cost on Pay-Per-Click Advertising." Paper presented at the Eleventh Workshop on the Economics of Information Security (WEIS 2012), June 25-26, Berlin. http://weis2012.econinfosec.org/papers/Chen_WEIS2012.pdf.

Christin, Nicolas. 2013. "Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace." In *Proceedings of the 22nd International Conference on World Wide Web (WWW '13)*, 213–24. http://dl.acm.org/citation.cfm?id=2488388.2488408.

Clayton, Richard. 2011. "Might Governments Clean-up Malware?" *Communication and Strategies*, no. 81: 87–104.

Colander, David. 2005. "The Making of an Economist Redux." *The Journal of Economic Perspectives* 19 (1): 175–98.

Constantin, Lucian. 2012. "Trustwave Admits Issuing Man-in-the-Middle Digital Certificate; Mozilla Debates Punishment." *Computerworld*, February 8. http://www.computerworld.com/s/article/9224082/Trustwave_admits_issuing_man_in_the_middle_digital_certificate_Mozilla_debates_punishment.

Cooper, Matt, Yuriy Dzambasow, Peter Hesse, Susan Joseph, and Richard Nicholas. 2005. "Internet X.509 Public Key Infrastructure: Certification Path Building." RFC 4158. Internet Engineering Task Force. http://tools.ietf.org/html/rfc4158.

CSIS, and McAfee. 2014. "Net Losses: Estimating the Global Cost of Cybercrime." Accessed July 14, 2015. http://www.cyberriskinsuranceforum.com/sites/default/files/pictures/rp-economic-impact-cybercrime2.pdf.

CVE. 2015. "Common Vulnerabilities and Exposures List Master Copy." Accessed July 7, 2015. https://cve.mitre.org/cve/cve.html.

Davenport, Thomas H, and John C Beck. 2001. *The Attention Economy: Understanding the New Currency of Business*. Boston, MA: Harvard Business School Press.

Demetz, Lukas, and Daniel Bachlechner. 2013. "To Invest or Not to Invest? Assessing the Economic Viability of a Policy and Security

Configuration Management Tool." In *The Economics of Information Security and Privacy*, edited by Rainer Böhme, 25–47. Berlin and Heidelberg: Springer.

Department of Justice, and Federal Trade Commission. 2010. "Horizontal Merger Guidelines." Issued August 19, 2010. http://www.justice.gov/atr/horizontal-merger-guidelines-08192010.

Diekman, Odo, and Hans (J.A.P.) Heesterbeek. 2000. *Mathematical Epidemiology of Infectious Diseases: Model Building, Analysis and Interpretation*. Chichester: John Wiley & Sons.

Dischinger, Marcel, and Krishna P. Gummadi. 2011. "Glasnost: Results from Tests for BitTorrent Traffic Shaping." *Max Planck Institute for Software Systems, Glasnost Project*. November 28. http://broadband.mpi-sws.org/transparency/results/.

Dischinger, Marcel, Massimiliano Marcon, Saikat Guha, Krishna P. Gummadi, Ratul Mahajan, and Stefan Saroiu. 2010. "Glasnost: Enabling End Users to Detect Traffic Differentiation." In *Proceedings of the 7th Symposium on Networked Systems Design and Implementation (NSDI '10)*. http://static.usenix.org/events/nsdi10/tech/full_papers/dischinger.pdf.

Dredge, Stuart. 2015. "MySpace – What Went Wrong: 'The Site Was a Massive Spaghetti-Ball Mess.'" *The Guardian*. March 6. http://www.theguardian.com/technology/2015/mar/06/myspace-what-went-wrong-sean-percival-spotify.

Durumeric, Zakir, James Kasten, Michael Bailey, and J Alex Halderman. 2013. "Analysis of the HTTPS Certificate Ecosystem." In *Proceedings of the 2013 Conference on Internet Measurement Conference (IMC '13)*, 291–304.

Eckersley, Peter. 2011. "Iranian Hackers Obtain Fraudulent Certificates: How close to a Web Security Meltdown Did We Get?" *Electronic Frontier Foundation Blog*. March 23. https://www.eff.org/deeplinks/2011/03/iranian-hackers-obtain-fraudulent-https.

Edelman, Benjamin. 2011. "Adverse Selection in Online 'trust' Certifications and Search Results." *Electronic Commerce Research and Applications* 10 (1): 17–25.

Edwards, Benjamin, Steven Hofmeyr, and Stephanie Forrest. 2015. "Hype and Heavy Tails: A Closer Look at Data Breaches." Paper presented at the Fourteenth Workshop on the Economics of Information Security (WEIS 2015), June 22-23, Delft University of Technology, The Netherlands. http://www.cs.unm.edu/~forrest/publications/weis-data-breaches-15.pdf.

Elgin, Ben, Michael Riley, and Dune Lawrence. 2014. "Home Depot Hacked After Months of Security Warnings." *Businessweek*, September 18. http://www.bloomberg.com/bw/articles/2014-09-18/home-depot-hacked-wide-open.

ENISA. 2011. "Operation Black Tulip: Certificate Authorities Lose Authority (version 2)." *European Union Agency for Network and Information Security*. December 5. http://www.enisa.europa.eu/media/news-items/operation-black-tulip.

ESET. 2014. "Threat Radar (June 2014) Feature Article: The Increasingly Strange Case of the Antipodean iOS Ransomware." Bratislava (Slovakia): ESET. http://www.eset.com/us/resources/threat-trends/Global_Threat_Trends_June_2014.pdf.

European Commission. 2013. "FP7 - ICT Projects in Trust & Security." June 12. http://cordis.europa.eu/fp7/ict/security/projects_en.html.

European Parliament. 2014. "European Parliament Legislative Resolution of 3 April 2014 on the Proposal for a Regulation of the European Parliament and of the Council on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (COM(2012)0238 – C7-0133/2012 – 2012/0146(COD))." T7-0282/2014. European Parliament. http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1442676385193&uri=URISERV:310603_1.

Evans, Chris, Chris Palmer, and Ryan Sleevi. 2012. "Public Key Pinning Extension for HTTP." RFC 7469 Draft 04. Internet Engineering Task Force. https://tools.ietf.org/html/draft-ietf-websec-key-pinning-04.

Federal Communications Commission. 2012. "U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers (ISPs)." http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-ReportFinal.pdf.

Fershtman, Chaim, and Neil Gandal. 2012. "Migration to the Cloud Ecosystem: Ushering in a New Generation of Platform Competition." *CEPR Discussion Paper*, no. DP8907. http://ssrn.com/abstract=2034125.

Financial Fraud Action UK. 2015. "Scams and Computer Viruses Contribute to Fraud Increases - Calls for National Awareness Campaign." http://www.financialfraudaction.org.uk/news-article.asp?genre=media&Article=2885.

Florêncio, Dinei, and Cormac Herley. 2010. "Where Do Security Policies Come From?" In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS '10)*, 10:1–10:14. http://doi.acm.org/10.1145/1837110.1837124.

———. 2013a. "Sex, Lies and Cyber-Crime Surveys." In *Economics of Information Security and Privacy III*, edited by Bruce Schneier, 35–53. New York: Springer. doi:10.1007/978-1-4614-1981-5_3.

———. 2013b. "Where Do All the Attacks Go?" In *Economics of Information Security and Privacy III*, 13–33. Springer. doi:10.1007/978-1-4614-1981-5_2.

Fox-IT. 2012. "Black Tulip – Report of the Investigation into the DigiNotar Certificate Authority Breach." Version 1.0. By Hans Hoogstraaten and Others. Fox-IT. http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2012/08/13/black-tulip-update.html.

Franklin, Jason, Adrian Perrig, Vern Paxson, and Stefan Savage. 2007. "An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants." In *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07)*, 375–88. doi:10.1145/1315245.1315292.

Fryer, Huw, Roksana Moore, and Tim Chown. 2013. "On the Viability of Using Liability to Incentivise Internet Security." presented at the Twelfth Workshop on the Economics of Information Security (WEIS 2013), June 11-13, Georgetown University, Washington, DC. http://weis2013.econinfosec.org/papers/FryerMooreChownWEIS2013.pdf.

Gaynor, Martin S., Muhammad Zia Hydari, and Rahul Telang. 2012. "Is Patient Data Better Protected in Competitive Healthcare Markets?" presented at the Eleventh Workshop on the Economics of Information Security (WEIS 2012), June 25-26, Berlin. http://weis2012.econinfosec.org/papers/Gaynor_WEIS2012.pdf.

Geer, Daniel, Kevin Soo Hoo, and Andrew Jaquith. 2003. "Information Security: Why the Future Belongs to the Quants." *IEEE Security and Privacy* 1 (4): 24–32.

Gill, Jeff. 2000. *Generalized Linear Models: A Unified Approach*. Sage University Paper Series on Quantiative Applications in the Social Sciences 07-134. Thousand Oaks, CA: Sage.

Gill, Jeff, and Kenneth J. Meier. 2000. "Public Administration Research and Practice: A Methodological Manifesto." *Journal of Public Administration Research and Theory* 10 (1): 157–99.

Ginsberg, Jeremy, Matthew H. Mohebbi, Rajan S. Patel, Lynnette Brammer, Mark S. Smolinski, and Larry Brilliant. 2009. "Detecting Influenza Epidemics Using Search Engine Query Data." *Nature* 457 (7232): 1012–14. doi:10.1038/nature07634.

Glazer, Emily. 2014. "J.P. Morgan's Cyber Attack: How The Bank Responded." *The Wall Street Jjournal MoneyBeat Blog*. October 3. http://blogs.wsj.com/moneybeat/2014/10/03/j-p-morgans-cyber-attack-how-the-bank-responded/.

Goldfarb, Avi, and Catherine Tucker. 2011. "Search Engine Advertising: Channel Substitution When Pricing Ads to Context." *Management Science* 57 (3): 458–70. doi:10.1287/mnsc.1100.1287.

Goodin, Dan. 2009. "Superworm Seizes 9m PCs, 'Stunned' Researchers Say." *The Register*, January 16. http://www.theregister.co.uk/2009/01/16/9m_downadup_infections/.

Gordon, Lawrence A, and Martin P Loeb. 2002. "The Economics of Information Security Investment." *ACM Transactions on Information and System Security (TISSEC)* 5 (4): 438–57.

Gordon, Lawrence A., Martin P. Loeb, and Lei Zhou. 2011. "The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs?" *Journal of Computer Security* 19 (1): 33–56.

Gottinger, Hans-Werner. 2003. *Economies of Network Industries*. London: Routledge.

Graves, James, Alessandro Acquisti, and Nicolas Christin. 2014. "Should Payment Card Issuers Reissue Cards in Response to a Data Breach?" Paper presented at the Thirteenth Workshop on the Economics of Information Security (WEIS 2014), College Park, PA. http://weis2014.econinfosec.org/papers/GravesAcquisti-Christin-WEIS2014.pdf.

Groenewegen, John, ed. 2007. *Teaching Pluralism in Economics*. Cheltenham, UK and Northampton, USA: Edward Elgar Publishing.

Groenleer, Martijn L.P., Arnout Mijs, Ernst Ten Heuvelhof, Bert Bert Meeuwen, and Jessica Van der Puil. 2014. "Strategic Behaviour and Crisis-Driven Change in Regulation and Governance of the European Financial and Economic System: From Networks to Hybrids." *Jerusalem Papers in Regulation & Governance Working Paper*, no. 63. http://papers.ssrn.com/abstract=2448280.

Grosse, Eric. 2012. "Security Warnings for Suspected State-Sponsored Attacks." *Google Online Security Blog*. June 5. http://googleonlinesecurity.blogspot.com/2012/06/security-warnings-for-suspected-state.html.

Hall, Rodney Bruce, and Thomas J. Biersteker. 2002. "Private Authority as Global Governance." In *The Emergence of Private Authority in Global Governance*, edited by Rodney Bruce Hall and Thomas J. Biersteker, 85:203–22. Cambridge Studies in International Relations. Cambridge: Cambridge University Press.

Hawkinson, John, and Tony Bates. 1996. "Guidelines for Creation, Selection, and Registration of an Autonomous System (AS)." RFC 1930. Internet Engineering Task Force. https://tools.ietf.org/html/rfc1930.

Herley, Cormac. 2009. "So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users." In *Proceedings of the 2009 Workshop on New Security Paradigms Workshop (NSPW'09)*, 133–44.

———. 2012. "Why Do Nigerian Scammers Say They Are from Nigeria?" presented at the Eleventh Workshop on the Economics of Information Security (WEIS 2012), June 25-26, Berlin. http://weis2012.econinfosec.org/papers/Herley_WEIS2012.pdf.

Herley, Cormac, and Dinei Florêncio. 2010. "Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground

Economy." In *Economics of Information Security and Privacy*, edited by Tyler Moore, David Pym, and Christos Ioannidis, 33–53. New York: Springer US. doi:10.1007/978-1-4419-6967-5_3.

Hoffman, Paul. 2012. "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA." RFC 6698. Internet Engineering Task Force. http://tools.ietf.org/html/rfc6698.

Hofmann, Jeanette. 2010. "The Libertarian Origins of Cybercrime: Unintended Side-Effects of a Political Utopia." *London School of Economics Discussion Paper*, no. 62. http://ssrn.com/abstract=1710773.62.

Hofmeyr, Steven, Tyler Moore, Stephanie Forrest, Benjamin Edwards, and George Stelle. 2013. "Modeling Internet-Scale Policies for Cleaning up Malware." In *Economics of Information Security and Privacy III*, edited by Bruce Schneier, 149–70. New York: Springer. doi:10.1007/978-1-4614-1981-5_7.

Holz, Thorsten, Moritz Steiner, Frederic Dahl, Ernst Biersack, and Felix C Freiling. 2008. "Measurements and Mitigation of Peer-to-Peer-Based Botnets: A Case Study on Storm Worm." In *First USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '08)*.

Hood, Christopher C., and Helen Z. Margetts. 2007. *The Tools of Government in the Digital Age*. Basingstoke, U.K.: Palgrave Macmillan.

House of Lords. 2007. "Personal Internet Security, 5th Report of Session 2006-07." HL Paper 165-I. Science and Technology Committee. London: The Stationery Office Limited. http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf.

Hurst, Ryan. 2012. "How to Tell DV and OV Certificates Apart | UNMITIGATED RISK." *Unmitigated Risk*. September 11. Accessed February 1, 2013. http://unmitigatedrisk.com/?p=203.

InfoSecurity. 2011. "Comodo Admits Two More Registration Authorities Hacked." *InfoSecurity Magazine*, March 31. http://www.infosecurity-magazine.com/view/16986/comodo-admits-two-more-registration-authorities-hacked.

Ioannidis, Christos, David Pym, and Julian Williams. 2013a. "Fixed Costs, Investment Rigidities, and Risk Aversion in Information Security: A Utility-Theoretic Approach." In *Economics of Information Security and Privacy III*, edited by Bruce Schneier, 171–91. New York: Springer.

———. 2013b. "Sustainability in Information Stewardship." presented at the Twelfth Workshop on the Economics of Information Security (WEIS 2013), June 11-13, Georgetown University, Washington, DC. http://weis2013.econinfosec.org/papers/IoannidisPymWilliamsWEIS2013.pdf.

Irwin, Barry. 2012. "A Network Telescope Perspective of the Conficker Outbreak." In *Information Security for South Africa (ISSA) 2012*, 1–8. doi:10.1109/ISSA.2012.6320455.

ITRC. 2014. "Data Bre$ch Reports." Identity Theft Resource Center. http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html.

Kanich, Chris, Christian Kreibich, Kirill Levchenko, Brandon Enright, Geoffrey M. Voelker, Vern Paxson, and Stefan Savage. 2008. "Spamalytics: An Empirical Analysis of Spam Marketing Conversion." In *Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS '08)*, 3–14. http://dl.acm.org/citation.cfm?id=1455774.

Karge, Sven. 2010. "The German Anti-Botnet Initiative." OECD Workshop, The Role of Internet Intermediaries in Advancing Public Policy Objectives. OECD. http://www.oecd.org/sti/ieconomy/45509383.pdf.

Kelkman, Olaf M. 2013. "DNSSEC Musings: DigiNotar, DANE and Deployment." Slides presented at the APNIC 35 Conference, Singapore, February 26. http://conference.apnic.net/__data/assets/pdf_file/0005/58901/dnssec-diginotar-dane_1361864377.pdf.

Kelley, Timothy, and L. Jean Camp. 2012. "Online Promiscuity: Prophylactic Patching and the Spread of Computer Transmitted Infections." presented at the Eleventh Workshop on the Economics of Information Security (WEIS 2012), June 25-26, Berlin. http://weis2012.econinfosec.org/papers/Kelley_WEIS2012.pdf.

Khattak, Sheharbano, Naurin Rasheed Ramay, Kamran Riaz Khan, Affan A. Syed, and Syed Ali Khayam. 2014. "A Taxonomy of Botnet Behavior, Detection, and Defense." *IEEE Communications Surveys & Tutorials* 16 (2): 898–924. doi:10.1109/SURV.2013.091213.00134.

Kim, Sunil, and Jun-yong Lee. 2007. "A System Architecture for High-Speed Deep Packet Inspection in Signature-Based Network Intrusion Prevention." *Journal of Systems Architecture* 53 (5): 310–20.

Kirk, Jeremy. 2011. "Ukraine Helps Disrupt $72M Conficker Hacking Ring." *CIO*, June 23. http://www.cio.com/article/2406864/intrusion/ukraine-helps-disrupt--72m-conficker-hacking-ring.html.

Kleiner, Aaron, Paul Nicholas, and Kevin Sullivan. 2014. *Linking Cybersecurity Policy and Performance*. Redmond, WA: Microsoft. www.microsoft.com/en-us/download/confirmation.aspx?id=36523.

Koivunen, Erka. 2012. "'Why Wasn't I Notified?': Information Security Incident Reporting Demystified." In *Information Security Technology for Applications*, edited by Tuomas Aura, Kimmo Järvinen, and Kaisa Nyberg, 7127:55–70. Berlin and Heidelberg: Springer Berlin Heidelberg. doi:10.1007/978-3-642-27937-9_5.

Kramer, Adam D. I., Jamie E. Guillory, and Jeffrey T. Hancock. 2014. "Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks." *Proceedings of the National Academy of Sciences* 111 (24): 8788–90. doi:10.1073/pnas.1320040111.

Krebs, Brian. 2011. "72M USD Scareware Ring Used Conficker Worm." *Krebs on Security Blog*. June 23. http://krebsonsecurity.com/2011/06/72m-scareware-ring-used-conficker-worm/.

Kuehn, Andreas, and Milton L. Mueller. 2012. "Profiling the Profilers: Deep Packet Inspection and Behavioral Advertising in Europe and the United States." *SSRN*. doi:10.2139/ssrn.2014181.

Kunreuther, Howard, and Geoffrey Heal. 2003. "Interdependent Security." *Journal of Risk and Uncertainty* 26 (2-3): 231–49.

Kwon, Juhee, and M. Eric Johnson. 2011. "An Organizational Learning Perspective on Proactive vs. Reactive Investment in Information Security." presented at the Tenth Workshop on the Economics of Information Security (WEIS 2011), June 14-15, George Mason University, Fairfax, VA. http://weis2011.econinfosec.org/papers/An%20Organizational%20Learning%20Perspective%20on%20Proactive%20vs.%20Rea.pdf.

———. 2013. "Healthcare Security Strategies for Regulatory Compliance and Data Security." In *46th Hawaii International Conference on System Sciences (HICSS 2013)*, 3972–81. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6480324.

Landau, Susan, and Tyler Moore. 2012. "Economic Tussles in Federated Identity Management." *First Monday* 17 (10). http://uncommonculture.org/ojs/index.php/fm/article/view/4254.

Langley, Adam. 2012. "Certificate Transparency." *ImperialViolet Blog*. November 6. http://www.imperialviolet.org/2012/11/06/certtrans.html.

———. 2013. "Real World Crypto 2013." *ImperialViolet Blog*. January 13. http://www.imperialviolet.org/2013/01/13/rwc03.html.

Laurie, Ben, Adam Langley, and Emilia Kasper. 2013. "Certificate Transparency." RFC 6962 Draft 12. Internet Engineering Task Force. http://tools.ietf.org/html/draft-laurie-pki-sunlight-12.

Lessig, Lawrence. 1999. *Code and Other Laws of Cyberspace*. New York: Basic books.

Levchenko, K., A. Pitsillidis, N. Chachra, B. Enright, M. Felegyhazi, C. Grier, T. Halvorson, et al. 2011. "Click Trajectories: End-to-End Analysis of the Spam Value Chain." In *IEEE Symposium on Security and Privacy (SP) 2011*, 431–46. doi:10.1109/SP.2011.24.

Lewis, James Andrew. 2005. "Aux Armes, Citoyens: Cyber Security and Regulation in the United States." *Telecommunications Policy* 29 (11): 821–30. doi:10.1016/j.telpol.2005.06.009.

Little, Daniel. 1993. "On the Scope and Limits of Generalizations in the Social Sciences." *Synthese* 97 (2): 183–207. doi:10.1007/BF01064114.

Liu, He, Kirill Levchenko, Márk Félegyházi, Christian Kreibich, Gregor Maier, Geoffrey M Voelker, and Stefan Savage. 2011. "On the Effects of Registrar Level Intervention." In *Proc. of the 4th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '11)*. https://www.usenix.org/legacy/event/leet11/tech/full_papers/Liu.pdf.

Livingood, Jason, Nirmal Mody, and Michael O'Reirdan. 2012. "Recommendations for the Remediation of Bots in ISP Networks." RFC 6561. Internet Engineering Task Force. http://tools.ietf.org/html/rfc6561.

Marlinspike, Moxie. 2013. "Trust Assertions for Certificate Keys." Edited by Trevor Perrin. Internet Engineering Task Force. http://tools.ietf.org/html/draft-perrin-tls-tack-02.

Maurer, Tim, and Robert Morgus. 2014. "Compilation of Existing Cybersecurity and Information Security Related Definitions." New America. https://www.newamerica.org/cyber-global/cyber-definitions/.

MaxMind. 2015. "GeoIP2 Country Database." Accessed September 9, 2015. https://www.maxmind.com/en/geoip2-country-database.

Menn, Joseph. 2012. "Key Internet Operator VeriSign Hit by Hackers." *Reuters*, February 2. http://www.reuters.com/article/2012/02/02/us-hacking-verisign-idUSTRE8110Z820120202.

Metcalf, Leigh B., and Jonathan Spring. 2014. "Blacklist Ecosystem Analysis Update: 2014." CERTCC-2014-82. Pittsburgh, PA: Software Engineering Institute. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=428609.

Microsoft. 2007. "Security Intelligence Report." Volume 3 (Jan-Jun 2007). By Vinny Gullotto and Others. Redmond, WA: Microsoft. http://www.microsoft.com/en-us/download/details.aspx?id=7277.

———. 2009. "Microsoft Trusted Root Certificate: Program Requirements." Accessed February 1, 2013. https://technet.microsoft.com/en-us/library/cc751157.aspx.

———. 2010. "Security Intelligence Report." Volume 9 (Jan-Jun 2010). By David Anselmi and Others. Redmond, WA: Microsoft. http://download.microsoft.com/download/8/1/B/81B3A25C-95A1-4BCD-88A4-2D3D0406CDEF/Microsoft_Security_Intelligence_Report_volume_9_Jan-June2010_English.pdf.

———. 2012a. "Security Intelligence Report: How Conficker Continues to Propogate." Volume 12 (Jul-Dec 2011). By Dennis Batchelder and Others. Microsoft. http://download.microsoft.com/download/C/9/A/C9A544AD-4150-43D3-80F7-4F1641EF910A/Microsoft_Security_Intelligence_Report_Volume_12_How_Conficker_Continues_To_Propagate_English.pdf.

———. 2012b. "Windows and Windows Phone 8 SSL Root Certificate Program (Member CAs)." *Microsoft TechNet Wiki*. December. Accessed February 1, 2013. http://social.technet.microsoft.com/wiki/contents/articles/14215.windows-and-windows-phone-8-ssl-root-certificate-program-member-cas.aspx.

———. 2015. "Security Intelligence Report." Volume 18 (Jul-Dec 2014). By Dennis Batchelder and Others. Redmond, WA: Microsoft. http://download.microsoft.com/download/7/1/A/71ABB4EC-E255-4DAF-9496-A46D67D875CD/Microsoft_Security_Intelligence_Report_Volume_18_English.pdf.

Miller, Amalia R., and Catherine E. Tucker. 2011. "Encryption and the Loss of Patient Data." *Journal of Policy Analysis and Management* 30 (3): 534–56. doi:10.1002/pam.20590.

Mills, Elinor. 2011. "Google Users in Iran Targeted in SSL Spoof." *CNET*, August 30. http://news.cnet.com/8301-27080_3-20099421-245/google-users-in-iran-targeted-in-ssl-spoof/.

Moore, Tyler, and Ross Anderson. 2012. "Internet Security." In *Oxford Handbook on the Digital Economy*, edited by Martin Peitz and Joel Waldfogel, 572–99. Oxford: Oxford University Press. https://spqr.eecs.umich.edu/courses/cs660sp11/papers/moore-anderson-infoeconsurvey2011.pdf.

Moore, Tyler, and Richard Clayton. 2007. "Examining the Impact of Website Take-down on Phishing." In *Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit (eCrime '07)*, 1–13.

———. 2009. "The Impact of Incentives on Notice and Take-Down." In *Managing Information Risk and the Economics of Security*, edited by M. Eric Johnson, 199–223. New York: Springer.

Moore, Tyler, Richard Clayton, and Ross Anderson. 2009. "The Economics of Online Crime." *Journal of Economic Perspectives* 23 (3): 3–20.

Mozilla. 2013. "Mozilla CA Certificate Policy, Version 2.1." https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/.

Mueller, Milton L. 2011. "DPI Technology from the Standpoint of Internet Governance Studies: An Introduction." http://dpi.ischool.syr.edu/Technology_files/WhatisDPI-2.pdf.

Mueller, Milton L., and Hadi Asghari. 2012. "Deep Packet Inspection and Bandwidth Management: Battles over BitTorrent in Canada and the United States." *Telecommunications Policy* 36: 462–75. doi:10.1016/j.telpol.2012.04.003.

Mueller, Milton L., Andreas Kuehn, and Stephanie Michelle Santoso. 2011. "DPI and Copyright Protection: A Comparison of EU, US and China." Paper presented at the Cyber-Surveillance in Everyday Life: An International Workshop, May 12-15, Toronto.

http://www.digitallymediatedsurveillance.ca/wp-content/uploads/2011/04/Mueller-Kuehn-Santoso-DPI-copyright-protection.pdf.

———. 2012. "Policing the Network: Using DPI for Copyright Enforcement." *Surveillance & Society* 9 (4): 348–64.

Musgrave, Richard A., and Peggy B. Musgrave. 1973. *Public Finance in Theory and Practice*. New York: McGraw-Hill.

Nadji, Yacin, Manos Antonakakis, Roberto Perdisci, David Dagon, and Wenke Lee. 2013. "Beheading Hydras: Performing Effective Botnet Takedowns." In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security (CCS '13)*, 121–32. doi:10.1145/2508859.2516749.

National Academies. 2005. "Facilitating Interdisciplinary Research." Washington, DC: The National Academies Press. http://www.nap.edu/read/11153/chapter/1#ii.

Nieuwesteeg, Bernold F.H. 2013. "The Legal Position and Societal Effects of Security Breach Notification Laws." Master Thesis, Delft University of Technology. http://repository.tudelft.nl/view/ir/uuid:38d4fa0e-8a3a-4216-9044-e8507a60ed66/.

Noam, Eli. 2009. *Media Ownership and Concentration in America*. New York: Oxford University Press.

NRC. 2011. "Mooie Dag Voor Een Black-Out' ('Nice Day for a Black-Out')." *NRC Handelsblad*, September 10.

OECD. 2012. "Proactive Policy Measures by Internet Service Providers against Botnets." OECD Digital Economy Papers 199. Paris: OECD Publishing. doi:10.1787/5k98tq42t18w-en.

Pastor-Satorras, Romualdo, Claudio Castellano, Piet Van Mieghem, and Alessandro Vespignani. 2014. "Epidemic Processes in Complex Networks." *arXiv Preprint*. arXiv:1408.2701v1 [physics.soc-ph].

Paxson, Vern. 2004. "Strategies for Sound Internet Measurement." In *Proceedings of the 4th ACM SIGCOMM Conference on Internet Measurement (IMC '04)*, 263–71. http://www.cs.cmu.edu/~srini/15-744/readings/meas-strategies-imc04.pdf.

Perset, Karine. 2010. "The Economic and Social Role of Internet Intermediaries." 171. OECD Digital Economy Papers. Paris: OECD Publishing. doi:10.1787/5kmh79zzs8vb-en.

Pfleeger, S.L., and R.K. Cunningham. 2010. "Why Measuring Security Is Hard." *IEEE Security and Privacy* 8 (4): 46–54. doi:10.1109/MSP.2010.60.

Plohmann, Daniel, Elmar Gerhards-Padilla, and Felix Leder. 2011. "Botnets: Measurement, Detection, Disinfection and Defence." Heraklion, Greece: European Network and Information Security Agency (ENISA). http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/botnets/botnets-measurement-detection-disinfection-and-defence.

Porras, Phillip, Hassen Saidi, and Vinod Yegneswaran. 2009. "An Analysis of Conficker's Logic and Rendezvous Points." Updated March 19, 2009. Menlo Park, CA: SRI International. http://www.mtc.sri.com/Conficker/.

Prins, J. Ronald. 2011. "DigiNotar Certificate Authority Breach - 'Operation Black Tulip' - Interim Report." Fox-IT. http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1.html.

Rains, Tim. 2012. "TeliaSonera – Finland's Secret for a Secure Internet." *Microsoft Cyber Trust Blog*. March 7. http://blogs.microsoft.com/cybertrust/2012/03/07/teliasonera-finlands-secret-for-a-secure-internet/.

Rajab, Moheeb Abu, Jay Zarfoss, Fabian Monrose, and Andreas Terzis. 2007. "My Botnet Is Bigger Than Yours (Maybe, Better Than Yours): Why Size Estimates Remain Challenging." In *Proceedings of the 1st USENIX Workshop on Hot Topics in Understanding Botnets (HotBots '07)*. https://www.usenix.org/legacy/event/hotbots07/tech/full_papers/rajab/rajab.pdf.

Ransbotham, Sam, and Sabyasachi Mitra. 2013. "The Impact of Immediate Disclosure on Attack Diffusion and Volume." In *Economics of Information Security and Privacy III*, edited by Bruce Schneier, 1–12. New York: Springer. doi:10.1007/978-1-4614-1981-5_1.

Rendon Group. 2011. "Conficker Working Group: Lessons Learned." Report commissioned by the Department of Homeland Security. http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf.

Riccardi, Marco, Roberto Di Pietro, Marta Palanques, and Jorge Aguilà Vila. 2013. "Titans' Revenge: Detecting Zeus via Its Own Flaws." *Botnet Activity: Analysis, Detection and Shutdown*, Special Issue, Computer Networks, 57 (2): 422–35. doi:10.1016/j.comnet.2012.06.023.

Romanosky, Sasha, Rahul Telang, and Alessandro Acquisti. 2011. "Do Data Breach Disclosure Laws Reduce Identity Theft?" *Journal of Policy Analysis and Management* 30 (2): 256–86. doi:10.1002/pam.20567.

Roosa, Steven B., and Stephen Schultze. 2010. "The 'Certificate Authority' Trust Model for SSL: A Defective Foundation for Encrypted Web Traffic and a Legal Quagmire." *Intellectual Property & Technology Law Journal* 22 (11): 3.

———. 2013. "Trust Darknet: Control and Compromise in the Internet's Certificate Authority Model." *SSRN*. doi:10.2139/ssrn.2249042.

Rosen, Harvey S. 2004. "Public Finance." In *The Encyclopedia of Public Choice*, edited by Charles Rowley and Friedrich Schneider, 252–61. Dordrecht: Kluwer Academic Publishers.

Rossow, C., D. Andriesse, T. Werner, B. Stone-Gross, D. Plohmann, C.J. Dietrich, and H. Bos. 2013. "SoK: P2PWNED - Modeling and Evaluating the Resilience of Peer-to-Peer Botnets." In *IEEE Symposium on Security and Privacy (SP) 2013*, 97–111. doi:10.1109/SP.2013.17.

Rysman, Marc. 2009. "The Economics of Two-Sided Markets." *The Journal of Economic Perspectives* 23 (3): 125–43.

Sandvine. 2012. "Global Internet Phenomena Report - 1H 2012." https://www.sandvine.com/downloads/general/global-internet-phenomena/2012/1h-2012-global-internet-phenomena-report.pdf.

Savage, Stefan. 2011. "An Agenda for Empirical Cyber Crime Research." Keynote presented at the 2011 USENIX Federated Conferences Week, June 14-17, Portland, OR.

Schmidt, Andreas. 2014. "Secrecy versus Openness: Internet Security and the Limits of Open Source and Peer Production." PhD diss, Delft University of Technology. http://repository.tudelft.nl/view/ir/uuid:ecf237ed-7131-4455-917f-11e55e03df0d/.

Schneier, Bruce. 2004. "Hacking the Business Climate for Network Security." *Computer* 37 (4): 87–89. doi:10.1109/MC.2004.1297316.

———. 2007. "A Security Market for Lemons." *Schneier on Security Blog*. April 19. https://www.schneier.com/blog/archives/2007/04/a_security_mark.html.

———. 2012. "When It Comes to Security, We're Back to Feudalism." *Schneier on Security Blog*. November 26. https://www.schneier.com/essays/archives/2012/11/when_it_comes_to_sec.html.

Schrodt, P. A. 2014. "Seven Deadly Sins of Contemporary Quantitative Political Analysis." *Journal of Peace Research* 51 (2): 287–300. doi:10.1177/0022343313499597.

Shadowserver. 2014. "Gameover Zeus." *Shadowserver Foundation*. Accessed February 23, 2015. https://goz.shadowserver.org/.

Shapiro, Carl, and Hal R. Varian. 1998. *Information Rules: A Strategic Guide to the Network Economy*. Boston, MA: Harvard Business School Press.

Shetty, Nikhil, Galina Schwartz, Mark Felegyhazi, and Jean Walrand. 2010. "Competitive Cyber-Insurance and Internet Security." In *Economics of Information Security and Privacy*, edited by Tyler Moore, David Pym, and Christos Ioannidis, 229–47. New York: Springer US. doi:10.1007/978-1-4419-6967-5_12.

Shim, W. 2006. "Interdependent Risk and Cyber Security: An Analysis of Security Investment and Cyber Insurance." PhD diss, East Lansing, MI: Michigan State University.

Shin, Seungwon, Guofei Gu, Narasimha Reddy, and Christopher P. Lee. 2012. "A Large-Scale Empirical Study of Conficker." *IEEE Transactions on Information Forensics and Security* 7 (2): 676–90. doi:10.1109/TIFS.2011.2173486.

Singer, Peter W, and Allan Friedman. 2013. *Cybersecurity: What Everyone Needs to Know*. Oxford: Oxford University Press.

Soghoian, Christopher, and Sid Stamm. 2012. "Certified Lies: Detecting and Defeating Government Interception Attacks against SSL." In *Financial Cryptography and Data Security*, edited by George Danezis, 250–59. Lecture Notes in Computer Science 7035. Berlin and Heidelberg: Springer. doi:10.1007/978-3-642-27576-0_20.

Spolsky, Joel. 2000. "The Joel Test: 12 Steps to Better Code." *Joel on Software Blog*. August 9. http://www.joelonsoftware.com/articles/fog0000000043.html.

Squatriglia, Chuck. 2008. "And the 14 Grand Engineering Challenges of the 21st Century Are…." *Wired*, February 15. http://www.wired.com/2008/02/and-the-14-big/.

Stajano, Frank, and Paul Wilson. 2011. "Understanding Scam Victims: Seven Principles for Systems Security." *Communications of the ACM* 54 (3): 70–75. doi:10.1145/1897852.1897872.

Staniford, Stuart, Vern Paxson, and Nicholas Weaver. 2002. "How to 0wn the Internet in Your Spare Time." In *Proceedings of the 11th USENIX Security Symposium (Security '02)*. http://www.icir.org/vern/papers/cdc-usenix-sec02/cdc.pdf.

Stone-Gross, Brett, Ryan Abman, Richard A. Kemmerer, Christopher Kruegel, Douglas G. Steigerwald, and Giovanni Vigna. 2013. "The Underground Economy of Fake Antivirus Software." In *Economics of Information Security and Privacy III*, edited by Bruce Schneier, 55–78. New York: Springer. doi:10.1007/978-1-4614-1981-5_4.

Stone-Gross, Brett, Marco Cova, Lorenzo Cavallaro, Bob Gilbert, Martin Szydlowski, Richard Kemmerer, Christopher Kruegel, and Giovanni Vigna. 2009. "Your Botnet Is My Botnet: Analysis of a Botnet Takeover." In *Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS '09)*, 635–47. doi:10.1145/1653662.1653738.

Stone-Gross, Brett, Christopher Kruegel, Kevin Almeroth, Andreas Moser, and Engin Kirda. 2009. "Fire: Finding Rogue Networks." In *Anual Computer Security Applications Conference 2009 (ACSAC '09)*, 231–40.

Sullivan, Kevin. 2012. "The Internet Health Model for Cybersecurity." New York: EastWest Institute. http://www.ewi.info/idea/internet-health-model-cybersecurity.

Sunshine, Joshua, Serge Egelman, Hazim Almuhimedi, Neha Atri, and Lorrie Faith Cranor. 2009. "Crying Wolf: An Empirical Study of SSL Warning Effectiveness." In *18th USENIX Security Symposium*

(Security '09), 399–416. http://static.usenix.org/legacy/events/sec09/tech/full_papers/sec09_browser.pdf.

Symantec. 2015. "Internet Security Threat Report Volume 20." Symantec. https://know.elq.symantec.com/LP=1542.

Tang, Qian, Leigh Linden, John S. Quarterman, and Andrew B. Whinston. 2013. "Improving Internet Security Through Social Information and Social Comparison: A Field Quasi-Experiment." presented at the Twelfth Workshop on the Economics of Information Security (WEIS 2013), June 11-13, Georgetown University, Washington, DC. http://weis2013.econinfosec.org/papers/TangWEIS2013.pdf.

Thaw, David Bernard. 2011. "Characterizing, Classifying, and Understanding Information Security Laws and Regulations." PhD diss, University of California, Berkeley. http://pitt.edu/~dbthaw/papers/DavidThawDissertationFinal.pdf.

Thomas, Kurt, Danny Yuxing Huang, David Wang, Elie Bursztein, Chris Grier, Tom Holt, Christopher Kruegel, Damon McCoy, Stefan Savage, and Giovanni Vigna. 2015. "Framing Dependencies Introduced by Underground Commoditization." Paper presented at the Fourteenth Workshop on the Economics of Information Security (WEIS 2015), June 22-23, Delft University of Technology, The Netherlands. http://weis2015.econinfosec.org/papers/WEIS_2015_thomas.pdf.

Thomas, Russell Cameron, Marcin Antkiewicz, Patrick Florer, Suzanne Widup, and Matthew Woodyard. 2013. "How Bad Is It? A Branching Activity Model to Estimate the Impact of Information Security Breaches (March 11, 2013)." *SSRN*. doi:10.2139/ssrn.2233075.

Thuraisingham, Bhavani. 2009. "Why Is Interdisciplinary Research Hard." https://www.utdallas.edu/~bhavani.thuraisingham/Motivational-Articles/Why_is_Interdisciplinary_Research_Hard.pdf.

Trustworthy Internet Movement. 2014. "SSL-Pulse: Survey of the SSL Implementation of the Most Popular Web Sites." https://www.trustworthyinternet.org/ssl-pulse/.

Van den Berg, Jan, Jacqueline van Zoggel, Mireille Snels, Mark van Leeuwen, Sergei Boeke, Leo van de Koppen, Jan van der Lubbe, Bibi van den Berg, and Tony de Bos. 2014. "On (the Emergence Of) Cyber Security Science and Its Challenges for Cyber Security Education." In *The NATO IST-122 Cyber Security Science and Engineering Symposium*.

Van der Velde, Mandy, Paul Jansen, and Neil Anderson. 2004. *Guide to Management Research Methods*. Hoboken, NJ: Wiley.

Van Eeten, Michel J.G., Hadi Asghari, Johannes M. Bauer, and Shirin Tabatabaie. 2011. "Internet Service Providers and Botnet Mitigation: A Fact-Finding Study on the Dutch Market." The Hague: Netherlands Ministry of Economic Affairs. www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/01/13/internet-service-providers-and-botnet-mitigation/tud-isps-and-botnet-mitigation-in-nl-final-public-version-07jan2011.pdf.

Van Eeten, Michel J.G., and Johannes M. Bauer. 2008. "Economics of Malware: Security Decisions, Incentives and Externalities." 2008/1. OECD Science, Technology and Industry Working Papers. Paris: OECD Publishing.

———. 2009. "Emerging Threats to Internet Security: Incentives, Externalities and Policy Implications." *Journal of Contingencies and Crisis Management* 17 (4): 221–32.

———. 2013. "Enhancing Incentives for Internet Security." In *Research Handbook on Governance of the Internet*, edited by Ian Brown, 445–84. Cheltenham and Northampton: Edward Elgar.

Van Eeten, Michel J.G., Johannes M. Bauer, Hadi Asghari, and Shirin Tabatabaie. 2010. "The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data." 2010/05. OECD Science, Technology and Industry Working Papers. Paris: OECD Publishing. doi:10.1787/5km4k7m9n3vj-en.

Van Eeten, Michel J.G., Johannes M. Bauer, and Shirin Tabatabaie. 2009. "Damages from Internet Security Incidents: A Framework and Toolkit for Assessing the Economic Costs of Security Breaches." Report for the Independent Post and Telecommunications Authority (OPTA, Now ACM). The Hague: OPTA. https://www.acm.nl/nl/download/publicatie/?id=9923.

Van Eeten, Michel J.G., and Milton L. Mueller. 2012. "Where Is the Governance in Internet Governance?" *New Media & Society* 5 (5): 720–36.

Vasek, Marie, and Tyler Moore. 2012. "Do Malware Reports Expedite Cleanup? An Experimental Study." In *5th Workshop on Cyber Security Experimentation and Test (CSET '12)*. https://www.usenix.org/system/files/conference/cset12/cset12-final20.pdf.

Verisign. 2010. "Verisign Annual Report 2009." http://files.shareholder.com/downloads/VRSN/2358873860x0x365048/ea1e2339-4582-4149-bf73-5391991cc3c1/.

Vratonjic, Nevena, Julien Freudiger, Vincent Bindschaedler, and Jean-Pierre Hubaux. 2013. "The Inconvenient Truth about Web Certificates." In *Economics of Information Security and Privacy III*, edited by Bruce Schneier, 79–117. New York: Springer. doi:10.1007/978-1-4614-1981-5_5.

Wagner, Ben. 2012. "Push-Button-Autocracy in Tunisia: Analysing the Role of Internet Infrastructure, Institutions and International Markets in Creating a Tunisian Censorship Regime." *Telecommunications Policy* 36 (6): 484–92. doi:10.1016/j.telpol.2012.04.007.

Walsh, Eric. 2014. "A Company That Does Background Checks For The US Government Was Victim Of 'State-Sponsored' Cyber Attack." *Reuters*, August 7. http://www.reuters.com/article/2014/08/07/us-usa-security-contractor-idUSKBN0G62N420140807.

Wash, Rick. 2010. "Folk Models of Home Computer Security." In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS '10)*.

Wash, Rick, and Jeffrey K. MacKie-Mason. 2007. "Security When People Matter: Structuring Incentives for User Behavior." In *Proceedings of the 9th International Conference on Electronic Commerce (ICEC '07)*, 7–14. doi:10.1145/1282100.1282105.

Weaver, Rhiannon. 2010. "A Probabilistic Population Study of the Conficker-C Botnet." In *Passive and Active Measurement*, edited by Arvind Krishnamurthy and Bernhard Plattner, 181–90. Lecture Notes in Computer Science 6032. Berlin and Heidelberg: Springer. doi:10.1007/978-3-642-12334-4_19.

Winn, Jane K. 2009. "Are 'Better' Security Breach Notification Laws Possible?" *Berkeley Technology Law Journal* 24 (3): 1133–66.

Wondracek, Gilbert, Thorsten Holz, Christian Platzer, Engin Kirda, and Christopher Kruegel. 2010. "Is the Internet for Porn? An Insight Into the Online Adult Industry." presented at the Ninth Workshop on the Economics of Information Security (WEIS 2010), June 7-8, Harvard University. http://iseclab.org/papers/weis2010.pdf.

Wood, Dallas, and Brent Rowe. 2011. "Assessing Home Internet Users' Demand for Security: Will They Pay ISPs?" presented at the Tenth Workshop on the Economics of Information Security (WEIS 2011), June 14-15, George Mason University, Fairfax, VA. http://weis2011.econinfosec.org//papers/Assessing%20Home%20Internet%20Users%20Demand%20for%20Security%20-%20Will%20T.pdf.

Yam, Marcus. 2009. "Microsoft: Pirated Windows 7 Will Still Get Updates." *Tom's Hardware*, April 29. http://www.tomshardware.com/news/windows-pirate-bootleg-security-patches,7666.html.

Zetter, Kim. 2014. "Sony Got Hacked Hard: What We Know and Don't Know So Far." *Wired*, December 3. http://www.wired.com/2014/12/sony-hack-what-we-know/.

Zhang, Changwang, Shi Zhou, and Benjamin M. Chain. 2015. "Hybrid Spreading of the Internet Worm Conficker." *PloS ONE* 10 (5). doi:10.1371/journal.pone.0127478.

Zhang, Jing, Zakir Durumeric, Michael Bailey, Mingyan Liu, and Manish Karir. 2014. "On the Mismanagement and Maliciousness of Networks." In *Proceedings of the Network and Distributed System Security (NDSS) Symposium 2014*. http://web.eecs.umich.edu/~jingzj/paper/jing_ndss14.pdf.

Zhuang, Li, John Dunagan, Daniel R Simon, Helen J Wang, Ivan Osipkov, and J Doug Tygar. 2008. "Characterizing Botnets from Email Spam Records." In *First Usenix Workshop on Large-Scale Exploits and Emergent Threats (LEET '08)*, 8:1–9. http://www.usenix.org/event/leet08/tech/full_papers/zhuang/zhuang.pdf.

Ziliak, Stephen T., and Deirdre N. McCloskey. 2004. "Size Matters: The Standard Error of Regressions in the American Economic Review." *The Journal of Socio-Economics*, Statistical Significance, 33 (5): 527–46. doi:10.1016/j.socec.2004.09.024.

Zittrain, Jonathan. 2008. *The Future of the Internet–and How to Stop It*. New Haven, CT: Yale University Press.

Zou, Cliff Changchun, Lixin Gao, Weibo Gong, and Don Towsley. 2003. "Monitoring and Early Warning for Internet Worms." In *Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS '03)*, 190–99. doi:10.1145/948109.948136.

Zou, Cliff Changchun, Weibo Gong, and Don Towsley. 2002. "Code Red Worm Propagation Modeling and Analysis." In *Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS '02)*, 138–47. doi:10.1145/948109.948136.

Appendix – pyasn 1.5 Manual[1]

pyasn is a Python extension module that enables very fast IP address to Autonomous System Number lookups. Current state and Historical lookups can be done, based on the BGP / MRT file used as input.

pyasn is different from other ASN lookup tools in that it providers offline and historical lookups. It provides utility scripts for users to build their own lookup databases based on any BGP/MRT dump file. This makes pyasn much faster than online dig/whois/json lookups.

The module is written in C and Python, and cross-compiles on Linux and Windows. Underneath, it uses a radix tree data structure for storage of IP addresses. In the current version, it borrows code from py-radix to support both IPv4 and IPv6 network prefixes. The current release is a beta. Compared to the previous version, it provides support for Python 2 and 3; adds new functionality, performance improvements, and unit-tests.

pyasn is developed and maintained by researchers at the Economics of Cybersecurity research group at Delft University of Technology. The package is used on an almost daily basis and bugs are fixed pretty quickly. The package is largely developed and maintained by Hadi Asghari and Arman Noroozian. Please report any bugs via GitHub or email the developers.

Installation

Installation is a breeze via pip:

```
pip install pyasn --pre
```

Or with the standard Python:

[1] pyasn is a tool that I developed early in the PhD research to determine who historically owned an IP address. Arman Noroozian has helped extend it since 2014. pyasn is open source (hosted at https://github.com/hadiasghari/pyasn) and used actively by other researchers.

```
python setup.py build
python setup.py install --record log
```

You will need to have pip, setuptools and build essentials installed if you build the package manually. On Ubuntu/Debian you can get them using the following command:

```
sudo apt-get install python-pip python-dev build-essential
```

Building the C module on Windows, using either pip or from source, requires Microsoft Visual C++ to be installed. pyasn has been tested using Visual C++ Express 2010, available freely from Microsoft's website, on both the official Python 3.4 release and Miniconda3. Other versions of Python, Visual Studio, and Cygwin might work with minor modifications.

Usage

A simple example that demonstrates most of the features:

```
import pyasn
# Initialize module and load IP to ASN database
# the sample database can be downloaded or built - see below
asndb = pyasn.pyasn('ipasn_20140513.dat')
asndb.lookup('8.8.8.8')
# should return: (15169, '8.8.8.0/24'), the origin AS, and the BGP prefix it
matches
asndb.get_as_prefixes(1128)
# returns ['130.161.0.0/16', '131.180.0.0/16', '145.94.0.0/16'], TU-Delft pre-
fixes
```

IPASN Data Files

IPASN data files are a long list of prefixes used to lookup AS number for IPs. An excerpt from such a file looks like this:

```
; IP-ASN32-DAT file
; Original file : <Path to a rib file>
; Converted on  : Tue May 13 22:03:05 2014
; CIDRs         : 512490
;
1.0.0.0/24  15169
1.0.128.0/17    9737
1.0.128.0/18    9737
1.0.128.0/19    9737
1.0.129.0/24    23969
...
```

IPASN data files can be created by downloading BGP/MRT dumps from Routeviews (or similar sources), and parsing them using provided scripts that tail the BGP AS-Path. This can be done simply as follows: ::

```
pyasn_util_download.py --latest
pyasn_util_convert.py --single <Downloaded RIB File> <ipasn_db_file_name>
```

NOTE: These scripts are by default installed to /usr/local/bin and can be executed directly. If you installed the package to a user directory, these scripts will not be on the path and you will have to invoke them by navigating to the folder in which they have been copied (e.g. ~/.local/bin).

We also provide download links to a large number of previously generated IPASN data files. These are based on weekly snapshots of the Routeviews data from 2005-2015, accessible here: http://data.3tu.nl/repository/uuid:d4d23b8e-2077-4592-8b47-cb476ad16e12

Performance Tip

Initial loading of a IPASN data file is the heaviest operation of the package. For fast lookups using multiple IPASN data files, for instance for historical lookups on multiple dates, we recommend caching of loaded data files for better performance.

Alternatively, you can convert the IPASN data files to binary format and load them using the binary load option to improve load time (in beta testing). You can save files to binary format using the --binary of the utility script

Uninstalling pyasn

You can remove pyasn as follows:

```
pip uninstall pyasn
```

If you built and installed the package yourself use the recorded log to remove the installed files.

Removing PyASN version 1.2: pyasn v1.5 and v1.2 can be installed side by side (due to lower-cased package name). To avoid mistakes, you can uninstall the old PyASN by deleting the following files from your Python installation:

```
PYTHONDIR/dist-packages/PyASN.so
PYTHONDIR/dist-packages/PyASN-1.2.egg-info
```

Package Structure

The main portions of the directory tree are as follows:

```
.
├── pyasn/__init__.py       # Python code of the main pyasn module
├── pyasn/pyasn_radix.c     # C extension code (Python module & bulk load)
├── pyasn/_radix/*          # C extension code (Based on MRTd RADIX code)
├── pyasn/mrtx.py           # module to convert MRT files to pyasn DB files
├── pyasn-utils/*.py        # Scripts to download & convert BGP MRT dumps
├── data/                   # Test Resources and some sample DBs to use
├── tests/                  # Tests
└── setup.py                # Standard setup.py for installation/testing
```

Testing pyasn Sources

A limited number of unit tests are provided in the tests/ directory when downloading the sources. They can be run with the following command:

```
python setup.py test
```

This beta release has been tested under python version 2.6, 2.7, 3.3 and 3.4. We appreciate contributions towards testing pyasn! Unit Tests are particularly appreciated.

License & Acknowledgments

pyasn is licensed under the MIT license. It extends code from py-radix (Michael J. Schultz and Damien Miller), and improves upon it in several ways, for instance in lowering memory usage and adding bulk prefix/origin load. The underlying radix tree implementation is taken (and modified) from MRTd. These are all subject to their respective licenses. Please see the LICENSE file for details. Thanks to Dr. Chris Lee (of Shadowserver) for proposing the use of radix trees.

Acknowledgements

I would like to thank all the companies and organizations that have made the research in this dissertation possible by providing data and feedback. This includes the Conficker Working Group (confickerworkinggroup.org), the Dutch Authority for Consumers and Markets (acm.nl), the Electronic Frontier Foundation (eff.org), Farsight Security (farsightsecurity.com), Fox-IT (www.fox-it.com), the German Internet Industry Association Eco (eco.de), Google (google.com), KPN (kpn.com), Measurement-Lab (measurementlab.net), Microsoft (microsoft.com), the Shadowserver Foundation (shadowserver.org), Trend Micro (trendmicro.com), XS4All (xs4all.nl), ZeelandNet (zeelandnet.nl), as well as other Dutch and North American ISPs that have participated in our workshops. Many thanks to the individual collaborators in these organizations, and in particular, Dave Rand and Dr. Paul Vixie.

Curriculum Vitae

Hadi Asghari was born on March 27, 1978, in Tehran, Iran. After earning his high school diploma in Mathematics and Physics in 1996, he studied Mechanical Engineering at Amirkabir University of Technology; he later changed his major and university, and graduated with a Bachelor of Software Engineering from Shamsipour Institute of Technology, Tehran.

Hadi was an early Internet adopter in Iran. In 2000, he led the technical team for the Roshd Project that connected Tehran high-schools to the Internet. In 2001, he cofounded Dotware Technologies, a network and software company that developed software to manage ISP networks and news websites.

In 2007, Hadi moved to the Netherlands to pursue a master degree in Management of Technology at TU Delft. He graduated top student of his faculty and won the IBM MoT thesis prize and the UFonds best graduate award.

He started a PhD program in 2010 under the guidance of Prof. Michel J.G. van Eeten. During the PhD research, he coauthored a number of peer-reviewed papers highlighted in this dissertation. The studies also received attention among industry and policy experts, and were presented at the Organization for Economic Cooperation and Development (OECD), the Dutch Ministry of Economic Affairs, the Dutch telecom regulator (ACM), and the European Commission.

Hadi maintained his entrepreneurial spirit during his PhD research: in 2010-2012, he served on TU Delft's PhD representative board; in 2013, he helped expand the Governance of Cybersecurity Group led by Prof. Van Eeten; and in 2015, he was the organizing chair for the annual Workshop on Economics of Information Security (WEIS).

List of Publications

Asghari, Hadi, Michel J.G. van Eeten, and Johannes M. Bauer. Forthcoming. "Economics of Cybersecurity." In *Handbook on the Economics of the Internet*, edited by Johannes M. Bauer and Michael Latzer. Cheltenham and Northampton: Edward Elgar.

Asghari, Hadi, Michel J.G. van Eeten, and Johannes M. Bauer. 2015. "Economics of Fighting Botnets: Lessons from a Decade Mitigation." *IEEE Security and Privacy* 13 (5): 16–23. doi:10.1109/MSP.2015.110.

Asghari, Hadi, Michael Ciere, and Michel J.G. van Eeten. 2015. "Post-Mortem of a Zombie: Conficker Cleanup After Six Years." In *Proceedings of the 24th USENIX Security Symposium (Security '15)*. https://goo.gl/LnguCn.

Moura, Giovane C.M., Carlos Ganan, Qasim Lone, Payam Poursaied, Hadi Asghari, and Michel J.G. van Eeten. 2015. "How Dynamic Is the ISPs Address Space? Towards Internet-Wide DHCP Churn Estimation." In *IFIP Networking Conference (IFIP Networking) 2015*. doi:10.1109/IFIPNetworking.2015.7145335.

Arnbak, Axel, Hadi Asghari, Michel J.G. van Eeten, and Nico van Eijk. 2014. "Security Collapse in the HTTPS Market." *Communications of the ACM* 57 (10): 47–55. doi:10.1145/2660574.

Tajalizadehkhoob, Samaneh, Hadi Asghari, Carlos Gañán, and Michel J.G. van Eeten. 2014. "Why Them? Extracting Intelligence about Target Selection from Zeus Financial Malware." Paper presented at the 13th Annual Workshop on Economics of Information Security (WEIS 2014), June 23-24, State College, PA. http://goo.gl/vzml7I.

Asghari, Hadi, Michel J.G. van Eeten, and Milton L. Mueller. 2013. "Internet Measurements and Public Policy: Mind the Gap." In *Proceedings of the 6th USENIX Workshop on Cyber Security Experimentation and Test (CSET '13)*. doi:10.2139/ssrn.2294456.

Asghari, Hadi, Michel J.G. van Eeten, Axel Arnbak, and Nico van Eijk. 2013. "Security Economics in the HTTPS Value Chain." Paper peer reviewed and presented at the 12th Workshop on the Economics of Information Security (WEIS 2013), June 11-13, Washington, DC. doi:10.2139/ssrn.2277806.

Mueller, Milton L., Brenden Kuerbis, and Hadi Asghari. 2013. "Dimensioning the Elephant: An Empirical Analysis of the IPv4 Number Market." *Info* 15 (6): 6–18. doi:10.1108/info-07-2013-0039.

Kuerbis, Brenden, Hadi Asghari, and Milton L. Mueller. 2013. "In the Eye of the Beholder: The Role of Needs-Based Assessment in IP Address Market Transfers." Paper presented at the 41st Research Conference on Communication, Information and Internet Policy (TPRC 2013), September 27-29, Arlington, VA. doi:10.2139/ssrn.2242432.

Asghari, Hadi, Michel J.G. van Eeten, Johannes M. Bauer, and Milton L. Mueller. 2013. "Deep Packet Inspection: Effects of Regulation on Its Deployment by Internet Providers." Paper presented at the 41st Research Conference on Communication, Information, and Internet Policy (TPRC 2013), September 27-29, Arlington, VA.

Mueller, Milton L., and Hadi Asghari. 2012. "Deep Packet Inspection and Bandwidth Management: Battles over BitTorrent in Canada and the United States." *Telecommunications Policy* 36: 462–75. doi:10.1016/j.telpol.2012.04.003.

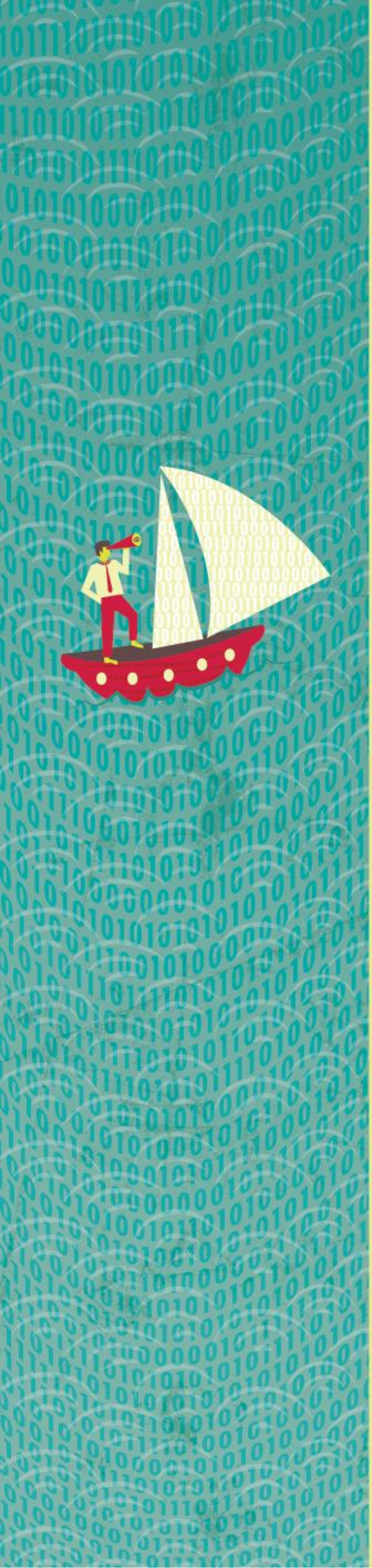
Asghari, Hadi, Michel J.G. van Eeten, and Milton L. Mueller. 2012. "Unraveling the Economic and Political Drivers of Deep Packet Inspection." Paper presented at the GigaNet 7th Annual Symposium, November 5, Baku, Azerbaijan. doi:10.2139/ssrn.2294434.

Van Eeten, Michel J.G., Hadi Asghari, Johannes M. Bauer, and Shirin Tabatabaie. 2011. "Internet Service Providers and Botnet Mitigation: A Fact-Finding Study on the Dutch Market." The Hague: Netherlands Ministry of Economic Affairs. http://goo.gl/ODJEBg.

Van Eeten, Michel J.G., Johannes M. Bauer, Hadi Asghari, and Shirin Tabatabaie. 2010. "The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data." 2010/05. OECD Science, Technology and Industry Working Papers. Paris: OECD Publishing. doi:10.1787/5km4k7m9n3vj-en.

Asghari, Hadi. 2010. "Botnet Mitigation and the Role of ISPs: A Quantitative Study into the Role and Incentives of Internet Service Providers in Combating Botnet Propagation and Activity." Master Thesis, Delft University of Technology. http://goo.gl/HUc2WN.

Zamanitabar, Mohsen, S. Mehdi Falsafy, Hadi Asghari, and Vahid Valizadeh. 2006. "Rescue Simulation League Team Kosar (Iran) Agent Competition." Paper presented at the Robocup Rescue Championships 2006, June 14-18, Bremen, Germany. http://goo.gl/tMTyAJ.



CYBERSECURITY via INTERMEDIARIES

Research in the field of information security economics has clarified how attacker and defender incentives affect cybersecurity. It has also highlighted the role of intermediaries in strengthening cybersecurity. Intermediaries are organizations and firms that provide the Internet's infrastructure and platforms.
This dissertation looks at how intermediary behavior and incentives can be understood from measurements—such as incident data and network logs. The question is answered through a literature review, four empirical studies, and two reflection chapters. The studies researched the role of ISPs in mitigating botnets, the success of anti-botnet initiatives in Conficker cleanup, vulnerabilities in the certificate authority ecosystem, and ISP incentives to deploy deep packet inspection, all using cross-country and longitudinal measurements. The dissertation concludes by reflecting on both the methodology and the broader implications for cybersecurity policy.

TUDelft