

**COORDINATING ACROSS CHAOS: THE PRACTICE OF
TRANSNATIONAL INTERNET SECURITY COLLABORATION**

A Dissertation
Presented to
The Academic Faculty

by

Tarun Chaudhary

In Partial Fulfillment
of the Requirements for the Degree
International Affairs, Science, and Technology in the
Sam Nunn School of International Affairs

Georgia Institute of Technology
May 2019

COPYRIGHT © 2019 BY TARUN CHAUDHARY

COORDINATING ACROSS CHAOS: THE PRACTICE OF TRANSNATIONAL INTERNET SECURITY COLLABORATION

Approved by:

Dr. Adam N. Stulberg
School of International Affairs
Georgia Institute of Technology

Dr. Peter K. Brecke
School of International Affairs
Georgia Institute of Technology

Dr. Michael D. Salomone
School of International Affairs
Georgia Institute of Technology

Dr. Milton L. Mueller
School of Public Policy
Georgia Institute of Technology

Dr. Jennifer Jordan
School of International Affairs
Georgia Institute of Technology

Date Approved: March 11, 2019

ACKNOWLEDGEMENTS

I was once told that writing a dissertation is lonely experience. This is only partially true. The experience of researching and writing this work has been supported and encouraged by a small army of individuals I am forever grateful toward. My wife Jamie, who has been a truly patient soul and encouraging beyond measure while also being my intellectual sounding board always helping guide me to deeper insight. I have benefited from an abundance of truly wonderful teachers over the course of my academic life. Dr. Michael Salomone who steered me toward the world of international security studies since I was an undergraduate, I am thankful for his wisdom and the tremendous amount of support he has given me over the past two decades. The rest of my committee has been equally as encouraging and provided me with countless insights as this work has been gestating and evolving. Dr. Adam Stulberg who has given me many intellectual opportunities and whose stewardship of my education has been invaluable. Dr. Peter Brecke who remains a steadfast supporter, and to whom I owe a tremendous debt of gratitude not only for his role on my dissertation committee, but for sparking a persistent intellectual curiosity to explore “complex systems across long timelines.” I may have never completed a draft of this dissertation without Dr. Jenna Jordan who insisted it was time for me to begin presenting, discussing, and refining early drafts and provided me with thoughtful, insightful, and wholly invaluable feedback. It is an honor to have Dr. Milton Mueller on my dissertation committee whose work has provided the basis for my own intellectual journey and whose insights and encouragement I am grateful for. I am also indebted to Dr. Seymour Goodman for his invaluable help in supporting my ambition to study all things cyber. Finally, I owe my parents more than I can ever express. No, writing a dissertation isn’t a lonely experience, it is one that allows an individual to create, investigate, and explore while lifted up by those they are surrounded by

TABLE OF CONTENTS

ACKNOWLEDGEMENTS	iii
LIST OF TABLES	vi
LIST OF FIGURES	vii
LIST OF SYMBOLS AND ABBREVIATIONS	viii
SUMMARY	xi
CHAPTER 1. Introduction	1
1.1 Defining the Domain of Analysis	3
1.2 Descriptive Framework	5
1.3 Shifting Away from ‘Cyber’ and Defining Security	9
1.3.1 “Cyber” Doesn’t Exist (but it should)	10
1.4 Information Security Management	13
1.4.1 Layered Model of Cyberspace	15
1.5 Information Centered IR Security (ICIRS) Model	18
CHAPTER 2. Social Practice: Agency, Structure and Culture	22
2.1 International Security and ICIRS	22
2.2 Security Provisioning Networks	26
2.3 Social Practice	27
2.3.1 Security as Practice	30
2.4 Organizational Seams	34
2.5 Related Literatures	39
2.5.1 Networked Governance	40
2.5.2 Peer Production	44
2.5.3 Regime Complexes	46
2.5.4 Science and Technology Studies	49
2.6 Agency, Structure, and Power during Security Provisioning	50
CHAPTER 3. Provisioning Security on the Internet: A Historical Context	53
3.1 Morris Worm: Security as a local concern	54
3.1.1 Debates	60
3.1.2 Knowledge preservation, communication and distribution	63
3.2 Seams Multiply: Explosive Growth, Professionalization, and Evolving Threat	66
3.2.1 1992 – Michelangelo Virus	67
3.2.2 1999 – Melissa Virus	69
3.2.2 2000 – ILOVEYOU Worm	73
3.2.3 2003 – SQL Slammer	76
3.2.4 2004 – MyDoom, SoBig, Sasser and the Monetization	78
3.2.5 2008 – Conficker	80
CHAPTER 4. The Modern Security Provisioning Space	87

4.1	Topology and Complexity	87
4.1.1-	BGP Routing Errors	93
4.2	The Operational Security Community of Practice and the “Takedown”	97
4.2.1	The “Takedown”	103
4.3	The Mariposa Botnet	107
4.4	Microsoft Botnet Takedowns	112
4.4.1	Rustock	113
4.4.2	Evolving Microsoft Strategy	117
4.5	Take-down operations in Summary	118
CHAPTER 5. Conclusion		129
5.1	Security as Practice <i>and</i> Power	130
5.1.1	Its networks all the way down...	133
5.2	Lessons for Policy Makers	135
5.3	Future Work	139
5.4	Complex Things Fail in Complex Ways	141
References		145

LIST OF TABLES

Table 1: Choucri and Clark Integrated Cyber-IR System.....	17
Table 2: Members of the Conficker Working Group.....	84
Table 3: CAIDA AS Core Graph.....	88
Table 4: Summary of Takedown/Security Provisioning Activities	119

LIST OF FIGURES

Figure 1: Simplified Model of Information Security Management	14
Figure 2: Choucri and Clark Layered Model of Cyberspace	16
Figure 3: Information Centered Security Model.....	19
Figure 4: Information Centered IR Security (ICIRS) Model.....	20
Figure 5 Example of Technical Information Shared on Phage.....	57

LIST OF SYMBOLS AND ABBREVIATIONS

ANT	Actor Network Theory
AOL	America Online
AP	Advanced Placement
ARPANET	Advance Research Projects Agency Network
AS	Autonomous System
BBC	British Broadcasting Company
BGP	Border Gateway Protocol
C&C	Command and Control
CAIDA	Center for Applied Internet Data Analysis
CERT	Computer Emergency Response Team
CTO	Chief Technology Officer
CWG	Conficker Working Group
DARPA	Defense Advanced Research Projects Agency
DDOS	Distributed Denial of Service
DHS	Department of Homeland Security
DNS	Domain Name Service
DNS	Domain Name Service
DoD	Department of Defense
DoDCSC	Department of Defense Computer Security Center
EU	European Union
EU	European Union
FAT	File Allocation Table
FBI	Federal Bureau of Investigation

FedCIRC Federal Incident Response Center

GAO Government Accountability Office

GSA General Services Administration

ICANN Internet Corporation for Assigned Names and Numbers

ICIRS Information Centered International Relations Security

IETF Internet Engineering Task Force

IP Internet Protocol

IR International Relations

ISAC Information Security Analysis Centers

ISOI Internet Security and Operational Intelligence

ISP Internet Service Provider

IT Information Technology

IXP Internet Exchange Point

MIT Massachusetts Institute of Technology

NANOG North American Network Operations Group

NASA National Aeronautics and Space Administration

NATO North American Treaty Organization

NCI National Council of ISACs

NCSC National Computer Security Center

NIE New Institutional Economics

NIPC National Infrastructure Protection Center

NIST National Institute of Standards and Technology

NOG Network Operations Group

NSFNET National Science Foundation Network

OPSEC Operational Security

Ops-T Ops-Trust

PCH Packet Clearing House

PDD Presidential Decision Directive

RCMP Royal Canadian Mounted Police

RICO Racketeer Influenced and Corrupt Organizations

SMTP Simple Mail Transfer Protocol

SQL Structured Query Language

STS Science and Technology Studies

TCP/IP Transmission Control Protocol over Internet Protocol

TLD Top Level Domain

TLP Traffic Light Protocol

URL Uniform Resource Locator

US-CERT United States Computer Emergency Response Team

W3C World Wide Web Consortium

XOR exclusive or

SUMMARY

This dissertation explores transnational security provisioning on/for the internet. A unique framework of analysis is established that melds traditional understandings of security drawn from computing disciplines with levels of analysis from international relations (IR) theory. This helps bridge the gap between IR security literatures that often places the State at the center of analysis with the system of distributed agency often called a “patchwork” that underlies security provisioning on/for the Internet. This results in the Information Centered IR Security Model (ICIRS pronounced *Icarus*). The recognition and remediation of large-scale issues on/for the Internet is shown to be a form of social practice which has instantiated a community of practice. Data across cases of malware recognition and remediation are used to establish a historical context for the provisioning of security on/for the Internet and to analyze the modern provisioning context. It is concluded that an information security community of practice has arisen as consequence of the Internet’s early structure while evolving through various important security events. That community is embedded within the functional structure of the Internet and, through the maintenance of professional social relations, individuals within the community can act both as sensors to recognize emerging threats and as agents to remediate such threats thus wielding an important dimension of power in a connected world.

CHAPTER 1. INTRODUCTION

Nation-states have acknowledged *cyber-space* as a medium of strategic focus and equivalent of air, land, sea, and space. A review of capstone strategy documents across NATO countries and other world powers support that conclusion and show that government centered initiatives often dominate discussion while also often espousing a desire to operate with impunity within the cyber realm (though not often stated in such stark terms).¹ Ostensibly, elevating the cyber environment to stand next to the four other strategic domains signals that *security* within cyber-space is to be pursued with equal vigor if such statements are taken at face value. This represents a paradox for national governments that must advance their interests and power within a strategic domain that relies on many private and non-domestic elements for *both* function and security while falling outside of exclusive control by any one State apparatus.²

Analysts and practitioners have not reached as singular definition of what the cyber realm

¹ See for example the list maintained by the NATO Cooperative Cyber Defence Center of Excellence at <https://ccdcoe.org/cyber-security-strategy-documents.html>; and specific strategic documents such as the 2015 National Security Strategy of the US available at <http://nssarchive.us/wp-content/uploads/2015/02/2015.pdf>. China, too, has elevated cyberspace to stand next to the other warfighting domains. For a summary of Chinese views see, the 26 April 2016 *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2016* issued by the US Office of the Secretary of Defense available at: <https://www.defense.gov>; specifically page 43

² This reliance on non-state centered elements for both function and security is what separates the Internet from other international 'commons'. Air, land, sea, and space all exist independent of any private entity. The Internet, however, is non-constituent and cannot exist in a useful form *unless* transnational private, public, and quasi-public networks are joined together and traversed. Additionally, the argument is being made here that unlike the four other strategic spaces, Internet wide network security cannot be imposed simply through the elements of hard state power such as tanks, airplanes, and ships but is, in fact, contingent upon collaboration between many constituent entities and elements. This means, while states may conceive of 'cyberspace' alongside other strategic spaces, *security* within the realm must to be thought up in a wholly different fashion.

consists of, but the Internet itself can be viewed as a large (if not the largest) component of that space. Thereby, I argue it is necessary to understand the basic mechanisms of security that keep the Internet functional and remediate large-scale threats as they present themselves. That infrastructure is commonly characterized as a “patchwork,” necessarily drawing on a diverse range of public agencies (civilian, military, and law enforcement), private entities, non-profit organizations, and academic institutions all falling across both domestic and international lines for response to large-scale events. Network security on/for the Internet involves multiple stakeholders and pervasive collaboration across many levels of structure and institutionalization that have resulted in a system of distributed agency. This is partially due to how the Internet is engineered as a network of networks, parts of which are owned and operated by a variety both private, public, and hybrid entities that cross political boundaries. What are the specific constituencies involved and how did those elements arise? Much of the prior work with regard to Internet security has focused on an abstract understanding of those elements, but this dissertation helps illuminate the individual level of analysis with regard to the patchwork response system while also defining an important aspect of power in the connected world, the ability to recognize and remediate threats on the Internet. That power is a product of where individuals are embedded within the connected infrastructure making up the Internet and when combined with the socio-professional connections these individuals maintain, they may act as sensors to recognize threats and as agents to help remediate those same threats.

In terms of international relations (IR) theory, traditional concepts of security, most of which are “state-centered” in nature, are ill-suited to fully conceptualize, operationalize and explore the diverse nexus of actors, governance structures, formal, and informal communities responsible for the provisioning of security and continued operation of the Internet. This

dissertation argues that the recognition of threat, and the provisioning of security across a certain class of large-scale threats present on the Internet represent a set of practices, which take place within a community of practice. The lens of practice can bridge the conceptual gap between traditional security understood to be a central responsibility of the State and the mechanism of distributed agency that underlies security on and for the Internet. In order to do so, this dissertation creates a unique model that fuses traditional understandings of information security developed within the discipline of computing with foundational levels of analysis utilized within the discipline of International Relations. The resultant model is applied to interrogate data on cases of botnet “takedowns” and malware remediation efforts. In doing so, the present work fills both an empirical hole within the discussion of security pertinent to “cyberspace” while also providing theoretical bridges for the disciplines of IR and Security Studies to connect with and understand this important and understudied facet of the modern international security landscape. Lastly, and importantly, this dissertation informs policy-making that seeks to advance both State and public interest while minimizing interference within the functioning system.

1.1 Defining the Domain of Analysis

It is patently obvious that *cyberspace* has become a strategic security concept in and of itself. Whether viewed as a constituent battle-space, a technological infrastructure, a socio-cultural concept, or an economic engine – information exchanged, stored and processed via electronic means and accessible through a variety of vectors to an international user-base has, for better or worse, become a central security concern for society at large. It is unsurprising then, a community of individuals, private/public entities, and institutions aimed at the continued function of the Internet has manifested and continues to evolve. Security and resiliency on and for the Internet is necessarily collaborative since a central characteristic of *networks* is that they propagate effects as

a mere function of pervasive connectivity. Despite the existence of disincentives because of competitive pressures, secrecy necessitated by security concerns, lack of comprehensive formal arrangements, a plethora of threats, and many other potential road blocks -- the Internet continues to function, and collaborative security is still pursued. The way this collaboration happens and the transnational coalitions that form to solve problems evolve present an interesting puzzle for those who study international security phenomena. Information security communities of practice connect with each other across political borders, across civilian/military lines, and across public and private spheres to address both specific and diffuse threats -- be those threats malicious or structural in nature. Sometimes these collaborations are born out of formal institutional linkages in a directed manner, but many other times informal collaboration instantiated through non-hierarchical means is a central mechanism of threat redress.

This isn't to say that computer security institutions and other represented entities represent some fanciful utopian community that simply does the right thing. The reality is much more interesting. Yet the degree, quality, and mechanisms of this collaboration are understudied facets of modern international life. International relations theory has not, as of yet, explored this type of important collaborative security activity in a comprehensive manner.

The issue of collaborative security with regarding to the internet, while understudied, has been looked at narrowly by other authors. This effort differs in the analytic approach used previously by varying both the theoretical lenses and levels of analysis applied. Previous authors such as Andreas Schmidt have characterized the types of security provisioning activities referred

to within this work as “peer production.”³ This effort does not try and walk away from such a characterization but seeks to add a layer of analytic understanding by submitting that “peer production” cannot account for how current security provisioning is co-constituted, arising from both a technological and sociopolitical context beyond the narrow context peer production draws from. Additionally, much of the current literature conceives of the security provisioning space as a network consisting of nodes that are far too homogeneous, thus abstracting away the institutions and hierarchies within which individuals and entities are embedded to the detriment of analytic utility. The analysis presented herein is rooted in pragmatic approach, often stated as “problem” or “concept” oriented research methodology. This perspective is not deductive or strictly inductive, instead it occupies a middle ground sometimes referred to as abduction.⁴ The process of abduction is not characterized by imposing an abstract theoretical template (deduction) from above or inferring propositions from facts (induction) but is characterized by reasoning at an intermediate level.⁵ The framework offered within the first two chapters of this work allows for a parsing of qualitative data to understand operational dynamics amongst security provisioning pathways in order to derive insight into that activity as a social practice.

1.2 Descriptive Framework

The present analysis offers a framework within which to place the emergence and

³ Schmidt, Andreas. *Secrecy versus openness: Internet security and the limits of open source and peer production* Doctoral Thesis. Delft University, available at:

<http://repository.tudelft.nl/view/ir/uuid:ecf237ed-7131-4455-917f-11e55e03df0d/>

⁴ The decision to use an abductive perspective is heavily influenced by literature such as: Friedrichs, Jörg, and Friedrich Kratochwil. "On acting and knowing: how pragmatism can advance international relations research and methodology." *International Organization* 63.04 (2009): 701-731; For a robust discussion on the merits of analytic eclecticism, see Sil, Rudra, and Peter J. Katzenstein. *Beyond paradigms: analytic eclecticism in the study of world politics*. Palgrave Macmillan, 2010

⁵ Friedrichs and Kratochwil (2009), p. 709

continued evolution of Internet security provisioning activities. It can be generally stated as follows: The success, qualified-success, and structure of international security provisioning activity on/for the Internet can be explained using the interplay of 1) the structure and interconnectedness of the Internet, 2) a local security culture specific to a problem and the individuals/entities whom first mobilize around it, and 3) interaction across ‘seams’ amongst constituencies brought together during the course of problem solving/ security provisioning. The interplay of these three layers represent the context within which security provisioning exists as an embedded social practice. The practice itself, while shaped by that context, also re-shapes the larger context and thus helps explain the evolution and structure of security provisioning.

Often private companies will partner with government agencies in order to investigate and neutralize nefarious cyber actors. This de facto deputating of private corporations acting on behalf of not just their own government, but on behalf of all Internet users, is a curious phenomenon as it speaks to a distribution of power and agency that is particularly hard to categorize. Partial explanations certainly revolve around the continued state of flux that the Internet’s governance regime is experiencing as it is still a young socio-political construct and technology by many measures. Such an explanation is not, however, comprehensive enough to stand alone. There remain mechanisms of threat redress on and for the Internet that are only vaguely understood and have not yet been formally studied as a form of collaborative security executed among a diverse set of international private and public actors. These forms of interaction are not easily placed within the traditional spectrum of international security behavior.

This could be the case for a variety of reasons, amongst which are the vexing ambiguity and imprecision of the term “cyber-security”, the difficulty in segmenting and assessing the variety of formal and informal institutions involved in cyber-security and cyber-governance that fall

across civil/military, public/private, and domestic/international lines. Additionally, there are few frame-works available, if any, on which to base analysis that can successfully conceptualize the information space alongside the trans-national political space that have also been widely accepted or applied. Finally, these activities are not always ‘State centered’, meaning the principal entity initiating the security provisioning activity isn’t imbued with the authority of the State, the traditional holder of *agency* in international (and trans-national) security activity. Often, parts of these communities of security professionals refer to themselves as the Internet operational security (OPSEC) community – indicating they view themselves as the operational security front line. Their communities are characterized by secrecy maintained through extensive peer vetting while shunning outsiders as participants on their mailing lists and web forums. That secrecy makes empirical observation difficult but, in and of itself, indicates cultural institutionalization and the existence of elements of *practice* helping define the constituency as a “community”.

Chapters one and two are meant to serve as an organizing tool and way out of the morass in order to better understand the evolving relationship between security *communities of practice*, outside institutions, and other involved entities with regards to the cyber-security. Several guiding assumptions will be made before proceeding. 1) The definitional ambiguity of the term ‘*cyber-security*’, while well worth discussing, cannot be solved here and will vary given institutional and regime context. 2) The overlapping, nested, and the otherwise complex relationship amongst cyber related institutions, regimes, bureaucracies, and normative milieu is larger than what can easily be mapped directly. 3) Existing frameworks related to security studies, international institutions, social theory, organizations, and collaboration can be leveraged to effectively explore and understand inter-institutional cyber-security provisioning relationships, though empirical

observation of ongoing and future dynamics may be difficult.⁶ First bridges will be built between traditional computational sciences' understanding of security and the manner in which security is thought about within social science, specifically within the realm of security studies, a sub-discipline of IR. This will result in defining security for/on the Internet in the broadest and simplest terms possible while simultaneously avoiding the pervasive confusion and imprecision introduced by the term "cyber-security". Doing so is an exercise in ontological definition, helping bound the entity(s) under examination. The second chapter will assemble a basis for analyzing security provisioning activities as an embedded social practice conceptualized as a network interacting across various functional boundaries termed *seams*. The chapter will also critically and briefly assess work on the issue of collaborative Internet security emanating from other literatures such as Network Governance, Peer Production, Regime Complexes, and Science and Technology Studies, which are all adjacent to or complementary to the current effort. These are reviewed to firmly seat the theoretical perspective within which this dissertation is placed.

The third chapter of this dissertation will set the act of provisioning security on/for the Internet into a historical context alongside the evolution of the Internet bookended by two canonical cases, the Morris Worm incident and the Conficker botnet. The chapter will also outline numerous events that help contextualize the rise of a security community of practice as the Internet exploded in size and importance and as security became a profession and central concern.

Chapter four of this dissertation will analyze the modern provisioning space by first exploring the issue of Border Gateway Protocol (BGP) routing errors, then by analyzing a specific segment of the Internet's security community of practice centered on operational security and

⁶ The term *inter-institutional* is used here to refer to collaboration across (non-exhaustively) private/public, civil/military, domestic/ international partners

intelligence to understand identity. Finally data gathered across numerous cases of malware and botnet remediation efforts that have taken place over the past twelve years will be used to help understand the phenomenon of modern “take-down” events when malware and botnets are neutralized by a constellation of actors and entities drawn from a community of practice.

Chapter five of this dissertation uses the communities of practice framework to provide implications for institutional design questions faced by policy makers within the cyber-security policy arena. The chapter will end by presenting a summary of findings, assess weaknesses with the argument being presented within this dissertation, and speaks to future work before offering concluding thoughts.

1.3 Shifting Away from ‘Cyber’ and Defining Security

Cyber-security as a term lacks a coherent or singular meaning. This is an often-made observation within the burgeoning cyber focused literature emanating from the collective disciplines falling loosely under the rubric of International Studies.⁷ Writers usually follow that observation by a parsing of the term before a definition is offered that tries to bring clarity within the context of an author’s purpose. While the present work is no different, the argument is made here that this definitional ambiguity cannot be solved due to a variety of normative and conceptual linkages the term gains when used within specific institutional context or in an area specific manner. Admittedly, the argument for this substitution and idiomatic shift in terminology is not robustly developed here but, in short, shifting away from the term “cyber-security” toward an understanding of information security management helps address a fundamental, and perhaps

⁷ See for example, Valeriano, Brandon and Maness, Ryan C. *International Relations Theory and Cybersecurity: Threats, Conflicts, and Ethics in an Emergent Domain* in The Oxford Handbook of International Political Theory. Oxford (2018)

widening, gap between technical computational/ IT security, policy discussion, and social science academic work.

1.3.1 “Cyber” Doesn’t Exist (but it should)

As a domain of knowledge, “cyber” is a poorly understood, emerging field composed of numerous asymmetric capabilities and concepts. As a medium of action and value, “cyber” is constituent, non-material, and necessarily mediated by the established mediums of existence. Unlike other domains in modern human knowledge, the individual components do not form a coherent whole when understood from a technically-informed, inter-disciplinary viewpoint. The pragmatic needs of various non-technical viewpoints to understand computer and network architecture and design are not served by the amorphous label “cyber” due to the occlusion of important technical details. It is interesting to note anecdotally, in the technical community, “cyber” as a prefix can induce a negative connotation unless one is attempting to acquire funding and/or a grant and then it is merely distasteful.⁸ This is a two-fold problem: the technical community removes itself from the policy discussion and the policy community shrouds vital technical details from comprehension. This dichotomous state of affairs is poisonous to successful “cyber” policy making. In short, while the “cyber” moniker is clearly over-leveraged within the

⁸ Take for instance various posts on well-read sites within the technical community: Geigner, T. “If Most Crime Involves A 'Cyber' Element, Can't We Just Call It Crime Instead Of Cybercrime?” Techdirt., 5 Mar. 2013, www.techdirt.com/articles/20130304/06541422191/if-most-crime-involves-cyber-element-cant-we-just-call-it-crime-instead-cybercrime.shtml.; 1 Aug 2004 | 4:00 GMT, Paul McFedries. “The (Pre) Fix Is In.” *IEEE Spectrum: Technology, Engineering, and Science News*, 1 Aug. 2004, spectrum.ieee.org/at-work/education/the-pre-fix-is-in.; For a less technical perspective from a more journalistic source see Yadron, Danny and Jennifer Valentino-DeVries. “This Article Was Written With the Help of a ‘Cyber’ Machine Overuse of prefix sparks a backlash, but alternatives are few; ‘computery’” *The Wall Street Journal* 5 March 2015 available at: <https://www.wsj.com/articles/is-the-prefix-cyber-overused-1425427767>

policy and social science academic world, and is sometimes frowned on the technical world, it will become increasingly necessary for both worlds to forge a common understanding.

The disconnect between social science and policy makers on one hand and the technical community on the other hand is wholly understandable. Society has embraced the integration of computing into their daily lives; there remains and likely always will remain a gap between those who can be considered experts and aware of the security implications of computing architecture and the general public. The concern with computer literacy has been a pervasive concern since the advent of personal computing, however despite that, by some measures progress has lagged.⁹ Both professional and non-professional use of computing remain replete with error-laden misunderstandings of the fundamental construction of computing systems and networks that manifest in varieties of confusion and imprecision during subsequent discussion and analysis. While not the subject of this dissertation, one need only look at the debates and discussions surrounding the application of deterrence theory to world of cyber-security. Concepts such as “counter proliferation” and “transparency” have contested meanings and even more contested implications across an ever-widening field of literature that emanates from an ever more diverse range of interested computing, engineering, social science academic, policy interested constituencies, and many others.¹⁰

⁹ For historic context see: Seidel, Robert J., et al. *Computer literacy: issues and directions for 1985*. Academic Press, 1985.

¹⁰ See for example, authors such as Libicki who is skeptical that cyber war grand strategy can or should evolve due, in part, to the contested nature of the domain: Libicki, Martin. “Why Cyber War Will Not and Should Not Have Its Grand Strategist.” *Strategic Studies Quarterly*, vol. 8, no. 1, 2014, pp. 23–39., also see the various debates in: National Research Council, et al. *Proceedings of a workshop on deterring cyberattacks: informing strategies and developing options for U.S. policy*. National Academies Press, 2010.

Computer technology is utterly pervasive in modern societies. Home users face a plethora of technical challenges in network and system configuration and administration due to the market in smart phones, tablets, network-aware entertainment devices, and personal computers. Lawmakers must legislate markets, and socio-political boundaries of permissible action regardless of their individual levels of specific domain knowledge in the fields of hardware architecture and software design. Corporate users must utilize a variety of office productivity suites, enterprise resource planning systems, and internal operations tools. Military users interact daily with a multitude of network-centric devices, many of which are *not* independent of more public networks. At all levels of modern society command and policy decisions must be made about the nature and disposition of information technology, yet there exists a pervasive lack of universal education in technical issues regarding IT systems. For example, if you use the Advanced Placement tests given to US high school students to approximate undergraduate curriculum, AP Computer Science still lags far behind calculus as a technical subject of basic study (though that number is trending upward historically).¹¹ This means technical knowledge of computing let alone robust technical understanding of security revolving around information technology is not universalized nor will it become so anytime soon. Therefore, one can safely conclude the ambiguities surrounding the prefix “cyber” are not likely to converge on an easily understood, widely accepted, and applicable definition across technical and non-technical constituencies.

That observation isn’t a critical assessment with negative intention, it is simply the natural state of affairs leading to the following conclusion: “Cyber” doesn’t exist as an easily identified domain drawing from a well understood ontology. Instead the idea of a “cyberspace” and thus the

¹¹ AP Archived Data 2016 Summary Report available at:
<https://research.collegeboard.org/programs/ap/data/archived/ap-2016>

domain of “cyber-security” is contested and not easily disentangled from any number of context specific usages.

1.4 Information Security Management

To sidestep the debate over what “cyber-security” means, a substitution can be made to analyze “information security management” at various levels of analysis and abstraction. The latter term being drawn from the computational and information technology disciplines and defined using the well-established McCumber Cube model of information security management. The model is often taught to students of information technology and computing to frame security along multiple dimensions of organizational foci. Information is conceived as being in one of three stages: storage, processing, or transmission. Each of these three stages is given an axis in the model’s representation. In addition, information can be compromised in any combination of three ways defined by, confidentiality, integrity, and availability.¹² The U.S. National Institute of Standards and Technology (NIST) gives the following definitions of objectives for each dimension:

- *Confidentiality* – “Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information”
- *Integrity* – “Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity.”

¹² Over the past two decades, this model has been firmly ensconced within computing security, however for a general overview of the model see: Maconachy, W. Victor, et al. "A model for information assurance: An integrated approach." *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*. vol. 310. New York, USA, 2001.

- *Availability* – “Ensuring timely and reliable access to and use of information.”¹³

The combined six dimensions can be represented as such:

	Storage	Processing	Transmission
Confidentiality			
Integrity			
Availability			

Figure 1: Simplified Model of Information Security Management

Within this conception, security is envisioned as being managed in a holistic way that pays attention to each intersecting state of information through each possible vector of compromise. The traditional McCumber Cube adds another three dimensions turning the above two-dimensional grid into a three-dimensional shape, however for the purposes of this discussion, the simplified model shown above will suffice. Using this as a heuristic, the definitional quandary resulting from the ill-defined term ‘cyber-security’ can be avoided by focusing on the constituent make-up of all

¹³ NIST FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems available at: <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>

things ‘cyber’, which is of course: information. Security is thereby incumbent upon maintaining the confidentiality, integrity, and availability of information as it is being stored, transmitted and processed. This does not change whether a computer scientist, CTO, political scientist, or layperson is discussing a ‘cyber’ prefixed topic. It also does not change as discussion moves away from computing hardware to ever more abstract levels incorporating political, cultural, and social dynamics and aggregations. In the end, ‘security’ comes down to assuring the six dimensions above are addressed for information at all levels of analysis, from individuals to the systemic level of nations-states and the various electronic networks intertwined therein. The next section will introduce a layered model of cyberspace to help further refine the domain of analysis.

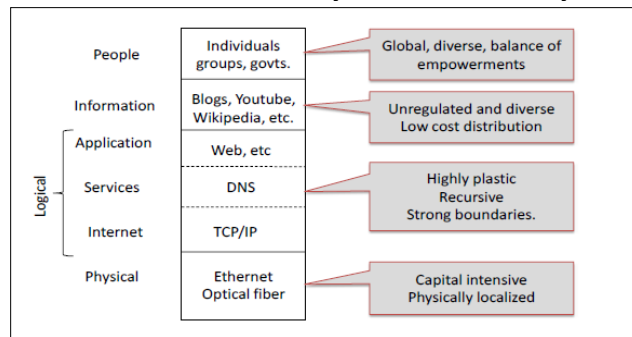
1.4.1 Layered Model of Cyberspace

Choucri and Clark build upon the traditional layered model of the Internet in order to establish a typology of analysis that integrates, according to them, traditional international relations levels of analysis with ‘cyberspace’. Specifically, they’re concerned with identifying a method of analysis that can be used to understand “cyber-actors” in terms of power relations across specific points of control that vary between conceptual layers. Each layer relies additively on those appearing below to function. At the lowest level is the physical infrastructure upon which cyberspace functions such as optical fiber and other hardware. Above that sits the ‘logical’ layer, itself made up of three sections, the Internet, Services, and Applications. The TCP/IP packet protocol, for example, is part the ‘Internet’¹⁴. The Domain Name Service (DNS) which translates numeric

¹⁴ The term ‘Internet’ is used throughout this chapter and dissertation to mean either a stratum of the logical layer within the discussed model or the larger socio-technical construct incorporating the world wide web and other various information technology related communication which characterizes modernity. The attempt has been made to be distinguish clearly between meanings within the prose around which the term appears.

addresses into the Uniform Resource Identifier (URL) commonly associated with specific internet addresses which end in ‘.com’, ‘.org’ etc. is the middle of the logical layer. The application layer consists of what we commonly conceive up as the ‘web’ or the graphical and searchable portion of the Internet. The model then incorporates two top layers. The first is labeled, quite simply, ‘information’ and represents, “encoded text, photos, videos, and other material that is stored, transmitted, and transformed in cyberspace,”¹⁵ At the very top, ‘people’ represent users and constituencies “who shape the cyber-experience and the nature of cyberspace itself.”¹⁶ Choucri and Clark present the following graphical representation of their model:

Figure 2: Choucri and Clark Layered Model of Cyberspace¹⁷



Traditional levels of global political analysis include the individual, state, and systemic (international system of states). Choucri and Clark introduce the following dimensions: 1) Global which is non-state centered but global in nature (such as the issue of spam), 2) Non-profit and 3) Profit-seeking. The layers discussed above can be analyzed across the various levels of analysis. Their “Integrated Cyber-IR System” appears below, the ‘logical layer’ appears in dark grey.

¹⁵ Choucri, Nazli, and David D. Clark. "Integrating cyberspace and international relations: The co-evolution dilemma." (2012) available at:

http://ecir.mit.edu/images/stories/Clark_WORKSHOP.pdf

¹⁶ Ibid.

¹⁷ Choucri and Clark 2012, p. 3

Examples of issues and actors are slotted into the matrix for illustrative purposes some of which appear in Choucri and Clark’s similar graphic. Not all spaces are filled. The idea is to use the matrix to understand an issue or cyber-actor as a function of where they sit within the layers of cyber-space and the levels of analysis.

Table 1: Choucri and Clark Integrated Cyber-IR System

	Individual	State	International	Global	Non-profit	Profit-seeking
People		Military Use	NATO/ EU			
Information		Censorship		Spam		Information Control
Applications					W3C	
Services					ICANN	
Internet					IETF	
Physical	Home Wiring		Telecommunications regime	Satellite Orbits and Spectrum		Infrastructure companies (L3, Verizon, etc.)

The additional nuance that can now be added to their ‘integrated’ system is the earlier described notion of information security management. Instead of trying to define ‘cyber-security’ across all the various and interactive layers and levels, ‘information security management’ can be thought of as having *implications at each level*. At each of the intersecting (and through combinations of) dimensions, information’s confidentiality, integrity, and availability can be compromised as it is being stored, transmitted, and processed. The two concepts together, the notion of information security management and a simplified heuristic representing a combined Cyber-IR system, defines the domain within which security provisioning activity occurs. A security threat on/for the Internet can now be easily identified as: *Issues that impact the confidentiality, integrity, or availability of information across the Cyber-IR system as its being processed, transmitted and/or stored.*¹⁸

¹⁸ This definition may seem deceptively simplistic. However, the combination of McCumber Cube and the Choucri and Clark Cyber-IR system is a novel synthesis being offered here for the

1.5 Information Centered IR Security (ICIRS) Model

Figures 3 and 4 below consist of synthesis graphics that can help one understand the various dimensions discussed above and how they interact.¹⁹ Figure 4 combines the layered model of the Internet with the dimensions of security while focusing on the information as a “first principal.” The logical layer is depicted as a single entity for simplification though it should be noted that the conceptual applications, services, and internet layers subsumed within the logical layer are all still analytically important as separate entities. The “information layer” from the Choucri and Clark model has been placed at the center of the diagram to help indicate importance. The states of storage, transmission, and processing have been augmented with a new state labeled “creation” to introduce a vector of consideration around information that is new enough to give rise to hitherto unseen security concerns. One example would be the advent of social media, which can be argued as having created a myriad of security concerns as various levels of analysis are crossed. The McCumber cube model has also been augmented with the dimension labeled “repudiation” to capture the importance of trust in information’s veracity at more abstract levels. In adding both *creation* and *repudiation* to the model, emerging issues such as “fake news” spread through social media can be analyzed in a more nuanced fashion. This dissertation does not explore such issues in depth, but the model is nonetheless meant to have larger general applicability than the present work.

first time. The idea is to define security for and on the Internet *in the simplest manner possible*. In doing so, subsequent analysis of security provisioning can be driven by tracing the issue across the various levels and layers of the Cyber-IR system and understanding the specific dimension of information security management impacted and addressed during the course of provisioning activities.

¹⁹ This representation using concentric circles across physical and logical layers is influenced, in part, by conversation with and work by Steven Bigham, a cybersecurity industry professional. It is incorporated here with permission.

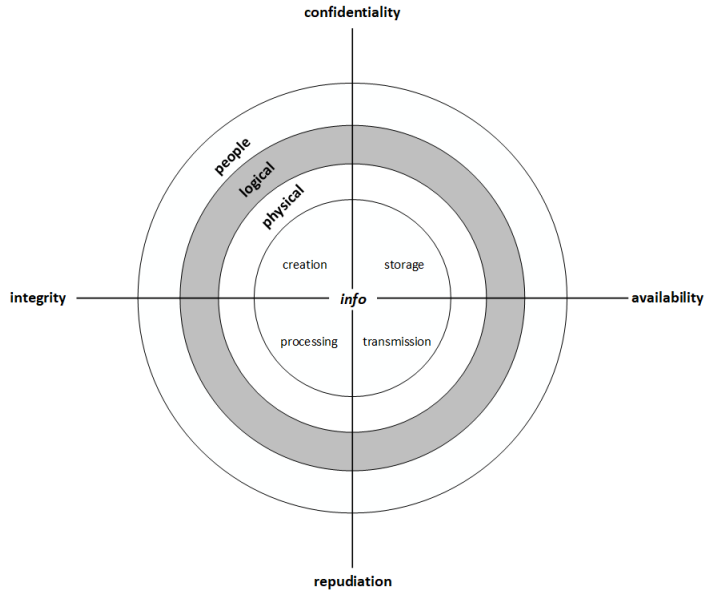
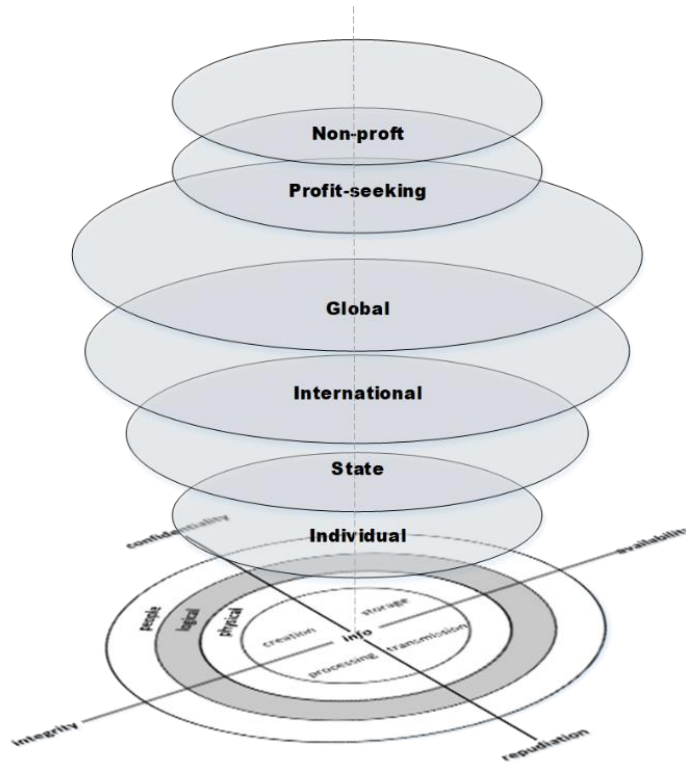


Figure 3: Information Centered Security Model

Figure 5 appearing below combines the information centered security model with the earlier outlined levels of analysis, which makes apparent that information centered security has implications at each level; analysis can be carried out with each level as a lens, much in the same way current IR scholarship utilizes traditional levels of analysis. This represents the Information Centered International Relations Security model or ICIRS which is pronounced *Icarus*.

Figure 4: Information Centered IR Security (ICIRS) Model



The obvious question to ask at this juncture is why use the ICIRS model as an analytic heuristic helping define the domain under examination within this dissertation? There is good reason to, the ICIRS model makes obvious how the idea of *information security* can be thought about as having implications within, and interacts with, a series of conceptual buckets that are well understood to scholars of International Relations. The conceptual buckets include conceiving of international politics as an activity carried out both between and within States while also interacting with both State and non-state institutions and constituencies. In shifting away from the ill-defined terminology of “cyberspace and cybersecurity” towards an information centered security model, the ICIRS model can drive exploration of foundational IR security concepts such

structure, agency, identity, and power. The model is still useful to analyze power relations across various control points of control similar to the Choucri and Clark model, however its utility is vastly augmented by representing threat and focusing on information thus further defining the “cybersecurity” conceptual space. Concerns of information security can be analyzed across several of levels of analysis as they interact and impact upon the various networks, institutions and hierarchies that exist across individual, state, international, global, profit-seeking, and non-profit levels of analysis. Importantly, each of those levels can be further segmented according to the nuances inherent within the logical layers: application, services, and, internet as information in various states (creation, processing, storage, and transmission) passes over physical infrastructure and interacts within the world. The next chapter will begin to assemble a larger framework around the ICIRS system to investigate the phenomena of collaborative security provisioning. The chapter will also review previous work on collaborative security and cyber security relevant to international relations in order to seat the usage of social practice literature, later in this work, within a larger theoretical context.

CHAPTER 2. SOCIAL PRACTICE: AGENCY, STRUCTURE AND CULTURE

2.1 International Security and ICIRS

As alluded to above academic explanations of international affairs are often organized across various “levels of analysis,” popularly these consist of the individual, the nation-state, and the systemic (system of nation-states). Within this system of levels, geopolitics are analyzed and explained, in-part, through assessments of structure, differential agency amongst actors, and involved cultural identities. Structurally, pertinent analysis may involve typologies of power and attendant benefits for those whom wield more power (as both the result of and product of position within a structural hierarchy) and disadvantages for those whose power is lacking. Power, itself, can be defined relative to other actors within a system or in absolute terms depending on school of theory being applied. Theories falling loosely under the rubric of Realism sometimes define power as “anything that can instantiate and/or maintain control of man over man”.²⁰

Institutionally, drawing on liberal theories of international relations, agency is another pertinent concept that can be useful for understanding the ability (perhaps better defined as capacity) of one entity to exert influence over cooperative initiatives and structuring decisions; be such an entity an individual within a collective, an institution within a system of institutions, or a nation within a system of nation-states. Lastly, generalizations about collective social proclivities are often manifested as typological distinctions labeled identities. In the most basic sense, tendencies toward cooperation or competition (and conflict) may be, within the tradition of

²⁰ Morgenthau, Hans J. *Politics among the nations: the struggle for power and peace*. Alfred A. Knopf, 1972.

ideational explanations, attributed to the existence of identities, which are either complementary or divergent respectively. These explanations do not represent a contiguous spectrum, far from it in fact, the discipline of International Relations could easily be viewed as competition for dominance amongst them, and maddeningly they are not mutually exclusive either. Often, they are invoked in combination with each other across levels of analysis to help explain international phenomena.

Security is a foundational concept within international studies. Often, security is conveyed as “high politics” which is to say, it occupies a central position within the spectrum of responsibilities expected of a State apparatus. When defined relative to stability, threat can be seen as the propensity (overt or covert) of one’s opponent to seek additional power which will, by its very nature, diminish your own according to Realist IR theorists and derivative schools of thought. Thereby the term *security* derives from this idea of threat. A *secure* environment is one that is *stable* and is characterized by the absence of threat. As discussed previously, States are presented with a paradox by placing “cyberspace” next to other strategic domains due the inherent differences between the non-constituent nature of the information space versus the well understood physical spaces that make up the four other domains. Security within and for the other domains is ensured, at the most basic level, by states maintaining an ability to move with impunity and maintain a position of force dominance within those physical spaces. The obvious question is then raised, how are the concepts of power and agency followed subsequently by security, defined within the strategic domain of cyberspace with regard to international relations?

The notion of power being rooted in structure and/or agency is inherent within the ICIRS model defined above. Joseph Nye’s neoliberal conception of power can be easily ported to the cyber context, and in fact, he has done so himself writing: “Cyber power behavior rests upon a set

of resources that relate to the creation, control and communication of electronic and computer based information”²¹ going further to state “defined behaviorally, cyber power is the ability to obtain preferred outcomes through use of electronically interconnected information resources in the cyber domain.”²² Nye identifies that cyberspace exists as a set of layered physical and virtual domains, though his writings on the subject don’t explicitly conceptualize the system as it is defined within this dissertation. The idea of power must be thought of as having various implications at the different layers and levels of analysis within the ICIRS model. One large facet of power within that system can be easily identified from the earlier conversation of threat. Entities that can 1) recognize threats and 2) act to effectively remediate those threats are then powerful within the context of that system, and by extension the real world. Certainly, the opposite is true as well, entities that can successfully project threat and harm also possess a dimension of power. It will be shown later in this work that a community of practice has arisen around the need to provide for recognition and remediation of large-scale threats to the Internet. Parts of that community may overlap with State resources, but large portions also exist independent of exclusive control of any single State. The usage of communities of practice will allow for conceptual bridges between traditional international relations theory and cyber-security. Using the ICIRS model defined above, *structure, agency, identity and power* can all be systematically explored within the context of security provisioning on/for the Internet.

The management of information security has implications across the levels of analysis and constituent layers of the combined international relations and information security model that has been presented. Clearly, the act of provisioning security across the entirety of that system cannot

²¹ Nye Jr, Joseph S. *Cyber power*. Harvard University Cambridge MA, Belfer Center for Science and International Affairs, 2010

²² Nye (2010)

be explained fully within the present work alone. This dissertation is only concerned with exploring security provisioning activities that occur to address *large-scale* problems arising on the Internet. The precise measure of what can be considered large-scale is purposefully not defined. Instead, an imprecise measure is used which is: problems that impact a significant portion of Internet users and impede the function of the Internet in a non-trivial manner.

These problems are numerous and occur with relative frequency.²³ Malicious software that either steals information or harnesses a computer's resources to perpetuate further criminal activity are common examples. As are problems that arise due to fragilities inherent in how the Internet is engineered. For example, the issue of Border Gateway Protocol (BGP) routing errors that will be discussed at length later in this work. Rather than define this class of problems here, specific case references appearing later in this dissertation will help further explicate this class of security threat. In addition to the scale of damage/impediment, this dissertation is chiefly concerned with security provisioning activity that is international in nature. This means, in the course of addressing these large-scale problems, individuals and entities involved engage in a measure of international collaboration at some point during the incident/case being studied. That in and of itself isn't an arbitrary requirement, but one that is inherent due to the nature of the Internet. Threats are often not confined to one geographic location but are, in fact, distributed internationally. Understanding the community of practice involved in the collaborative provisioning of security on/for the Internet helps further define and operationalize a facet of power regarding "cyberspace" as conceived of by Nye and other theorists and practitioners. Having established the domain and activity under

²³ For numerous examples see: Healey, Jason. *A fierce domain: conflict in cyberspace, 1986 to 2012*. CCSA, 2013

examination, the next section will place security communities of practice within a larger body of international relations and social theory.

2.2 Security Provisioning Networks

Consider the *Network*. As a concept, abstraction, and metaphor, the *network* is having its moment in the sun, though according to some, that moment may even already have passed in a blur. Given the centrality of digital networks to everyday existence, the pervasive application of the network moniker to other domains isn't particularly surprising. Conceptually, networks, have reached buzzword status within the popular, let alone academic, zeitgeist. They're conceptually easy to understand, and highlight the operationalized mechanism du jour, the *relationship*. This is to say, nodes connected in a relational graph, either explicitly conceived or abstractly referenced are thought to highlight import facets of modern social and socio-technical structure. Network metaphors aside, collaborative forms of security have long been a feature of the international system and the study of how such mechanisms emerge, evolve, dissolve and sustain themselves is a topic of scholarly political and social science research. Historically, this research centers on bilateral and multilateral alliances and/or the balancing against or around such arrangements, focusing on the state as the central unit of analysis. More recently, scholars have tried to incorporate sub-state interaction into analysis of not just security collaboration but of international behavior in general. In the largest sense, schools of theory such as Constructivism have tried to incorporate intersubjective meaning across the levels of analysis allowing for sub-state actors to play central roles in shaping behavior and thus inter-state interaction.

At the mid-level of theory building, the idea of informal networks that exist across political boundaries has gained some traction. Slaughter, for example, focuses on governmental networks

that exist between states comprised of low and mid-level bureaucratic elements within their respective governments.²⁴ Gerspacher and Dupont detail “the nodal structure” of international police cooperation, characterizing informal initiatives pursued by law enforcement agencies outside of formal state to state mechanisms.²⁵ Analysis within the present work conceives of the various constituencies involved with the provisioning of security on/for the Internet as a form of social practice within communities of practice that interact across “seams” aggregated as a “security provisioning network. Literature emanating from social science and international studies seeking to explicate network collaboration must be explored to establish a detailed basis for the conception of such a network

2.3 Social Practice

Information security provisioning is referenced within this dissertation as an “embedded social practice.” That formulization derives from a tradition within sociology and political theory that relates group behavior, intersubjective meaning, preferences, incentives, and outcomes to individual agency. In short, an embedded practice is established within a *cultural context*. Victoria Hand writes, “Sociocultural or situative perspectives conceptualize culture as being located in the joint social activity of individuals as they do work together, use tools, solve problems, and reify the meanings of their activities.”²⁶ Social practice then is an operationalized expression of that cultural context. Specifically, social practice comprises of language, tools, procedures, norms,

²⁴ Slaughter, Anne-Marie. *A New World Order*, Princeton University Press, March 2004.

²⁵ Gerspacher, Nadia, and Benoît Dupont. "The Nodal Structure of International Police Cooperation: An Exploration of Transnational Security Networks." *Global Governance* 2007: 347. JSTOR Journals. Web. 28 Jan. 2015.

²⁶ Hand, V. (2006). Operationalizing Culture and Identity in Ways to Capture the Negotiation of Participation across Communities. *Human Development*, 49.1, 36.

subtle gestures, word-views, and other explicit and implicit signs of community membership.”²⁷

Understanding security provisioning on or for the Internet requires an analytic framework that describes how the activity is shaped, influenced and co-constituted within a community of practice. This community of practice centers on security and an evolving response to perceived threats based on interactions across boundaries with other constituencies and communities of practice from other domains.

Above, it was noted that this dissertation takes a pragmatic approach to analysis. The approach is pragmatic because it does not try to project or presuppose intentions upon the individuals and entities under study. Instead, it is first concerned with what those entities do. Meaning, the analysis is rooted in understanding the social practice of provisioning security and how that practice represents and generates a specific and discernable culture. Analyzing that culture means explicating the working practices, problem solving indications, language, tools, explicit and implicit meanings generated by a specific constituency of individuals. Social practice literature represents a response to a supposed rationality bias which has dominated social theory over the past several decades. Vincent Populiot writes:

“...most of what people do, in world politics as in any other social field, does not derive from conscious deliberation or thoughtful reflection – instrumental, rule-based, communicative, or otherwise. Instead, practices are the result of inarticulate, practical knowledge that makes what is to be done appear “self-evident” or commonsensical. This is the logic of practicality, a fundamental feature of social life that is often overlooked by social scientists.”²⁸

²⁷ Hand (2006) p.38

²⁸ Pouliot, Vincent. "The logic of practicality: A theory of practice of security communities." *International organization* 62.2 (2008): 257.

Populiot proposes that “the logic of practice” helps fill a gap in the explanatory toolkit of social science which normally explains social action as deriving from, 1) instrumental rationality (logic of consequences), 2) norm-following (logic of appropriateness), or 3) communicative action. (logic of arguing). Importantly, according to Populiot, the logic of practice is ontologically prior to the other three due to its location at the intersection of agency and structure. Whereas both instrumental rationality and communicative action derive from individual agency, and norm-following is overly determined by an ideological super-structure, the logic of practice allows for an eclectic blending along the agent-structure spectrum.²⁹ That being said, the logic of practice is complementary to the others and Populiot is advocating using it as such. Practice, in many ways, can be easily understood as “tacit knowing” which allows reflexive actions. This is useful because it allows analysis to follow naturally from observing regularities or differences in the way action is carried out instead of trying to discern indications of an ideological frame. This isn’t to say that intersubjective meaning isn’t important or doesn’t exist, but is to say that focusing on practice doesn’t rely on extrapolating representational knowledge from indirect indications. It instead allows behavior that aligns across a constituency to serve as an indication of a culture comprised of social practice. Quoting Zerubavel, Populiot discusses representational bias: “...social scientists sometimes ascribe rules to the actor when it is only the actor’s behavior that is being described. In many cases in which behavior is described as following rules, there may be in fact no rules inside the actor.”³⁰ The types of behaviors referenced here are diverse. These can include a choice regarding the type of community or collaboration chosen to address certain problems. For example, the designation of a ‘working-group’ or the choice of one amongst a number of

²⁹ Ibid.

³⁰ qtd. in Populiot (2008), 268

possible partners. These types of choices are examples of abstract goals reified into practical solutions. This shift from representational and ideational knowledge to behavior as an indication of practice is necessary when analyzing information security provisioning activities due to the complex, diffuse, and largely unmapped structure. These provisioning networks are surrounded by the ideological flux the ‘cyber’ domain engenders. That complexity precludes analysis that starts by trying to understand structure first and agency second. By defining Internet security provisioning as an embedded social practice, one is able to define a collection of people who engage on an ongoing basis in some common endeavor that are bound not by virtue of a shared abstract characteristics or through simple co-presence, but by shared practice.³¹ This collection can be termed a “community of practice” and is discussed below.

2.3.1 Security as Practice

Using the ICIRS model and social practice as a starting point, the thrust of this dissertation defines the Internet security provisioning community as a constituency whose actions constitute “practice” and follow from a distinct culture. Later in this dissertation that culture is separated into two levels, one which operates at a systemic level (with regards to the Internet) and one that emerges to address specific problems. This leads to a security provisioning network fashioned across multiple separate constituencies and conditioned by the specific context within which each node is embedded. Conceptually, communities of practice help define the boundaries of each distinct constituency being examined. Members of a community of practice are not simply individuals that share an interest instead, “...members of a community of practice are practitioners. They develop a shared repertoire of resources: Experiences, stories, tools, ways of addressing

³¹ Eckert, Penelope. “Communities of Practice” appearing in the *Encyclopedia of Language and Linguistics* (2006)

recurring problems – in short a shared practice. This takes time and sustained interaction.”³² Etienne Wenger and Jean Lave developed the concept as way to understand learning in social settings. The concept is widely leveraged in organizational and sociological literature and was developed from the perspective of cultural anthropology. Originally it was leveraged to explain the type of learning occurring during apprenticeship, and the term community of practice referred to the “community that acts as a living curriculum for the apprentice.”³³ The concept has been further subsumed and incorporated into (relatively) recent international organization literature emanating from political science disciplines and generally referred to the as “practical turn.”³⁴ Within the present work, communities of practice provide a way to operationalize social practice within the analyzed sets of social actors. The following characteristics of communities of practice are identified by Wegner:

- “Communities of practice enable practitioners to take collective responsibility for managing the knowledge they need recognizing that, given the proper structure, they are in the best position to do this.
- “Communities among practitioners create a direct link between learning and performance, because the same people participate in communities of practice and in teams and business units
- “Practitioners can address the tacit and dynamic aspects of knowledge creation and sharing, as well as the more explicit aspects
- “Communities are not limited by formal structures: they create connections among people across organizational and geographic boundaries.”³⁵

While those characteristics are specifically formulated about business communities, the characteristics are easily ported to alternative contexts. Operationalizing such characteristics can

³² Wenger, Etienne. *Communities of Practice: a brief introduction*. (2009)

³³ Wegner (2009), p. 3

³⁴ Feldman, Martha and Wanda Orlinkowski "Theorizing Practice and Practicing Theory." *Organization Science* 22.5 (2011): 1240-253.

³⁵ Wegner (2009)

be done by looking for specific instances of: 1) problem solving, 2) explicit acts of seeking out experience through social networks, 3) reusing assets across problem-sets, 4) coordination and synergy through combining efforts amongst actors, 5) active discussions amongst a set of linked practitioners, 6) documentation of processes to codify skills and document resources, and 7) mapping knowledge to identify gaps through intentional interrogation of knowledge networks to establish baseline understanding amongst practitioners.³⁶ This non-exhaustive list describes indications of shared practice amongst a discrete group of actors/entities.

The lens of practice is only just now being applied to the study and continued operation and security of the Internet. Ashwin Matthew's 2014 dissertation in the field of information and human geography argues that stability of Internet infrastructure relies on "distributed governance" of technical communities connected both within themselves and amongst communities by reciprocal trust relationships. He extends this argument to discuss trust in technology, trust in institutions, and trust in processes that have evolved across the communities, technologies and institutions.³⁷ More recently Matthew revisits the ideas of trust and practice to describe the cybersecurity space as a "fragmented whole" that relies on a community of practice characterized by trust to execute cybersecurity. In doing so he is further extending his dissertation research from the network operations space to the cybersecurity space.³⁸ Matthew also draws on the communities of practice literature of Wenger and Lave to operationalize security execution referencing the idea

³⁶ Synthesized from Wenger 2009, Wenger and Lave 1990, Friedrichs and Kratochwil (2009), Brown and Duguid (1991), Adler and Greve (2009)

³⁷ Synthesized from Ashwin. (2014). Where in the World is the Internet? Locating Political Power in Internet Infrastructure.

³⁸ Mathew, Ashwin & Cheshire, Coye. (2018). A Fragmented Whole: Cooperation and Learning in the Practice of Information Security. Available at: <https://www.ischool.berkeley.edu/research/publications/2018/fragmented-whole-cooperation-and-learning-practice-information-security>

of problem solving. The recent work does not robustly establish the communities of practice elements it claims to draw from, instead the claim is established in a few short paragraphs contained in the appendix to the paper. The paper's main accomplishment is presenting data gathered through surveys and interviews, which establish the characteristic of trust as a central element of a community of practice centered on information security. Matthew's work reinforces the claim argued in this dissertation that conceives of communities of practice as the way in which large scale security is addressed on/for the Internet, instantiating a constituency to problem solve and reify shared goals into action. However, while Matthew makes ontologically similar social science-based arguments to the present work, Matthew's work leaves several gaps, 1) Trust, while a central characteristic of the communities of practice under examination, is but one dimension amongst many that define the space. Others can be derived from the larger body of social practice literature and include language, world views, normative behaviors, and others. 2) What Matthew terms distributed governance, and herein is termed 'distributed agency', intersects and interreacts with multiple dimensions across the levels of analysis defined within the ICIRS model, and should be analyzed as such. 3) Communities of practice within the information security space necessarily interact in due course of problem solving with a plethora of communities, individuals, entities and institutions that are outside of the trust relationships Matthew identifies. This fact is also inherently obvious when using the ICIRS model to analyze the case studies that appear later in this work. How then, can these necessary and important interactions be operationalized for the purposes of understanding?

Explaining how that process is structured rests heavily on the idea of "seams". Seams are simply boundaries that exist between culturally distinct sub-sets. As social networks (addressing Internet security) are built across and amongst other distinct constituencies, seams become an

important nexus forcing decisions related to the structure, direction, tenor, and design of burgeoning collaborative environments/communities. Additionally, the concept of seams serves as a useful abstraction connecting the socio-theoretical underpinnings of this analysis to the above elucidated ICIRS modes. Levels of analysis and above discussed ‘layers’ of the Internet can be considered helpful signposts at which to look for important seams. The intersection of the dimensions of information security management, similarly, help identify other important seams. The next section will introduce and operationalize the idea of seams.

2.4 Organizational Seams

The term “organizational seams” refers to boundaries between separate organizations or their component sub-organizations, the boundaries arise due to anything that can inhibit free and easy communication/coordination. Seams are a natural by-product of the need to specialize, to provide for division of labor, or to divide gross organizational size into more manageable parts. The concept was developed by Salomone and Crecine to analyze NATO forces drawn from various national militaries that were pursuing coordination and interoperability in the central region of Europe during the Cold War, and extends the work of Simon, Cyert, and March in the 1950s and 1960s that looks at organizational behavior.³⁹ Seams, conceptually, make intuitive sense, in that whenever two or more distinct organizations or sub-components of an organization(s) interact, information must pass between the sets. That “chasm” across which communication and resources must flow is a “seam”. The sources of seams abound and as similarities give way to differences, seams will multiply. This framework extends the idea of specialized division of labor necessitated

³⁹ Cyert, R, March, J. *A Behavioral Theory of the Firm*. Wiley-Blackwell, 1963; March, J, Simon, H. *Organizations*. John Wiley, 1958; The Seams framework is derived from the work of, and used with permission from, Crecine and Salomone, (unpublished manuscript, 1991)

due to limits in a rational actor's cognitive capacity, a hallmark of the Carnegie School of management literature. When applied to the realm of cyber security provisioning, the seams framework helps discern a central structuring mechanism of the "patchwork" response system which has grown organically over the course of the Internet's evolution. That mechanism consists of two parts, one is the need to pass information and resources amongst partners involved in the threat recognition and remediation of large-scale problems (i.e. in order to accomplish task x, with whom do I need to collaborate?). The second part is the distinct context within which a single 'node' (individual, institution, and/or entity) is *already* embedded. Those two considerations then help drive structuring decisions defining the nature and specific instantiation of a security provisioning community of practice relevant to the problem/threat at hand.

These "seams" within and amongst organizations and their subunits can be either minor or major, depending on the dissimilarities of the organizations and subunits involved. The nature of the seams can either enable or constrain attempts at coordination. Entities involved in provisioning security across cyberspace are not homogenous in terms of their goals, incentives, and disincentives. In fact, their own unique organizational culture, their standard operation procedures, and their internal supervisory controls all condition the way in which they coordinate with other entities. This helps explain the range of outcomes and pathways possible during instances of security provisioning. The seams within the patchwork response mechanism and involved constituencies can result in the *cyber response coordination problem*, named to highlight the inherent difficulty of managing security response across the patchwork system.

Coordination can be defined rather simply as the management of interdependent relationships that necessitates the exchange of information in order to align actors' intentions, goals, and actions. The coordination problem with regards to the cyber security patchwork relates

to the overlapping institutional and inter-institutional make-up of necessary resources brought to bear on both the threat recognition and remediation phases of any particular cyber security problem/event. Writing with regard to Computer Emergency Response Teams (CERTs) which will be discussed further later in this work, Choucri et al. argue the primary inhibitor to using CERTs as a vector for cyber security coordination regards hesitation among members making data available across their cohort of partners.⁴⁰ Many private companies that participate in such collectives are hesitant to share cyber vulnerability intelligence due to fear or reputational harm. This is but one example of the coordinative inhibitions that plague the cyber response patchwork leading to characterization of the space as “ad-hoc” shifting and/or abstract. The patchwork remains hard to categorize in unitary fashion. Empirically, too many involved entities and stakeholders exist to directly map, but that doesn’t mean structure is not present. The ICIRS system, along with the concept of seams, is aimed at helping discern, and give shape to that structure.

The application of seams within the cyber context is motivated by two observations. First, the cyber response patchwork consists of capabilities distributed horizontally across various technical, non-technical, private, public, domestic and international constituencies. Second, within the US context, cybersecurity has evolved in an ever more specializing manner that is continually creating additional seams while sometimes forcing change across others. This is obvious by observing the evolution of offensive and defensive cyber missions within the US military.⁴¹ Currently, for example, the recent elevation of a US Cyber Command to a full combatant command

⁴⁰ Choucri, Nazli, Stuart Madnick, and Jeremy Ferwerda. "Institutions for cyber security: International responses and global imperatives." *Information Technology for Development*.20.2 (2014): 96-121.

⁴¹ Healy, J. *A Fierce Domain: Conflict in Cyberspace, 1986-2012*. Cyber Conflict Studies Association, 2013

status may create new seams between Cyber Command and the subunits it will now direct while also widening existing seams between US Cyber Command and its antecedent organizations as relationships that have historically developed change, and as new seams are created by the new structure.

Solving the coordination problem becomes even more difficult if there are both inter- and intra-organizational coordinative necessities, as with the cyber domain in which seams exist within organizations and between several disparate organizations. The cyber response infrastructure has intragovernmental seams, interagency seams, international seams, and seams between the private and government sector, among others. Currently the cybersecurity response infrastructure has not institutionalized a structure that can fully solve or ameliorate the coordination problem within its domain. These seams and the multitude of stakeholders with different interests and capabilities can create coordination problems complicating effective responses across the myriad of issues definable across the ICIRS conceptual space.

Even further, technology can exacerbate organizational seams and heightens the boundaries between individual organizational agents. Simply as a straightforward organizational issue, any new technology brings new standards, new information, and new capabilities, all of which must be integrated into existing technologies and practices. As an emerging technology, the cybersecurity space is further characterized by intense volatility and rapid technological evolution. When thought of in this manner, the current flux and continued evolution of the cybersecurity response infrastructure should lead to confusion.

Recognizing and responding effectively and efficiently to large-scale cyber mediated attacks requires a level of coordination across decentralized resources, a fundamental feature of

the Internet and information exchange networks. Within the public sector, each entity maintains its own information systems (i.e. computer systems, servers, and so forth), at multiple levels of classification, with ranging security protocols and policies. Consequently, there exist inherent challenges marshaling those resources that may not be directed by a centralized command scheme and instead be located within and across organizations not adept at coordinating with each other.

This obviously begs the question, how can one identify the important seams present with any set of issues or inherent to a particular situation or problem? This is where the ICIRS framework is useful to keep in mind. When parsing an issue or security threat and/or looking at a historical example of a remediation effort, it helps to focus on the exchange of information and resources across levels of analysis, and/or through various layers of the information centered security model (logical, people, etc.) to help drive seam identification. This can help illuminate places where an information gulf exists and some sort of coordinative reconciliation needs to happen. The case studies in subsequent chapters of this dissertation will further operationalize this.

It is important to note that there are other theoretical frameworks for understanding coordination in cyberspace. For example, Raymond argues that mitigation and management processes are essential in order to maintain internet stability and prevent disruptions. Consistent with the seams framework presented in this dissertation, Raymond finds that these challenges are due, in part, to the large number of rules and the involvement of a wide array of actors.⁴² He argues that decisions made by one actor could have “intended or unintended effects” on other actors. The combination of these effects with the decentralized nature of the regime complex can create

⁴² Raymond, M. Managing decentralized cyber governance: The responsibility to troubleshoot. *Strategic Studies Quarterly* 2016; 10:4 (Winter): 124.

coordination and conflict resolution problem.⁴³ However, Raymond suggests that coordination can occur and offers a solution to these problems, through the creation of a prohibition regime able to address threats in the international security realm. As noted above, coordination within this dissertation is defined as the act of exchanging information to align goals and intentions, and furthermore its definition here is in support of establishing the idea of practice within a community of practice. Admittedly, the concept isn't further defined in relation to related terminology such as "cooperation" and the terms are sometimes used interchangeably. However, the key idea is that information must flow across seams in order for problems to be recognized and remediated, those seams can be small or minor and help enable a solution or they can be large and major which will impede progress toward a solution. Chapter three and four will provide evidence of these coordination challenges and evidence of the emergence of a community of practice within the cyber security response system through an examination of the Internet's evolution and specific cases of security response. Before doing so, related work collaborative security on and for the Internet will be reviewed.

2.5 Related Literatures

The issue of cybersecurity and information security within the transnational security space is studied from a several of theoretical and academic perspectives. Some of those literatures related to this area are relevant here, both ontologically in terms of theoretical derivation and via examined content (security provisioning on/for the Internet) and are briefly reviewed and summarized below. Without a doubt, the theoretical lens of practice should be complementary to many of the efforts

⁴³ Raymond, 2016

detailed below. The ICIRS model is also useful as a tool to help sort and make sense of the level analysis and unit of analysis each of these literatures focus on.

One area of widespread agreement within the ambit of analyzing the modern socio-political security implications of the Internet is that the literature has yet to mature and is in its “infancy”. Often this means the existing literature suffers from any number of limitations despite making useful contributions to understanding the various facets of security on/for the Internet. Just as the idea that cyber-security is a contested term that makes it hard define analytically - taken as a whole- social science literature regarding cyber-security can be difficult to categorize systematically. Still, authors have looked at the Internet security provisioning space narrowly producing descriptive and nascent theoretical literature. Judged independently of the academic literature, information security infrastructure springing up around the Internet clearly indicates a rapid growth and an ever-enlarging scale. Early social science academic works were descriptive in nature and sought to describe the number of organizations and their role with respect to the Internet’s security mechanism. Those descriptive works didn’t extend to operationalizing that mechanism analytically for the production of deeper insights. More recent work does use theoretical frameworks to generate insight, the following sections will review a few bodies of literature that sit adjacent to or are complementary to the current effort. The purpose of discussing these works is to place this dissertation within the larger theoretical body of work looking at cybersecurity emanating from international relations social science.

2.5.1 Networked Governance

Mueller et.al. suggest that Internet security provisioned by non-hierarchical collectives represents a form of “networked governance” in international relations, using the cases of response

activities to the Conficker botnet and security surrounding internet routing as examples.⁴⁴ Networked governance is defined in their work through a discussion how the idea of ‘networks’ emerged as a separate organizational type distinct from markets and hierarchies before being applied to social relations and international affairs. The key distinction of networked forms of governance, according to Mueller et.al. is that actors are relationally linked and choose to collaborate in a manner that is not imposed from the top (hierarchy) nor based on transactional interaction in a market defined manner. The idea that network analogies are being utilized by social science in two separate ways is echoed by Kahler who separates two approaches termed networks as “structures” and networks as “actors”. When used to convey structural facets of importance, network theory uses formalized quantitative measures such as “embeddedness” and “centrality” to precisely describe a node’s structural relationship with regards to other nodes in formally defined network. However, when used in conjunction with the idea of networks as actors, Kahler defines networks in much the same way as Mueller et. al. According to this tact, “Networks are not treated as omnipresent features of social life,” but are a specific form of organization that is separate from the hierarchical organization of states.⁴⁵

This idea of entwining cyber-security and networked governance has a developed history. Prior to the above discussed works, networked governance is defined by Muller in his 2010 work Networks and States in which he draws connections between the organizational metaphor of networks and the regulatory features that allow the Internet to function within the modern system of States. Security is an area Mueller does spend time to develop, both through case study

⁴⁴ Mueller, Milton, Andreas Schmidt, and Brenden Kuerbis. "Internet Security And Networked Governance In International Relations." *International Studies Review* 15.1 (2013): 86-104.

⁴⁵ Kahler, Miles. *Networked Politics : Agency, Power, and Governance*. Cornell University Press, 2009.

exploration and theoretical discussion. Most relevant to this dissertation, he makes the following observations:

“(1) responding to cybersecurity problems involves highly scalable, difficult to-trace actions and distributed actors and attacks that easily cross national borders, which often exceeds the capabilities of national approaches to Internet governance; (2) the inadequacy prompts the development of new organizational arrangements that reconstitute relationships among business, government, and civil society in this sphere; (3) the successes and failures of these new arrangements pose novel political issues and governance problems that generate institutional change at the transnational level.”⁴⁶

This dissertation uses Mueller’s observations detailed above as a jumping off point to understand in a less abstract matter what sorts of organizational arrangements across government, business, and civil society provision security in the face of large-scale threats to the Internet’s function.

Most recently, Kuerbis and Badiei attempt to “map the cybersecurity institutional landscape” using a theoretical framework based on new institutional economics (NIE) onto which they graft the concept of governance structures. Their analysis connects the various activities performed under the rubric of cybersecurity as being part of an institutional landscape organized into three buckets: markets, networks, and hierarchies. This represents an extension of themes visited in the earlier work co-authored by Kuberis and touched on above.⁴⁷ Botnet mitigation (also utilized as a case study in this dissertation) is discussed briefly as an example in which all three structures are readily apparent as a form of successful cybersecurity provisioning. The paper is a useful abstraction of the provisioning space, especially as it helps define the diverse number of incentives emanating from various actors/entities involved within the space. Those incentives may

⁴⁶ Mueller, Milton. *Networks and States: The Global Politics of Internet Governance*. MIT Press, 2010. p183

⁴⁷ Kuerbis, Brenden and Farzaneh Badiei “Mapping the cybersecurity institutional landscape.” *Digital Policy, Regulation, and Governance*. 19.6, 2017, pp. 429–448.

lead to establishment of market, hierarchical, and networked organizational collectives that then address cybersecurity related issues.⁴⁸

Writing in the same journal volume in which Kuerbis and Badiei's work appears, van Eeten deftly points out the disconnect between the *discourse* of governance and the application of *control* as a direct outcome of governance. He shows that much of the debate surrounding cybersecurity governance seems to be divorced from the "actual provisioning of cybersecurity on the ground."⁴⁹ This begs the question, what connects the idea of "networked governance" to the actual provisioning activities which that place in the real world? To be sure, the case studies explored together and independently by Mueller, Mueller et.al., Schmidt and by many other authors help operationalize that connection. However, much of the emerging literature places Internet security response activities coordinated among transnational coalitions of public/private entities within a networked structure, while failing to discretely define nodes and edges due the explicit separation of "networks as structures" vs "networks as actors" and/or a distinct organizational type. Instead, such work theorizes about networks and hierarchies in the abstract, qualitatively describing what amounts to case studies or sketches lacking formal conceptualization as a network nor a robust understanding of how that network's ability to turn goals and intentions into "action on the ground" as pointed out by van Eeten. This abstract discussion of the Internet security provisioning space points to a conspicuous gap within the emerging literature, one that can be filled, with regards to security, with the concept of a "security community of practice" operating in a networked fashion as discussed below. To be sure, Mueller's body of work develops the network metaphor in relation

⁴⁸ *ibid*

⁴⁹ Eeten, Michel van "Patching Security Governance: an Empirical View of Emergent Governance Mechanisms for Cybersecurity." *Digital Policy, Regulation and Governance*, vol. 19.6, 2017, pp. 429–448.

to the governance of the Internet robustly and usefully. This dissertation seeks to add another level of nuance to better specify and understand the ‘network’ under examination. In order to do so, there must be a recognition that nodes within the provisioning network do not exist in a vacuum, this is to say each node is embedded in a specific social context that conditions and shapes interactions that they have with other nodes. This, in turn, gives rise to a unique problem solving/provisioning culture that influences subsequent interactions. The lens of practice can be seen as helping fill in the gaps around and complementing the network governance literature, thus addressing the space identified by van Eeten.

2.5.2 *Peer Production*

Andreas Schmidt speaks more directly to the specific issue of this dissertation by submitting that the production of internet security (by which he means the addressing of threats and problems) is currently going through a change in which collaborative networks are evolving hierarchies due to increased government intervention. Schmidt terms these networks “hybrids” referencing both the hierarchical and non-hierarchical elements of security production systems.⁵⁰ Schmidt is worth discussing further, as his work has followed from his own dissertation that looked at “social production” of internet security. He asserts that the type of security collaboration present, historically, on the Internet represents a unique form of distributed production indigenous to the information age, although his dissertation then moves on to focus on speculation about the concept’s future.⁵¹ Peer production, central to Schmidt’s argument partially follows Benkler’s

⁵⁰ Schmidt in Kremer, Jan-Frederik, and Benedikt Müller. *Cyberspace And International Relations : Theory, Prospects And Challenges* / Jan-Frederik Kremer, Benedikt Müller, Editors. n.p.: Heidelberg : Springer, (2014.),pp. 181-202. GT Library Catalog. Web. 27 Jan. 2015.

⁵¹ Schmidt, Andreas. *Secrecy versus openness: Internet security and the limits of open source and peer production* Doctoral Thesis. Delft University, available at: <http://repository.tudelft.nl/view/ir/uuid:ecf237ed-7131-4455-917f-11e55e03df0d/>

formulation of social production, which is aimed at explaining how new collaborative technologies (such as peer produced open sourced software) have given rise to a “networked information economy.” Benkler did not develop any examples specific to information security within his book on the subject.⁵² Using two case studies, the response to the attack on Estonian networks in 2007 and the Conficker botnet response in 2008-2009, Schmidt concludes that the production of security on the Internet represents a unique form characterized by a tension between openness (which typically characterizes peer production) and necessitated secrecy. He labels this a “variant” of peer production and sketches a topology of such networks using the Conficker botnet remediation effort to operationalize various facets. Openness is discussed as having limits when applied within the operational security segment of Internet security production and Schmidt points to various models of trust which that community has tried to evolve.⁵³

Schmidt’s later paper on emerging hierarchies within Internet security networks begins discussion by briefly outlining three “prominent ideal-type systems for international security.” He lists balance-of-power relations, collective security, hegemonic peace, and international regimes all as a way in which war is prevented within an anarchic international system. He then goes on to make the assertion that ‘networked security’ represents a fifth ideal type.⁵⁴ In doing so he is borrowing Gruszczak’s conceptualization of networked security, which was developed as an explanation of the types of loosely coupled information exchanges and governance structures used to address security in failed states such as Afghanistan.⁵⁵ Instead of applying the concept within

⁵² Benkler, Yochai. *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. New Haven, Conn.: Yale University Press, 2006. Print.

⁵³ Schmidt (2013)

⁵⁴ Schmidt in Keremer (2014)

⁵⁵ Schmidt in Kremer (2014) and Gruszczak, A. “Networked security governance: Reflections on the EU’s counterterrorism approach.” *Journal of Global Change Governance*, 1.3 (2008) and

the milieu of counter-insurgency doctrine, Schmidt claims networked security, conceptually, describes the manner in which internet security is provided relying on the same examples he and Mueller cited in the work discussed above along with brief sketches of several more recent examples. Schmidt does not robustly develop the claim that networked security can stand beside the other four systemic ideal-types he cited. Instead he simply states ‘security scholars’ have begun to explore diffuse networked structures as a way in which security is provided. The argument he develops shifts from discussing international security between states, to how collaborative security is provisioned on the Internet. According to him, states are currently asserting and defining what constitutes ‘legitimacy’ when it comes to Internet security and governance. As such he concludes hierarchies are being established over the previously diffuse networked nature of Internet security and by extension governance. Peer production is a useful analytic lens with which to describe the types of activities under consideration within this dissertation. However, peer production is difficult to seat and operationalize within the larger theoretical literature of International Relations and Security, which is another thrust of this dissertation. That difficulty stems, in part, from the fact the remediation activities under examination involve constituencies which extend beyond and outside the information technology means on which peer production relies on, and the activities exist in within a much larger socio-political context and culture. The idea that “security scholars” are now grappling with the issue of networked security archetypes is correct, and as such the practice lens is complementary to Schmidt’s work

2.5.3 Regime Complexes

Regimes are a formalized set of norms and regime complexes are the loose affiliation amongst regimes that lay between formal legal instruments and disparate patchworks of applicable institutions within an issue area. Regime complexes are thereby identified by the existence of

overlap between institutions. Cyber-space has been described as representing a space governed through a myriad overlapping institutions, regimes, and norms. Joseph Nye has described the “Regime Complex for Managing Global Cyber Activities” within which there exists a subset, across a large swath of the totality, which impact upon security. Nye positions his work as a mapping exercise meant to describe the system as a whole, but readily admits a comprehensive direct mapping is not possible given the breadth of total involved entities, formal and informal, is vast.⁵⁶ Regime Complexes have a larger history within IR and security literature, Hofmann, for example, describes the manner in which NATO and EU security institutions have evolved in relation to each other as a regime complex in which developments *within* one can lead to a reordering *within* the other.⁵⁷ She describes this sort of interaction as “chessboard politics” and typologizes among a set of behaviors within such a system. Hofmann states such “chessboard politics” manifest themselves in member state strategies that she calls “‘hostage taking,’ ‘turf battles,’ and ‘muddling through.’”⁵⁸ Using the example of Cyprus and Turkey, Hofmann shows how each country was able to take advantage of their position to shape the relationship between their two respective organizations (the EU and NATO) despite neither being reciprocal members of both organizations, this ‘hostage’ taking relies on overlapping regime connectivity and not on direct control of consequences. The ‘turf-battle’ strategy is used to differentiate, shape and influence mandates of involved organizations to include or exclude various interests. Hofmann cites the view taken by Belgium, Luxembourg, and Spain during the Berlin Plus negotiations that favored calls for an independent and autonomous alternative to NATO instead of a closer

⁵⁶ Nye, Joseph S. "The regime complex for managing global cyber activities." (2014).

⁵⁷ Hofmann, Stephanie C. "Overlapping institutions in the realm of international security: The case of NATO and ESDP." *Perspectives on politics* 7.1 (2009): 45-52.

⁵⁸ Hofmann (2009)

arrangement.⁵⁹ When the two strategies are implemented, it can lead to the situation where a clear division of labor between institutions does not develop and the resulting dynamic is one in which ambiguity reigns and informal alternatives are sought –the act of muddling through as it were. Hofmann’s assessment is useful as it lends several ‘sign posts’ to look for when analyzing systems displaying regime complexity.

Similarly Raymond argues that mitigation and management processes are essential in order to maintain Internet stability and prevent disruptions, finding that these challenges are due, in part, to the large number of rules and the involvement of a wide array of actors.⁶⁰ He argues that decisions made by one actor could have “intended or unintended effects” on other actors. The combination of these effects with the decentralized nature of the regime complex can create coordination and conflict resolution problems.⁶¹ However, Raymond suggests that coordination can occur and offers a solution to these problems through the creation of a prohibition regime able to address threats in the international security realm.

The regime complex literature is typical of IR/security literature in that it has a bias towards state centric conceptions of relationships, despite its discussion of norms and institutions (which while a main focus are always placed relative to the state centric model). Hofmann’s work is of interest as it provides a way to operationalize regime connectivity that can lead to various effects despite a lack of formal direct connection between two entities, but instead possessing a shared third-party vector. Similarly, the seams framework should be seen as a step towards understanding and operationalizing and eventually allowing for typologies of certain types of behaviors across

⁵⁹ Ibid.

⁶⁰ Raymond, M. Managing decentralized cyber governance: The responsibility to troubleshoot. *Strategic Studies Quarterly* 2016; 10:4 (Winter): 124.

⁶¹ Raymond (2016).

various contexts, beyond the major/minor divide identified earlier in this dissertation. Admittedly, the lens of practice is suited to a less abstract and more individual level of analysis than regime complexes.

2.5.4 *Science and Technology Studies*

Another emerging area of literature involves using the lens of Science and Technology Studies (STS) to describe cybersecurity. STS views technology as part of a social, political, and cultural fabric that cannot be separated. The STS lens has been used extensively to understand the connection between technology and politics, this includes security. Most recently, Cavelti uses the STS to focus on cybersecurity as social practice “enacted and stabilized through the circulation of knowledge about vulnerabilities.”⁶² STS includes approaches such as Actor Network Theory (ANT) that treats technological artifacts as objects possessing “general ontological symmetry between human and non-human entities”. In doing so, the entities are analyzed as having relational implications that explain socio-cultural and political emergence and sustainment. Scholars within this school of thought are often interested in how social practices emerge, spread, and become normalized and when such practices break down. That process (of breaking down) is called “depunctualization” and characterized by the interruption of a stable network which reveals how those networks function.⁶³ Cavelti approaches the topic first by discussing the various meanings cybersecurity has with respect to technology and social science. She does this by usage of bibliometric data which quantified cybersecurity publications filtered through the subject heading of “international relations” within several citation databases. Afterward, Stuxnet is discussed as a

⁶² Cavelti, Myriam Dunn. "Cybersecurity Research Meets Science and Technology Studies." *Politics and Governance* 6.2 (2018): 22-30.

⁶³ Cavelti (2018), p27

depunctualization event to show how a technological object (a vulnerability in this case) depicts the network representing cybersecurity practices have political implications. Cavelty concludes that the intersection of technical understandings of cybersecurity and vulnerabilities need to be bridged with the social perspective to understand how “knowledge about vulnerabilities is created, disseminated and transformed into political (and other) effects.”⁶⁴ This dissertation is a step in that direction, the lens of practice helps show how knowledge is created, codified, shared, and leveraged to produce security and create a community of practice. This has implications at various levels of social order, the ICIRS model helps define discreet levels of analysis at which those implications play out. While sharing a focus on practice, this dissertation does not adopt the full ANT worldview linking technology and human actors as social objects with similar features. Instead the lens of practice used here is developed through a separate theoretical tradition and substantiates its descriptive usage by exploring provisioning activities at a less abstract level of analysis than Cavelty

2.6 Agency, Structure, and Power during Security Provisioning

The ICIRS model defined in chapter one introduced the reader to a series of intersecting and interacting dimensions to help define a conceptual space within which security provisioning on/for the Internet can be holistically explored in conjunction with and in regard to the socio-political space. Thus far chapter two has drawn together a subset of IR and social science literature to help understand the provisioning of security within specific subsets of people and institutions as a *social practice* that can be further defined as a *security community of practice* operating across *seams*. This framework will be leveraged in the next chapter to show how a unique problem-

⁶⁴ Dunn Cavelty (2018), p28

solving culture evolved amongst internet security professionals as consequence of early structure, decision making, and evolution of the Internet through important security events. The framework that has been described thus far is uniquely built to understand security as conceived of by social science and operationalized as a set of practices that occurs on and for the Internet. The framework has synthesized multiple levels of analysis defining conceptual layers inherent to how the Internet is engineered while building bridges to traditional international relations levels of theoretical exploration. This framework can help drive analysis of issues related to agency, structure, identity, and power systematically. Coordination, which was defined above, as the act of aligning actors' goals, intentions, and actions can be observed as the evolved practice of security provisioning which has arisen as the Internet has been instantiated and grown. Coordination is most recognizable during the threat recognition phase in which problem- solving is being engaged in and active discussions are occurring. Observing practice can be achieved by analyzing the various indicators of practice emanating from a community of practice. As detailed above, these indicators of practice may include:

- Seeking to identify a problem and looking for a solution
- Explicit acts of seeking out experience through social networks,
- Reusing assets across problem-sets,
- Coordination and synergy through combining efforts amongst actors,
- Active discussions amongst a set of linked practitioners,
- Documentation of process to codify skills and document resources, and
- Mapping knowledge to identify gaps through intentional interrogation of knowledge networks to establish baseline understanding amongst practitioners

Structure of a communities of practice and their interaction with outside elements can be defined, in part, through ease of communication. Communication amongst a constituency will be easier when such it is routinized and habituated through repeated interaction. When the gulf between two coordinating parties is small, it can be categorized as a minor seam and may help enable

coordination. As similarities give way to differences, the chasm across which information must flow may deepen thus comprising a major seam which will impede coordination. Distinguishing between major and minor seams can help one understand the structure and pathway of security provisioning specific to an event or context. Finally, the idea of identity can be observed through the manner in which communities of practice adjudicate participation. Which is to say, how do such communities judge who is part of their constituency and who is outside of it? Various models of trust will be discussed in chapter four and facets of group dynamics impacting identity will also be explored through various cases in chapters three and four.

The next two chapters will utilize the framework to build an understanding how security communities of practice collaborate to recognize and remediate problems occurring at a large-scale on the Internet. Across the cases presented below, the ICIRS model is utilized, implicitly, as an analytic heuristic to help drive insight into the various indications of practice across threat recognition and security provisioning in the face of emergent threats. In each of these cases, there exists a constituency of individuals that can mobilize as a response to those emergent threats based, in part, on their unique position embedded within the structure of the Internet's physical, logical, and governance structure and their ability to utilize professional and social connections. The current system which consists of distributed agency, often described as a patchwork, has evolved from practices emerging through security events over the course of the Internet's history. Chapter three will sketch the trajectory of that history bookended by two canonical cases before the modern provisioning environment is discussed in chapter four. The issue of power will be revisited and discussed in chapter five.

3.1 Morris Worm: Security as a local concern

November 1988 was a watershed time in the development of collaborative information security. At the time, the Internet consisted of approximately 60,000 computers connected throughout the US and overseas. Reports of widespread shut-downs of network connected computers began spreading on or about 2 November. The resulting effort to diagnose and eradicate the problem, which was identified as a “self-replicating, self-propagating,” piece of code authored by Robert Morris Jr., a graduate student at Cornell University, drew together several computer experts throughout academia. The Morris Worm, as it was dubbed, provided the historic impetus to pursue more formalized standing institutions focused on information security. After action reports estimated the worm to have infected between 5 and 10% of Internet connected computers. The estimated eradication costs of the worm were pegged at \$98 million by the GAO.⁶⁵ DARPA, in the wake of the Morris Worm, set up the first Computer Emergency Response Team (CERT), which was established to provide a nexus for coordinating information security response activities and information dissemination. The worm highlighted some of the coordinative weakness associated with the manner network management was executed on the then nascent Internet.

Often cited in contemporaneous analysis of the incident was the observation that there was no “Internet-wide management.”⁶⁶ The 1989 GAO report on the incident documented that “According to a DARPA official, decentralization provided the needed flexibility for the Internet’s continuing growth and evolution.” In practice this meant universities and government agencies

⁶⁵ United States, Congress. “Virus Highlights Need for Improved Internet Management.”, General Accounting Office. 1989 .<https://www.gao.gov/assets/150/147892.pdf>

⁶⁶ GAO (1987)

managed their own network back-bones while no one agency was responsible for overall management.⁶⁷ The Morris worm itself exploited security flaws in the popular UNIX operating system to gain access, copy itself, and then send itself to other computers. GAO analysis of the incident highlighted the following three vulnerabilities made apparent by the incident: 1) the lack of an Internet focal point for addressing security issues, 2) security weaknesses at some sites, and 3) problems in developing distributing and installing software fixes. The analysis also pointed out there were no federal statutes which “makes such conduct a crime, other laws must be applied.”⁶⁸

The relevance of this case to the present work is to demonstrate long lasting and patterned institutional development can result from large-scale security mobilizations due to emergent threats on the Internet. Response activities, in subsequent years, reflect much of the same manner of collaboration as that witnessed during the Morris Worm incident. Therefore, security response on and for the Internet does have a historical context that is necessary to understand, despite the often-raised notions of continual evolution and flux that are discussed when analyzing the space.

One of the more interesting dynamics highlighted by reviewing writing and analysis published subsequent to the remediation efforts relates to how various individuals acted as sensors that first recognized the threat, as agents whom diagnosed the specific set of technical issues it represented, and then helped coordinate and execute a remediation effort. One of those individuals was Eugene H. Spafford who played a central role in helping coordinate amongst academics studying the worm during the initial remediation effort, he later went on to create several articles discussing the event including a detailed timeline sourced from his own correspondence along with

⁶⁷ United States, Congress. “Virus Highlights Need for Improved Internet Management.”, General Accounting Office. 1989 .<https://www.gao.gov/assets/150/147892.pdf>, p2

⁶⁸ GAO (1989)

information gathered from other participants. Reviewing that timeline helps map the flow of information and the manner of collaboration which characterized the Morris Worm incident in a non-trivial manner. After the Worm was initially released, a solution was found within 12 hours, however, the speed of worm propagation and the lack of any formal communication channel among the various local system administrators of Internet connected networks, meant the worm nevertheless spread. In some cases, the fix was not able to be distributed due to email being inaccessible as a result of issues connected to the Morris Worm. Several individuals at places like NASA, Perdue University, MIT and other institutions were the first to notice the issue and exchanged a series of messages regarding the worm. One of the earliest was from Peter Yee at NASA:

“A virus is currently affecting a number of network hosts and may affect yours. It is spread via the electronic mail (SMTP and Sendmail) and attacks machines running 4.3 and 4.2 UNIX BSD and possibly SUN 3.X machines. The following are three messages which provide some background information about the virus and supply a fix. The fix will prevent reinfection by the virus, but it will not fix any damage the virus has done.”⁶⁹

His message went on to offer technical information regarding fixing the issue and appears in Figure 5 below:

⁶⁹ DDN MGT. “DDN MGT Bulletin #43.” Phage. 3 November 1988. Mailing List. <http://securitydigest.org/phage/archive/383>

```

Subject: Fixes for the virus
Index: usr.lib/sendmail/src/srvrsmtp.c 4BSD

Description:
There's a virus running around: the salient facts. A bug in
sendmail has been used to introduce a virus into a lot of
Internet UNIX systems. It has not been observed to damage the
host system, however, it's incredibly virulent, attempting to
introduce itself to every system it can find. It appears to
use rsh, broken passwords, and sendmail to introduce itself
into the target systems. It affects only VAXen and Suns, as
far as we know.

There are three changes that we believe will immunize your
system. They are attached.

Thanks to the Experimental Computing Facility, Center for
Disease Control for their assistance. (It's pretty late,
and they certainly deserved some thanks, somewhere!)

Fix:
First, either recompile or patch sendmail to disallow the 'debug'
option. If you have source, recompile sendmail after first
applying the following patch to the module svrsmtp.c:

*** /tmp/d22039 Thu Nov  3 02:26:20 1988
--- svrsmtp.c Thu Nov  3 01:21:04 1988
*****
*** 85,92 ****
+ "cmex",          CMDONEX,
+ # ifdef DEBUG
+   "showq",      CMDDBGQSHOW,
-   "debug",      CMDDBGDEBEG,
+ # endif DEBUG
+ # ifdef WIZ
+   "kill",       CMDDBGKILL,
+ # endif WIZ
--- 85,94 ----
+ "cmex",          CMDONEX,
+ # ifdef DEBUG
+   "showq",      CMDDBGQSHOW,
+ # endif DEBUG
+ # ifdef notdef
+   "debug",      CMDDBGDEBEG,
+ # endif notdef
+ # ifdef WIZ
+   "kill",       CMDDBGKILL,
+ # endif WIZ

Then, reinstall sendmail, refreeze the configuration file,
using the command "/usr/lib/sendmail -bz", kill any running
sendmail's, using the ps(1) command and the kill(1) command,
and restart your sendmail. To find out how sendmail is
executed on your system, use grep(1) to find the sendmail start
line in either the files /etc/rc or /etc/rc.local

If you don't have source, apply the following patch to your
sendmail binary. SAVE A COPY OF IT FIRST, IN CASE YOU MESS
UP! This is mildly tricky -- note, some versions of strings(1),
which we're going to use to find the offset of the string
"debug" in the binary print out the offsets in octal, not
decimal. Run the following shell line to decide how your
version of strings(1) works:

/bin/echo 'XXXXXXXXabed' | /usr/ucb/strings -o

```

Figure 5 Example of Technical Information Shared on Phage⁷⁰

The Morris Worm, however, necessitated further analysis and remediation action due to the scale at which it was spreading. Recognizing this, Spafford decided to set up a dedicated forum within which a closed set of participants could discuss via a mailing list. This list became known as *Phage*:

“First, I have created (at Steve Bellovin's suggestion) a mailing alias at arthur.cs.purdue.edu named "phage." You are all on it, unless you ask to be removed. I will also add other names if you ask.”⁷¹

⁷⁰ DDN MGT. “DDN MGT Bulletin #43.” Phage. 3 November 1988. Mailing List. <http://securitydigest.org/phage/archive/383>

⁷¹ Spafford, Gene. “A worm ‘condom’ enclosed.” Phage. 3 Novmeber 1988. Mailing List. <http://securitydigest.org/phage/archive/013>

Phage was instantiated to discuss the emerging threat, but it was not the first security-based mailing list. Several others had already existed. These included the UNIX mailing list which was started by in 1984 and the TCP-IP list, named for the network protocols enabling the transition from ARPANET to the nascent Internet. Shortly after Yee's message was sent, an anonymous individual posted the following warning to the TCP-IP list:

“A Possible virus report:

There may be a virus loose on the internet.

Here is the gist of a message Igot [sic]:

I'm sorry.

Here are some steps to prevent further transmission:

- 1) don't run fingerd, or fix it to not overrun its stack when reading arguments.
- 2) recompile sendmail w/o DEBUG defined
- 3) don't run rexecd

Hope this helps, but more, I hope it is a hoax.”⁷²

The message is interesting as it appears to be posted by someone in touch with the virus writer hence the “sorry” reference. It was later revealed the anonymous poster was Andy Sudduth of Harvard University who had been contacted via phone by the worm's author Robert Morris Jr.⁷³ According to the chronology published by Spafford in 2003, the message was unable to be propagated for 24 hours due to network and system overload attributable to the worm.⁷⁴ Despite

⁷² Anonymous. “(none).” *Comp.protocols.tcp-ip*. 3 November 1988. Mailing List. <http://securitydigest.org/tcp-ip/archive/1988/11>

⁷³ Sprafford, Eugene H. "A Failure to Learn from the Past." *Computer Security Applications Conference, 2003. Proceedings. 19th Annual*. IEEE, 2003.

⁷⁴ Sprafford, 2003

the multiple individuals exchanging messages, it was Sprafford's Phage list that became the most central discussion forum. He writes:

"I read Keith's mail, I forward his warning to the Usenet news.announce.important newsgroup to the nntp-managers mailing list, and to over 30 other site admins. This is the first notice most of these people get about the Worm. This group exchanges mail all day about progress and behavior of the Worm, and eventually becomes the *phage* mailing list based at Perdue."⁷⁵

Around 11:30am, the Defense Communications Agency "inhibits the mailbridges between ARPA and Milnet," which would be one of the first indications federal authorities were getting involved actively, though it appears the government was first informed of the issue earlier that day when an academic called the National Computer Security Center. The NCSC was the successor to the Department of Defense Computer Security Center (DoDCSC) which was itself established in 1981. While the NCSC was focused on computer security, it did not become the central coordinating entity during the Morris Worm incident. Instead, the post-mortem workshop conducted by the NCSC and attended by central figures in the remediation effort, concluded that the reason the Worm was "...stopped so quickly was due almost solely to the UNIX 'old-boy' network, and not due to any formal mechanism in place at the time."⁷⁶ That 'old-boy' network communicated using mailing lists like Phage and the UNIX security list in addition to phone calls and individual messages to spread awareness and problem-solve. In reviewing archived messages, certain aspects of practice, discussed in the previous chapter, become apparent through the unfolding discourse amongst participants.

⁷⁵ Spafford (2003)

⁷⁶ Spafford, Eugene H. "Crisis and aftermath." *Communications of the ACM* 32.6 (1989): 678-687.

3.1.1 *Debates*

Some of the indications of practice involve the way in which communities of practice reconcile legitimacy of authority and participation along with legitimacy of action and definition of problem, threat and other common operational level details (perhaps better stated as the “common operational picture” to borrow a term from military circles). Such discussions are apparent when reviewing archived messages across the Phage, TCP-IP, and UNIX mailing lists.

Early discussions on Phage included distributing general awareness of the worm and clarified basic terminology. This included whether the term “worm” or “virus” should be used to describe the issue, and extended to the list’s name, “phage” as accurately describing the list’s function. Those debates were meaningful as they helped define How to communicate the problem to an ever-enlarging circle of awareness, becoming less and less technical as awareness spread to the media and general public. According to Spafford and others “Clarifying the terminology was an important aspect of later technical reports”⁷⁷ and doing so was an impetus for after action reports and meetings. While Phage emerged as one of the central places to exchange information, members of the larger UNIX security community debated if that should be the case. Individuals posted messages expressing that the UNIX Security List, while recently dormant, should be revived and was a more appropriate vector for collaboration, and other individuals believed the TCP-IP list was more appropriate. Early messages of the worm were posted on the TCP-IP list and the debates as to the legitimacy of any these places as the central collaborative space continued throughout the remediation effort. In addition, users debated the line between transparency and

⁷⁷ Phage List. “Security Digest Archives. 1 March 2005. <http://securitydigest.org/phage/>

necessity of confidentiality. One Mike Crawford posted to the Phage list that “unneighbourly” sites were hoarding information. Another list participant wrote:

“One thing about this list: it was assembled hastily for an emergency purpose. Great thanks to Gene Spafford for creating it! As an emergency list, however, it has a large number of bad addresses on it (or shutdown mailers :-). At some point, we should retire this list, and re-create the security mailing list. While people may agree or disagree about whether the security list should be “secure” (and please let’s not rehash all of this again here), we should remember that this list is not secure. Not that this was a problem, since the more information that could be distributed on the virus, the better. But some people may disagree about whether this is appropriate for general security discussions.”⁷⁸

That participant, Theodore Ts’o was concerned that “...if anyone discovers any other holes, they could reuse parts of the virus to build a new one” arguing that posting technical details of the worm’s inner workings could be dangerous. These discussions extended past the immediate remediation efforts and later in the waning days of the Phage List’s active life, participants engaged in further debate as to whom should be privy to the discussions. Spafford asked the larger community if he should add a New York Times reporter, John Markoff to the list:

“I told him that would be up to all of you. He promised that he would not print anything obtained from the list without prior approval of the author(s) involved. I indicated that I would not add him to the list if there was significant negative reaction from any of the current members of the list.”⁷⁹

⁷⁸ Phage List. “Security Digest Archives. 1 March 2005. <http://securitydigest.org/phage/>

⁷⁹ Spafford, Gene. “Addition to the list.” Phage. 8 November 1988. Mailing List. <http://securitydigest.org/phage/archive/169>

The consensus was that the reporter should not be added, and other security concerns related how the various security related mailing lists, not just Phage, should be managed continued. In fact, specific differences within the community, between security through transparency and security through confidentiality led to defection away from the UNIX Security –List and the establishment of a new list named Zardoz. One of the first posts by that list’s administrator, Lyle McElhaney, sketched several debates which presaged larger issues that the information security community and industry are still trying to reconcile thirty years later! Quoting one Doug Gwen, he writes “I am in favor of broadcasting information about UNIX problems, security or otherwise, as WIDELY as possible. Yank your dial-ins if you want security.”⁸⁰ McElhaney goes on to state that while he agrees with that sentiment, some security is necessary. He then writes the following:

“Assuming we have to have some security then, first: who gets the list? In my original message, I referred to root users only. Several people have pointed out that there are others who need the data; bonafide consultants, people doing security development work, and so on. Then there's the other side: with micros abounding on the net, anyone can be a root. Many people with their own machines also have access to large machines, whose owners might not appreciate them knowing how to mangle their system.”⁸¹

These issues, whom to trust and how to judge and extend trust are issues that modern information security communities of practice still wrestle with in the modern era and will be discussed in chapter four.

⁸⁰ McElhaney, Lyle. “Security Mail List, #1.” Unix Security Mailing List. 18 December 1984. Mailing List. <http://securitydigest.org/unix/archive/001>

⁸¹ McElhaney, 1984

3.1.2 Knowledge preservation, communication and distribution

One important dynamic to note was the apparent organic emergence of individuals that consolidated and summarized information that they then posted to the list as a means of knowledge preservation, sharing for awareness and action. The early messages discussed above shared technical information regarding the worm and proposed fixes. Individuals emerged as connected nodes providing a means of coordination. These posts are not excerpted here, however, when reviewed and coded for content with regards to indications of practice, the messages help paint a comprehensive picture of an existing security community of practice, referenced above as a UNIX “old boy’s” club reconciling with the implications of a new threat/issue while also evolving in response to that issue to remediate and problem-solve. For example, multiple posts summarized information as the event unfolded, questions were posted and answered to help identify best practices and solutions, and further debates were had over the crowded palimpsest of issues and implications flowing from the Morris Worm’s release and effects.⁸² The community itself recognized the importance of preserving knowledge and carrying forward lessons learned from the experienced (though the effectiveness of those lessons learned measures continue to be questioned years after⁸³). One way this happened was through the academic process. Sprafford, Yee, Ts’o

⁸² See archived messages: Mamakos, Louis A. “initial portion of virus and how to catch the rest.” Phage. 4 November 1998. Mailing List. <http://securitydigest.org/phage/archive/029>; LoVerso, John Robert. “source of the worm.” Phage. 4 November 1998. Mailing List. <http://securitydigest.org/phage/archive/030>; Shaver, Dave. “Re: Sendmail hacking.” Phage. 4 November 1988. Mailing List. <http://securitydigest.org/phage/archive/031>; Johnson, Eric S. “Re: initial portion of virus and how to catch the rest.” Phage. 4 November 1998. Mailing List. <http://securitydigest.org/phage/archive/033>; Rosenblum, Gary J. “What is everyone doing?” phage. 4 November 1988. Mailing List. <http://securitydigest.org/phage/archive/034>; Rowan, Miek. “Re. What is everyone doing?” Message to phage. 4 November 1988. Mailing List. <http://securitydigest.org/phage/archive/032>

⁸³ Spafford, Eugene H. "A Failure to Learn from the Past." *Computer Security Applications Conference, 2003. Proceedings. 19th Annual.* IEEE, 2003.

and others who were central players in the remediation effort all went on to publish both academic and trade articles detailing all aspects of the Morris Worm, from technical analysis of its inner workings to chronologies and discussions of the effort to organize a response. The Phage list helped coordinate those initial efforts as well, Spafford posted the following message:

“Would each of you take a few moments to jot down the history of when the bug hit you, when you got news of patches to keep it out, when you eliminated all copies of the worm, times & names of other significant discoveries/discoverers, etc? Before this all slips from our minds, I'd like to coordinate a global history of how this thing hit and how we beat it. If you lost and files, tell me that too. Figures on numbers of infected machines, highest single load, etc will all be much appreciated. Once I collate it all, I will circulate the master history back to everyone who contributes information for it.”⁸⁴

Additionally NCSC/DARPA sponsored a workshop aimed at discussing and documenting the response effort while also trying to plan a path forward. Individuals on the various mailing lists such as Phage, Zardoz, and others distributed word of the meeting and several key players attended. The central outcome of that meeting was the establishment of a Computer Emergency Response Team or CERT that would be funded through DARPA and implemented at Carnegie Mellon University. The CERT was meant to serve as a central response point for future network based security issues the existing mailing lists were used to inform the community of the new entity.⁸⁵ By late 1988 Phage's usefulness was winding down, members of the core group involved in the Morris Worm activities looked to consolidate continued security collaboration on other, more general lists, for example Spafford posted the following to the group:

⁸⁴ <http://securitydigest.org/phage/archive/222>

⁸⁵SEI “History of Innovation at the SEI”. Software Engineering Institute. https://www.sei.cmu.edu/about/history-of-innovation-at-the-sei/display.cfm?customel_datapageid_40842=41019 and Brand, Russell. “CERT” Message to phage. 12 February 1988. Mailing List. <http://securitydigest.org/phage/archive/320>

“Andrew Burt has started to mail things out to his list, and the security list at zardoz seems to be alive and well. Specific security holes and fixes should be addressed to those lists in the future. If you aren't subscribed to those lists, you should consider doing so (could the moderators of those two lists post something to this list on how people can join?.”⁸⁶

The Morris Worm served, not only as a galvanizing moment in which network information security became an important point of discussion, but also served to clearly show elements of a nascent Internet security community of practice and thus discernible culture. That nascent community of practice included elements easily bucketed across the layers within the ICIRS model and seams are identifiable.

Clearly, in terms of the Morris Worm, fundamental security issues of integrity and availability during the processing and transmission phases of the information cycle were compromised. Post-event, the Morris Worm undermined assumptions of data integrity and fueled questions of repudiation about an evolving system of communication that was emerging as an important and relied upon technology. Both major and minor seams are clearly present across the threat recognition and the remediation phases of the event. Both recognizing that there was a threat and the subsequent response relied upon traversing minor seams through leveraging messages amongst small groups of socially connected individuals. Major seams between network administrators and larger government entities constrained the effectiveness of the efforts initially due to an immature and, in large part, non-existing national response mechanism. The next section will help fill in the timeline between the Morris Worm in 1989 and Conficker Botnet in 2008. This

⁸⁶ Spafford, Gene. “This Group.” Message to phage. 26 November 1998. Mailing List. <http://securitydigest.org/phage/archive/301>

discussion isn't a comprehensive history, though it will highlight major threats within the realm of malware as they evolved in the intervening time period.

3.2 Seams Multiply: Explosive Growth, Professionalization, and Evolving Threat

If there is one characteristic that describes the Internet longitudinally through time from the 1988 Morris Worm incident to the present, that characteristic is obviously, and easily *growth*. Growth in the breadth of connected networks, in users, in commerce, and in activity has been the most obvious descriptive term associated with the Internet. As that growth has happened and the Internet has become ever more central to the infrastructure of human endeavor, so too has threat grown and *security* of that infrastructure has become a task given to professionalization and ever more specialization. In using the ICIRS model to guide and segment the history of that security evolution, it becomes apparent that the very structure of the Internet is intrinsically linked to the way in which that professionalization and specialization has bred and operationalized the practice of security. From the perspective of governance of core Internet infrastructure, the history of that growth and its implications has been well documented and analyzed by authors such as Mueller and DeNardis.⁸⁷ As such, the history of the Internet's core governance features need not be retread here. However, the core institutional arrangements and histories associated with entities such the Internet Corporation of Assigned Names and Numbers (ICANN), the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C), and others are all important to note. In terms of the ICIRS model, the non-profit, trans-national, governance mechanisms do interact with the information centered security model as it is projected upward through the levels of analysis.

⁸⁷ For developments through 2014 See both Mueller, Milton L. *Ruling the Root: Internet governance and the taming of cyberspace*. MIT press, 2002. and DeNardis, Laura. *The Global War for Internet Governance*. Yale University Press, 2014.

They also overlap, in terms of membership and social circles involved with the community of practice defined below in various case studies. Instead, the focus of the next section is to help sketch the *operational* level of *practitioners* that link the more abstract governance institutions to the *practice* of security and *continued operation* on the ground. That patchwork response mechanism has been less explicitly mapped nor well operationalized in social science and policy literature, though parts and pieces have been referenced, albeit lightly. The evolution of what this dissertation references as a “community of practice” has been co-constituted over the course of the Internet’s growth, and the following section will sketch some development through brief targeted discussion of select cases.

Post Morris Worm there was a recognized need, within the United States, to amend the Computer Fraud and Abuse Act of 1984 to clarify specific language and meanings that became central to the prosecution of Robert Morris Jr. during the legal proceedings of the incident, though he was successfully prosecuted under the original law. The act was amended in 1996. Between 1996 and 2000, the Internet exploded across a number of metrics including users, traffic volume, and geographic access coverage. New electronic information centric terms entered into the world’s written/spoken vernacular. These terms such as “cyber,” “information superhighway,” “net,” and many others ushered in a new era of discussion, culture, economic activity, and unavoidably, security concern. Before describing the modern provisioning environment and the complexity of the modern Internet, a few post Morris Worm incidents will be briefly explored to help fill in the timeline between 1989 and 2008.

3.2.1 1992 – *Michelangelo Virus*

After the Morris Worm the threat to information on and through the Internet increased both in terms of potency of threat and in terms of attention paid. The 1990s saw a succession of worms

and viruses that captured public attention and further evolved the communities of practice surrounding threat recognition, remediation, and related activities.

In 1992 international news media fixated on possible damage that could be done by a newly discovered threat dubbed the Michelangelo Virus due to it being programmed to execute on “any March 6” which is the birthday of the Renaissance artist, though there was no reference to the artist within the virus itself. The newly formed CERT issued the following statement in the alert it sent out

“The Michelangelo virus triggers on any March 6. On that date, the virus overwrites critical system data, including boot and file allocation table (FAT) records, on the boot disk (floppy or hard), rendering the disk unusable. Recovering user data from a disk damaged by the Michelangelo virus will be very difficult.”⁸⁸

The virus is less notable for the actual damage it caused and better known for the hysteria, which ensued that consequently drove sales of anti-virus software and further established the computer virus in the public imagination. An IBM report notes, “...people did find the Michelangelo virus, but they found far more viruses of other kinds. The Stoned virus, for instance, the most prevalent virus at the time, was found about three times more frequently than was the Michelangelo virus.”⁸⁹ The virus helped further establish a security industry that marketed to the public’s fear of possible damage done via computer virus and worms, which may have contributed to a general lack of concern before the Melissa Virus hit in 1999. That virus will be highlighted next.

⁸⁸ SEI “1992 CERT Advisories” SEI Carnegie Mellon University. 1992.
https://resources.sei.cmu.edu/asset_files/WhitePaper/1992_019_001_496266.pdf

⁸⁹ IBM “Michelangelo Madness” IBM Research Report. 1992.
<https://web.archive.org/web/20080309235614/http://www.research.ibm.com/antivirus/SciPapers/White/VB95/vb95.distrib-node7.html>

3.2.2 1999 – Melissa Virus

Often cited in the history of computer viruses and worms is the Melissa Virus. The 1999 CERT alert sent out to warn the public stated the following:

At approximately 2:00 PM GMT-5 on Friday March 26, 1999 we began receiving reports of a Microsoft Word 97 and Word 2000 macro virus which is propagating via email attachments. The number and variety of reports we have received indicate that this is a widespread attack affecting a variety of sites.

One of the characteristics that made the Melissa Virus such a notable threat is the rapidity with which it spread. Testifying before the Subcommittee on Technology in the House of Representatives, Keith A. Rhodes said:

“Melissa showed just how quickly viruses can proliferate due to the intricate and extensive connectivity of today’s networks in just days after the virus was unleashed, there were widespread reports of infections across the country. Worse yet, as the virus made its way through the Internet, variations appeared that were able to bypass security software designed to detect Melissa. These two factors alone made it extremely difficult to launch countermeasures for the infection.”⁹⁰

Mr. Rhodes testimony also offers a small bit of information pointing back toward the importance of private elements of the burgeoning private security community of practice. He testified “Melissa showed how hard it is to trace any virus back to its source.” Authorities had believed that an individual with the online handle “VicodinES” distributed the virus via an America Online (AOL) account, however with a tip originating from the same service, investigators discovered

⁹⁰ United States, Congress, Rhodes, Keith A. “Information Security: the Melissa Computer Virus Demonstrates Urgent Need for Stronger Protection over Systems and Sensitive Data.” *Information Security: the Melissa Computer Virus Demonstrates Urgent Need for Stronger Protection over Systems and Sensitive Data*, General Accounting Office, 1999.

that this account was allegedly stolen by the suspect arrested for creating the virus. Without this level of cooperation, the suspect might not have ever been identified. Even before the account was revealed to be stolen, the initial investigation into the author of the virus was helped along substantially by private constituencies. A 1999 article in the New York Times details that one Richard Smith, the president of Phar Lap Software, helped track the virus origins:

“Mr. Smith found indications that the virus is a work of a programmer -- or possibly a small group -- who wrote and distributed a similar program two years ago. Moreover, by searching the World Wide Web, he has found clues to the identity of the programmers and even more striking evidence that could lead the authorities to the computer on which the program was written.

Today Mr. Smith turned that information over to the Federal Bureau of Investigation. Paul Bresson, an F.B.I. spokesman, would say only, "We have a case that's open and we're actively investigating the virus." Distributing a computer virus is a Federal crime.”⁹¹

Like the Morris worm before, threat recognition and remediation were again coordinated, in part, via online mailing lists. The Times reported that Mr. Smith “...collected that information and posted it to an internet news group that discusses software viruses. Later that evening he received a response from a Swedish computer science graduate student...” That student was Fred Björck and he recognized similarities between what Mr. Smith posted and a virus author known to him.⁹² Mr. Björck suggested to Mr. Smith that metadata associated with MS Word documents could be used to help determine where the virus originated and could be used for attribution. While VicodinES was identified, the virus was released via AOL to the alt.sex newsgroup by David Smith

⁹¹ Markoff, John. “Digital Fingerprints Leave Clues to Creator of Internet Virus.” *The New York Times*, 30 Mar. 1999, p. A00017, www.nytimes.com/1999/03/30/us/digital-fingerprints-leave-clues-to-creator-of-internet-virus.html.

⁹² Ibid.

(no relation to the earlier Richard Smith). The confusion over the identity of VicodinES and whether or not David Smith was one and the same or, as it turned out, a separate individual pointed to the immaturity of law enforcement's ability to execute technical investigations. It also reinforced the role technical communities of practice continued to play in the evolving threat environment a decade post Morris Worm. This provides further evidence of the major seam between public law enforcement and private technical communities of practice that had existed during Morris Worm, and continues to the persist today. In the Melissa case, the collaboration between Mr. Björck, a grad student in Sweden, and Richard Smith who was a private business owner in the US, led to the FBI being able to track down and prosecute a guilty party. According to the FBI, the virus had caused more than \$80 million in damage.⁹³ The virus' originator was sentenced to 20 months in jail and prevented from participating on online forums and using a computer network for a period of time without the court's permission. Mr. Smith wasn't sentenced until 2002 and in the intervening period after his arrest he provided extensive help to the FBI. He posed online under a false name and communicated with other virus authors and was instrumental in helping authorities with other cases (including the 2001 Anna Kournikova Virus mentioned below).⁹⁴ The 2002 FBI press release noted both AOL for its assistance and ICSA.net of Reston, VA for technical assistance "...which included an analysis of damage caused by the Melissa virus."⁹⁵ ICSA.net was one several private companies coordinating with members of the security

⁹³ "Creator of Melissa Virus Gets 20 Months in Jail." *The New York Times*, The New York Times, 2 May 2002, www.nytimes.com/2002/05/02/nyregion/creator-of-melissa-virus-gets-20-months-in-jail.html.

⁹⁴ <https://www.welivesecurity.com/2016/07/15/flashback-friday-melissa-virus/>

⁹⁵ "Creator of Melissa Computer Virus Sentenced to 20 Months in Federal Prison." *FBI Press Releases*, The United States Department of Justice, 1 May 2002, www.justice.gov/archive/criminal/cybercrime/press-releases/2002/melissaSent.htm.

community via discussion groups and providing assistance to the authorities.⁹⁶ ICSA.net is worth discussing further as an example of the continued professionalization and specialization of information security.

ICSA was founded in 1989 by David Kennedy, the company became an early purveyor of security related software and services. Reporting from the time during and after the Melissa virus helps discern some of the early indicators of developing practice and establishment of a burgeoning community of practice. The Wall Street Journal reported: “Viewing its mission as counterintelligence in a game of guerrilla warfare, the company is unusually aggressive among antivirus researchers.”⁹⁷ It goes on to say, “The IS-Recon agents [a reference to ICSA employees] can hide their identities while communicating with virus writers over the Internet. They keep tabs on messages on Internet news groups such as alt.comp.virus...” ICSA.net is an example of individuals within a company developing technical knowledge and relationships across industry and constituencies in the same manner that network engineers (at places like CloudFlare) will be detailed below the case of BGP routing. The same article describes ICSA.net in the following manner:

“The team is an eclectic mix. Spread throughout the U.S. and connected via computer, the team includes the police-trained Mr. Kennedy as well as other experts in information gathering, including a former journalist. There's an academically oriented computer expert, a so-called virus "zoo-keeper" who has samples of 31,000 viruses, and a couple of recent college graduates young enough to look and act the part of virus writers. The agents work on computers that can't be traced to

⁹⁶ Cluley, Graham. “Memories of the Melissa Virus.” *Naked Security*, Sophos, 10 Nov. 2013, nakedsecurity.sophos.com/2009/03/26/memories-melissa-virus/

⁹⁷ Takahashi, Dean. “Hackers and Virtual Perps: Beware of ICSA.net Sleuths.” *The Wall Street Journal*, Dow Jones & Company, 30 Sept. 1999, www.wsj.com/articles/SB938637421701976364.

the company, and the zookeeper, Bruce Hughes, uses software programs dubbed "bots" to scour the Internet for activity at sites operated by virus writers."⁹⁸

ICSA.net went on to become a central player in the emerging specialized information security products and services industry. The company was eventually merged with another before being bought by Verizon, the company currently still exists as an independent division of Verizon under the name ICSA Labs. The arch of its history, given that it was founded in 1989 mirrors the expansion, professionalization and subsequent specialization that has characterized the information security space. As the Internet grew explosively, individuals within the security field developed ever more specialized knowledge, skills, and seams across which such professionals coordinate have multiplied and grown. Before discussing the modern provisioning space in chapter four, several more notable security events will be discussed.

3.2.2 2000 – *ILOVEYOU* Worm

On 4 May 2000, yet another newly released threat laid claim to the title “fastest spreading” and “most damaged caused”.⁹⁹ Like the viruses and worms explored above, this one too spread through email, and also by making use of an attachment which held a Visual Basic script. The worm itself was not sophisticated in terms of code, but it did play on the social proclivities of people in order to propagate. The subject line contained the words “I Love You” and the email body implored individuals to open the attachment. The worm then emailed itself to all the

⁹⁸ Takahashi (1999)

⁹⁹ Weinberger, Sharon. “Top Ten Most-Destructive Computer Viruses.” *Smithsonian.com*. 19 March 2012. <https://www.smithsonianmag.com/science-nature/top-ten-most-destructive-computer-viruses-159542266/?c=y&page=2>

addresses within a user's address book using the Microsoft Outlook program.¹⁰⁰ It should be noted that the academic and technical community during and following the ILOVEYOU worm incident seemed to be at odds at how to classify the threat, some wanted to use the term virus others the term worm. This represents an ongoing indication of practice as the community surrounding computer security worked to develop a vernacular of common definition. Eugene Spafford, known from the Morris Worm incident and by then a popular academic authority on computer security, made the following distinction during Congressional testimony:

“Unlike viruses, worms are programs that can run independently and travel from machine to machine across network connections; worms may have portions of themselves running on many different machines. Worms do not necessarily change other programs, although they may carry other code that does, such as a true virus. It is this replication behavior that leads some people to believe that worms are a form of virus, especially those people using Cohen's formal definition of virus (which also would classify automated network patch programs as viruses).¹⁰¹

The testimony hints at the one of the larger seams across which threat recognition and remediation must occur and overcome during this time period, largely due to the increasing scale of damage. That seam is between the general public and the technical community. Issues of *how* to communicate threat and discussing collective language to do so highlights an indication of practice, namely evidence of specialized language and communication firmly establishing within the burgeoning community. The ILOVEYOU worm is useful to highlight for another reason which is the international coordinative impediments and prosecutorial failures associated with the case. Despite the coordinative mechanisms put in place since the Morris Worm incident and the

¹⁰⁰ Symantec. “VGS.LoveLetter.Var.” Symantec. <https://www.symantec.com/security-center/writeup/2000-121815-2258-99>

¹⁰¹ Spafford, Eugene. Testimony to the House Armed Services Committee. 24 July 2003. <https://spaf.cerias.purdue.edu/usgov/hasc.pdf>

maturing security awareness amongst governments, corporations, and the public, the ILOVEYOU worm still caught the Internet, as a whole, unaware and unprepared. Take for instance testimony given before the Subcommittee on Financial Institutions, Committee on Banking, Housing and Urban Affairs by Jack Brock the director for Government wide and Defense Information Systems:

However, the NIPC had less success with the ILOVEYOU virus. As noted earlier (in figure 1), the NIPC first learned of the virus at 5:45 a.m. EDT from an industry source. Over the next 2 hours, the “NIPC checked other sources in attempts to verify the initial information with limited success. According to NIPC officials, no information had been produced by intelligence, Defense, and law enforcement sources, and only one reference was located in open sources, such as Internet websites. The NIPC considers assessment of virus reports to be an important step before issuing an alert because most viruses turn out to be relatively harmless or are detected and defeated by existing antivirus software. According to the NIPC, the commercial antivirus community identifies about 20 to 30 new viruses every day, and more than 53,000 named viruses have been identified to date. At 7:40 a.m., two DOD sources notified the NIPC that the virus was spreading through the department’s computer systems, and the NIPC immediately notified the Federal Computer Incident Response Center (FedCIRC), at GSA, and CERT-CC. FedCIRC then undertook a rigorous effort to notify agency officials via fax and phone.”¹⁰²

This points back towards the necessity of commercial, private, and academic constituencies to recognize and characterize the emerging threats before government law enforcement and other public resources could mobilize. The authors of the ILOVEYOU worm were identified as a Philippine nationals Onel de Guzman and Reonel Ramones. The two were identified as part of a group of “hackers” known as GRAMMERSoft, providing services to small businesses and allegedly selling homework to other students at AMA Computer College in the Philippines. US

¹⁰² United States, Congress, Brock, Jack L. “Critical Infrastructure Protection: ‘ILOVEYOU’ Computer Virus Highlights Need for Improved Alert and Coordination Capabilities: Statement of Jack L. Brock, Jr., Director, Government wide and Defense Information Systems, Accounting and Information Management Division, before the Subcommittee on Financial Institutions, Committee on Banking, Housing and Urban Affairs, U.S. Senate” , GAO, 2000. www.gao.gov/new.items/ai00181t.pdf

and European authorities both desired to try the perpetrators in Western courts as much of the damage (much of it manifested as loss of productivity) had occurred in Western governments and corporations. However, the Philippines lacked the necessary laws to charge them. Thereby nobody was prosecuted for the incident.¹⁰³ The incident led directly to the Philippines updating their information technology and security laws to address computer crime, much in the same way the Morris Worm incident forced change in the US. The incident highlighted much of the same sort of ad-hoc coordination present during previous events, just at a much larger scale and within multiple communities of practice. Recalling the event for the BBC one information security specialist was quoted saying “When I hung up my phone and looked at the screen, it showed that I had received and missed 40+ phone calls during that 30-minute conference call,” he was further quoted, “All those calls were coming in from partners, vendors and media...Everybody wanted to know what was happening and how to fight the outbreak”¹⁰⁴ One of the things that ILOVEYOU presaged was the oncoming torrent of malicious email spam which would characterize a new era of computer crime.

3.2.3 2003 – SQL Slammer

In 2003 the SQL Slammer worm infected more than ninety per cent of vulnerable hosts (computers connected to the Internet and susceptible to the threat) within ten minutes of being released. While again unprecedented in the speed and scale compared to what came before, Slammer was particularly alarming in that it spread faster than human scale response times could manage, causing significant damage to financial organizations, travel systems, and

¹⁰³ Cluley, Graham. “Memories of the Love Bug Worm.” *Naked Security*, Sophos, 4 May 2012, nakedsecurity.sophos.com/2009/05/04/memories-love-bug-worm/.

¹⁰⁴ Ward, Mark. “A Decade on from the ILOVEYOU Bug.” *BBC News*, BBC, 4 May 2010, www.bbc.com/news/10095957.

governments.¹⁰⁵ Even more interesting, SQL Slammer was modeled after a proof of concept academic exercise in which the original author disclosed the vulnerability to Microsoft whose software the Slammer virus exploited. David Litchfield was responsible for finding the original exploit and he writes: “Coding an exploit up I sent a copy of it to the Microsoft Security Response Center (secure@microsoft.com) with a short write up of my findings then proceeded to own all of our client’s SQL Servers.”¹⁰⁶ Afterward, Litchfield contacted Microsoft to ask if he could present the newly found vulnerability at the yearly Blackhat security conference, Microsoft assented noting that there would be an available patch by that time. While presenting at the conference Litchfield implored his audience to install the patch. Six months later an unknown entity used the code Litchfield presented in the Slammer virus which crashed Microsoft’s SQL server product while also generating a random IP address to which the virus would propagate further.¹⁰⁷ The resulting quick propagating virus clogged networks causing failures of airline, banking, and even emergency services infrastructure around the world. An analysis of Slammer noted that it had infected more than 75,000 hosts within a few minutes of its release despite the fact that it was a known vulnerability that had been demonstrated and Microsoft had released a patch beforehand.¹⁰⁸ Slammer is useful in that it demonstrates the manner in which the security community of practice is intrinsically related to the threat-scape. Members of the security community, such as David Litchfield, work to find exploits and publicize them through interactions and knowledge sharing such as presenting at Blackhat. However, that very same vector serves to inform the adversaries

¹⁰⁵ Moore, David, et al. "Inside the slammer worm." *IEEE Security & Privacy* 99.4 (2003): 33-39

¹⁰⁶ Litchfield, David. “The Inside Story of SQL Slammer.” *Threatpost*, 20 Oct. 2010, 14:30, threatpost.com/inside-story-sql-slammer-102010/74589/.

¹⁰⁷ *Ibid.*

¹⁰⁸ Moore, David, et al. "Inside the slammer worm." *IEEE Security & Privacy* 99.4 (2003): 33-39.

as well. That dynamic will be further discussed later in this dissertation. Slammer's code was rather unsophisticated, though Litchfield notes that virus' author did not make the code as efficient and short as possible and further notes differences across the code in utilizing the exclusive or (XOR) function may indicate that the virus had at least two separate authors. This act of deconstructing code for the sake of attribution (even though, in this case, nothing came of it) shows another central responsibility of the third-party technical contributors across the Internet security community of practice.

3.2.4 2004 – MyDoom, SoBig, Sasser and the Monetization

2004 represented a new era in Internet security and ushered in the realization that previous computer worms and viruses spread through the Internet had been rather quaint next to what was on the horizon. What was the change signaling the new era? Money. The MyDoom and SoBig pieces of malware did not represent the sorts of viruses and worms that had come before, these new threats were purpose built and represented the introduction of an organized criminal element focused on making money through surreptitious control of infected computers. Controlling networks of infected computers meant those captured resources could be directed, in a for-hire fashion, to send out email spam or create on demand distributed denial of service (DDOS) attacks. Their arrival heralded the end to an era in which computer worms and viruses were written and released as demonstrations of skill or for thrill, and instead indicated that malware would become a commodity through which crime could be conducted and criminals could earn money. MyDoom, in particular, spread faster than SQL Slammer but while Slammer simply propagated, MyDoom turned infected computers into zombies and targeted specific websites, initially that of SCO corporation. When looking back, a number of experts interviewed by this author cited both

MyDoom and SoBig as the events marking virus writing as a commercial enterprise.¹⁰⁹ MyDoom originated in Russia and the original variant of the worm was intended to launch a denial of service attack against the SCO Corporation, possibly as retaliation of the company's copyright claims against parts of the Linux operating system's open-source code-base.¹¹⁰ SCO offered a \$250,000 reward for information leading to prosecution of the worm's authors, and Microsoft later also offered reward money. While the rewards did not lead to an arrest, the technique was successful for Microsoft in other cases in 2004. Microsoft's \$250,000 bounty that it offered with regard to the Sasser Worm, another piece of malware emerging in 2004, led to the arrest of Sven Jaschan, a German minor who was turned in by two friends motivated by the pay-out. The Sasser incident also provides a brief insight into the way international law enforcement collaboration for cyber investigations was evolving. The FBI posted the following on their website in October 2005 describing the investigation into Sasser after Mr. Jaschnan had been identified through his friends: "The student had erased vital evidence on his computer. How to link him to the crime?"¹¹¹ The FBI went on to state "The cyber saboteur admitted sending the malicious code to an acquaintance through a U.S.-based instant messaging service. German authorities called us...and we contacted the messaging service, enabling us to trace the transmission to a specific IP address. Then, German investigators used the information to make the direct link to the student."¹¹²

¹⁰⁹ Author interviews, also see news and industry articles such as: Roberts, Paul F. "MyDoom One Year Later: More Zombies, More Spam." *InfoWorld*, InfoWorld, 26 Jan. 2005, www.infoworld.com/article/2669026/security/mydoom-one-year-later--more-zombies--more-spam.html.

¹¹⁰ Peline, Jeff. "MyDoom Downs SCO Site." *CNET*, CNET, 2 Feb. 2004, www.cnet.com/news/mydoom-downs-sco-site/?i10c.ua=1&i10c.encReferrer=aHR0cHM6Ly93d3cuZ29vZ2xILmNvbS8&i10c.dv=7.

¹¹¹ FBI "Catching a Cyber Saboteur.", FBI, 19 Sept. 2005, archives.fbi.gov/archives/news/stories/2005/september/global_partner091905.

¹¹² FBI, 2005

Over the course of the ensuing months 2004 - 2006, MyDoom variants began to show up, each of which added new IP addresses to target various other entities proving its utility as a “directed” DDOS “weapon.” Similarly, SoBig also created networks of infected computers that could be directed, these networks are known as “botnets” and have become a focused concern amongst security professionals ever since (botnets are discussed in much further detail later within this work). The control of both MyDoom and SoBig were fought over by various criminal elements vying for command and control of the networks through the release of variants, ostensibly to sell for denial of service attacks and to send out email spam.

3.2.5 2008 – Conficker

The Conficker Botnet represents one of the most studied modern coordinated incident response cases within the information security space. The case has been studied from technical and social science academic perspectives, been reported about extensively in popular news media, and there exists an account of the effort in popular mass marketed book form. Thereby its usage here is to leverage those established narratives to understand the event from the perspective of social practice. In fact, the availability of these various accounts is a valuable indication of practice, central figures within the remediation effort interviewed for this dissertation made clear that circulating information about Conficker and participating in efforts to spread the story were *intentional* on their part so as to institutionalize knowledge and codify normative response mechanisms.¹¹³ The book is named *Worm: The First Digital World War* and was written by

¹¹³ Author interview

Mark Bowden.¹¹⁴ The book names a number of individuals that played roles within the effort to respond, but the book also leaves a number of specific names out. According to interviews done for this dissertation with key individuals within the cohort of names that do not appear, Mark Bowden was approached due to his previous work that looked at US Special Operations soldiers. He was asked to obfuscate the identities of certain individuals he interviewed and allowed to use details without explicitly identifying them.¹¹⁵ The individuals involved in the effort to grant Bowden access to key communities of practice and central players wanted the story of Conficker to be publicized and memorialized both as a deterrent and as way to help institutionalize the various lessons learned.¹¹⁶ Not only was the avenue of a book length account undertaken but the constituency involved decided to permanently host various artifacts and information pertinent to the Conficker case online as a way to document the effort. The Department of Homeland Security funded the Rendon Group to research and publish a lessons learned document, also available on the Conficker Working Group's website. Specific segments of the operational security community will be discussed later in chapter four but first, the Conficker case will be broadly outlined to help round out the historical context in which information security communities of practice have arisen since the advent of the Morris Worm.

The Conficker effort is often cited as a template of sorts on how private, public, domestic, and international constituencies establish ad-hoc coordination to respond to a widespread Internet threat. Conficker was first noticed infecting computers in November of 2008 (Conficker A) and a second variant named Conficker B began showing up on infected computers in December 2008. Eventually five separate variants of Conficker would be identified. The Conficker malware was

¹¹⁴ Bowden, Mark. *Worm: The first digital world war*. Grove/Atlantic, Inc., 2011.

¹¹⁵ Author interview

¹¹⁶ Author interview

engineered to create a botnet. Botnets consists of computer code placed on machines (usually) owned or operated by a separate party to utilize that machine's processing power for one's own purposes, often illegal or nefarious in nature. One of the things that made Conficker more dangerous than previous botnets was the method it used to coordinate and control the network of computers it infected. Early versions of Conficker would attempt to "reach-out" to 250 "pseudo-randomly generated domains" each day, the domains were spread across eight Top Level Domains (TLDs). A TLD is defined as the last segment of a domain name such as '.com', '.net', '.org' or others. This tactic helped ensure that command and control (C&C) of the botnet was able to stay ahead of typical remediation methods which would simply block the handful of C&C servers which typically would be utilized to direct more run of the mill botnets. This fact meant combating Conficker necessitated registering the domains as they were being created in order to "sinkhole," essentially taking control of, Conficker's C&C infrastructure. That task was first done by hand by a select few early responders within the constituency of aware and able-bodied security practitioners. However, that strategy was fast seen as insufficient and requiring too great a degree of collaboration.¹¹⁷ The Rendon Group's report details the beginning of the larger effort. A Microsoft employee contacted the domain name registrar, Neustar that operated the .biz domain and asked their help to register a large block of .biz domains in order to stay ahead of Conficker. Rodney Joffe at Neustar then, in turn, contacted ICANN to request they waive the mandatory registration fees. This led to a robust agreement with ICANN and "Since that time, ICANN has instituted a formal process for registry operators to request a fee be waived when dealing with an

¹¹⁷ Conficker Working Group. "Conficker working group: Lessons learned." *Conficker-Working-Group-Lessons-Learned-17-June-2010-final. pdf*, published Jan (2011)

attack on the DNS system.”¹¹⁸ This brought several different constituencies into contact with each other: Microsoft whose software was exploited by Conficker, domain name registries that administer the process of registering new domains, ICANN that oversees and governs that process, security professionals within private companies, and academics that study and practice information security. As noted by the Rendon Group, this was not the first time such collaboration had ensued, the cases detailed above make that clear. What Conficker represented was a new scale and degree of collaboration. That collaboration was established, in part, due to a wider realization within the information security space that the community needed to be more proactive against the evolving threats present on the Internet.¹¹⁹ The community had tried to organize a response to another botnet earlier in 2008 named Srizbi, which was responsible for alarming amount of spam email. However, that effort was seen as a failure due to a lack of close coordination between involved parties along with an inability to sustain the effort to register domains used for Srizbi’s C&C due to insufficient funds on the part of the coordination entity, security firm FireEye.¹²⁰

With regards to Conficker, initial efforts at organizing by a small group of involved individuals coincided with a conference on DNS security being held in Atlanta, GA in early February of 2009. Initial work on registering Conficker domains had begun in late January, but the conference served as a meeting place to discuss Conficker and resulted in a partnership amongst a core group of individuals representing several organizations. That initial group then formed the Conficker Working Group (CWG), the members of which are listed in table 2.

¹¹⁸ Conficker Working Group. "Conficker working group: Lessons learned." *Conficker-Working-Group-Lessons-Learned-17-June-2010-final. pdf*, published Jan (2011), p17.

¹¹⁹ CWG (2011) Conficker Working Group, 2011 <http://www.confickerworkinggroup.org/>

¹²⁰ Ibid.

Table 2: Members of the Conficker Working Group¹²¹

Member	Description
IandI	German web hosting company
Afilias	US based top level domain registry
America Online (AOL)	US based internet service and content provider
Cisco	US based enterprise level hardware manufacturer
ESET	Canadian provider of antivirus and security software/solutions
F-Secure	Finnish cyber security and privacy company
Facebook	US based social network platform provider
Georgia Institute of Technology	US State university and research organization
Global Domains International	US based domain name registrar
IBM	US based provider of hardware/software and enterprise business solutions
ICANN	Governance organization responsible for the DNS system
Internet Storm Center (ISC)	Nonprofit entity of the SANS (Escal Institute of Advanced Technologies) that relies on an all-volunteer effort to detect and analyze problems on the Internet.
Internet Systems	US based security software company
IT-ISAC	Non-profit entity that facilitates information sharing within the IT sector
Juniper Networks	US based provider of network software and enterprise network hardware
Kaspersky	Russian based antivirus and security company
MacAfee	US based antivirus and security company
Microsoft	US based provider of operating systems and variety of productivity and other software and hardware
Neustar	US based internet security company
NIC Chile	Chilean administrator of the .CL domain
OpenDNS	Company and service which extend the DNS system and provides security solutions
SecureWorks	US based security solutions company now owned by Dell
Shadowserver	US based non-profit which helps provide server space for sinkholing operations
Sophos	UK based security software and hardware company
SRI International	US base non-profit scientific research organization
Support Intelligence	Security software and intelligence provider
Symantec	Antivirus and security solutions provider
Team Cymru	US based security non-profit that provides a variety of security services centered on the Internet
Trend Micro	US based security solutions provider
Verisign	US based operator of network infrastructure including a number of Internet root servers

In addition to working with US based domain registrars, the working group coordinated with the Chinese (.cn) domain registrar. Contact was made with the Chinese domain administrators that themselves are closely aligned with the Chinese government, in fact, getting China to cooperate proved easier than anticipated. Once that agreement was obtained, the Chinese were able to quickly block necessary domains, including ones that were already registered by another party. This fact was due to the level of control China exerts over its TLD domain and may not have been

¹²¹ CWG. “Working Group Members.” <http://www.confickerworkinggroup.org/wiki/>

possible within other countries.¹²² The captured domains were redirected to a set of servers, which at first, were operated independently among various involved parties. Microsoft announced the existence of the CWG publicly on 12 February 2009 while also offering a \$250,000 reward for information leading to the arrest of Conficker's author.

Interestingly and tellingly, the CWG did not formally coordinate with the US Government in any great measure. The following paragraph is quoted from the Rendon Group report and is an important and often cited justification for indicating the non-public, ad-hoc, nature of information security provisioning on and for the Internet:

“There were few formal contacts with the US government as an institution, but a large number of connections through personal channels. Several researchers within the Conficker Working Group, without coordinating with others, communicated through their own social networks with the FBI, DHS, DoD and various intelligence agencies. Questions were asked about how law enforcement could help and whether the group could help law enforcement. Later, law enforcement agencies from a number of countries placed representatives on the Working Group lists so they could follow developments, but these agencies were unable or unwilling to formally contribute to the group (though collaboration with specific individuals may have occurred)”¹²³.

The CWG did coordinate amongst themselves regularly, scheduling calls and exchanging messages electronically. The lessons learned portion of the Rendon report points out how this regularly scheduled contact was deemed a key factor to the CWG's successes. The “day to day” tactical workings of the CWG consisted of checking on the status of registered domains, making sure legitimate traffic wasn't impacted, generating reports, and in some cases, interacting with both the public and other parties to convey information and update progress. It is noted in the after-action report that most individuals with the CWG were volunteers lending their time above and

¹²² Ibid.

¹²³ Ibid.

beyond their normal “day jobs.” The CWG also experienced internal tensions as various parties within the CWG spoke independently of each other to the public and the media. Concerns brought about by other parties not participating directly in the group discussing their own remediation plans also helped dictate when Microsoft decided to announce the CWG. Coordinating attempts to manage public relations proved difficult: “At one point, people questioned why they could not talk to the media when they knew others in the group were briefing the government or private sector clients on the threat. This issue was never fully resolved.”¹²⁴

The Conficker case is an important milestone in the history of collaborative Internet security. It represents a culmination of the various practices established over the course of the post Morris Worm history of information security provisioning. In addition, it helps substantiate one of the central claims of this dissertation. That being the claim security communities of practice are products of an ever-evolving security culture that changes in response to threats and lessons learned during critical security events. Evidence for this is embedded within accounts of Conficker that note there was a shift prior to that effort within the operational security community toward a more proactive posture. Where was that shift happening, where does the operational security community exist? It exists, in part, as a social network built upon online communication and in-person interaction at conferences and other events. It will be discussed further below in chapter four.

¹²⁴ Ibid.

CHAPTER 4. THE MODERN SECURITY PROVISIONING SPACE

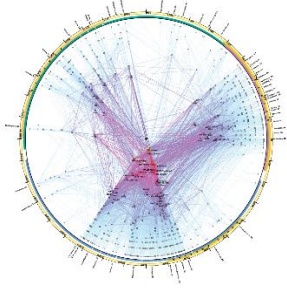
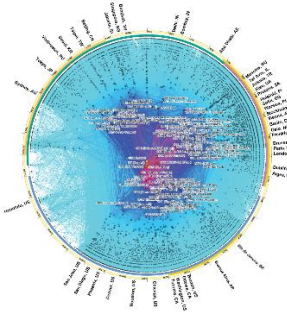
The following chapter helps understand the modern security provisioning space as interpreted through the ICIRS model and after establishing the historical context reviewed in chapter three. That environment includes several more institutionalized mechanisms than were in place during the Morris Worm incident and also includes parts that have evolved through and since the Conficker experience. The following chapter isn't chronological in arrangement, instead it is divided into five sections. The first section seeks to further explain and operationalize the way in which individuals and entities are embedded within the logical layer of the ICIRS model as consequence of the Internet's topology, the second section provides a discreet example of how those embedded entities result in a community of practice executing a task, in this case remediating a Border Gateway Protocol (BGP) issue. The third section considers a particular type of security provisioning activity called a "take-down" within the context of the Internet's operational security community of practice. The fourth section looks at the case of the Mariposa botnet to understand the post-Conficker world, and the fifth section holistically analyzes data gathered across twenty-eight incidents spanning the last twelve years. In doing so, the security community of practice is further substantiated, important seams and communities are characterized, discussed and understood.

4.1 Topology and Complexity

As the Internet itself became more complex, the various top-level autonomous systems (AS) over the course of the 1990s and 2000s multiplied and became far more interconnected. Evidence of the topological complexity and evolution is obvious from perusing data produced by the Center for Applied Internet Data Analysis (CAIDA). The visualizations represent AS Core

graphs. An AS references an independent “autonomous system” that identifies itself to other autonomous systems. These systems then route packets addressed to entities within that AS independently. The system that controls the identification and routing of data between various AS is called border gateway protocol (BGP) and will be further described later in this work. For now, however, there are two important dynamics to understand that are conveyed by Table 3. The first is the increase in the number of autonomous systems and the second is the interconnection of the systems in terms of the traffic polled/collected to visualize its snapshot in time.

Table 3: CAIDA AS Core Graph

AS Core Graph in 2000	AS Core Graph in 2018
	
<p>Source: Center for applied Internet Data Analysis¹²⁵</p>	

Outlining the way traffic transits the system and infrastructure management contributes to understanding the implication of this topological complexity. Internet traffic, that is the information represented as data packets, traverses various Autonomous Systems in order to get from a point of origin to a destination. Historically, a hierarchical designation of various networks designated Tier 1, Tier 2 and Tier 3 helped distinguish among various typologies (defined through

¹²⁵ CAIDA “A Historical View of the AS Core.” CAIDA.
https://www.caida.org/research/topology/as_core_network/historical.xml

scale and traffic volume) of managed interconnected networks. The modern Internet is less hierarchical and not as easily classified by such nomenclature, but the designations persist to help understand Internet topology. A common example of a Tier 1 Network is the vast interconnected physical and virtual infrastructure operated by L3 Communications. L3 is a provider of backbone Internet services (among many other services) to other industry players, which include internet service providers (ISPs), who provide “last mile” connections to everyday users (i.e. companies such as Comcast, AT&T and others). As data traverses the various networks within the Internet, formal and informal agreements allow for both “transit” and “peering” amongst various autonomous systems. Transit is an agreement to allow data to cross one’s network providing both upstream and downstream routing to the networks connected to the entity network being transited. These agreements are often formal and are characterized as service level agreements (SLAs) that involve contracts to provide access to the larger Internet. A second sort of arrangement is called “peering”. Peering involves sharing traffic volume and downstream routing with a partner, and these arrangements are often traditionally informal in nature. Peering involves hardware interconnection done at a physical location known as an Internet Exchange Point or IXP. According to a list maintained by Packet Clearing House (PCH) an international non-profit organization responsible for some aspects of IXP governance, there are at least 924 physical IXP locations, but those locations support more than a million individual peering agreements between entities.¹²⁶ Traditionally, this is seen as a mutually beneficial relationship in that downstream routes (towards the endpoint/user) can be shared to the mutual benefit of both participants instead of paying for an upstream transit arrangement, thus reducing cost to IXP participants while

¹²⁶ Woodcock, Bill, and Marco Fingino. *2016 Survey of Internet Carrier Interconnection Agreements*. Packet Clearing House, 2016. <https://www.pch.net/resources/Papers/>

granting them access to larger downstream population. Surveys find that these peering arrangements are remarkably resistant to formalization and instead rely on informal “handshake” agreements. According to PCH, of 1,935,822 analyzed agreements in 2016 found .07% were formalized in written contracts.¹²⁷ This represents a drop from the 0.49% found in a 2011 survey.¹²⁸ This means the 99.93% were informal handshake agreements that PCH characterized as “...in which the parties agreed to informal or commonly understood terms without creating a written document.” The same survey report goes on to state:

“These numerous informal agreements are arrived at by the “peering coordinators” or carrier-interconnection negotiation staff of the networks, often at self-organized regional or global “peering forums” that take place many times each year. Several of the respondents who participated in follow-up interviews noted that they expected the portion of written contracts to continue to decline over time because, in many cases, existing written contracts were expiring as their defined terms passed or their original signatories were subsumed, and although the relationships continued to grow on an informal basis, the written contracts related to them were not being renewed.”¹²⁹

This informality also breeds social connectivity among the individuals charged with making sure the IXPs function and connectivity is maintained. That social strata instantiated through peering forums is but one way communities of practice arise. Those types of connections will be further operationalized in the section below. Two technical distinctions have been made above, 1) The Internet relies on a system of *routing* of data packets amongst many autonomous networks and subnetworks, and 2) this means there is pervasive interconnection in the form of transit and peering which is controlled through both formal and informal mechanisms. The implications of this

¹²⁷ Woodcock, Bill, and Marco Fingino. *2016 Survey of Internet Carrier Interconnection Agreements*. Packet Clearing House, 2016. <https://www.pch.net/resources/Papers/>

¹²⁸ Ibid.

¹²⁹ Ibid.

interconnected system of operation are apparent *each level of analysis* when viewed through the ICIRS model. The physical and logical layers of the Information Centered Security Model (which are both part of ICIRS) encompasses the resources and constituencies being discussed here. The system of routing and the protocol stack across which the discussed interconnection of tier 1, 2, and 3 network providers operate can be thought of as having implications when coming into contact with individual, state, international, global, for-profit and non-profit levels of analysis. As discussed above, the system of interconnection is governed by non-profit entities such as the IETF and ICANN that have been studied and detailed by other authors as they impact on each of those levels, however at a less abstract level, how are problems solved when something goes wrong in terms of everyday function?

Answering that question means looking at the operational level of practice, at which other institutions have evolved as the Internet has grown. The various network operators across the various tiers have evolved regional collectives known as Network Operations Groups (NOGs), several which exist across various regions. Network engineers and practitioners can exchange information through these collectives. The first of these collectives was the North American Network Operators Group (NANOG), which evolved from NSFNET “Regional-Techs” meetings. These meetings were a chance for technical staff from various regional networks that made up NSFNET to discuss operation issues of common concern eventually formalizing into NANOG. Meetings are held three times each year, and include presentations, tracks, and tutorials. The meetings are informal, NANOG membership and meetings are open to all interested individuals. Conference participants typically include senior engineering staff from tier 1 and tier 2 ISPs. Participating researchers present short summaries of their work for operational feedback. Individuals interviewed for this dissertation spoke of “bird of a feather” (BoF) gatherings taking

place on the periphery of NOG meetings.¹³⁰ These sorts of periphery meet-ups can be social in nature or centered on a specific topic or job function drawing a smaller subset of attendees from the larger NOG conferences.¹³¹ Matthews studies and details the establishment and activities of the North American NOG (NANOG) in his dissertation, his findings reinforce the assertions made here. He asserts that the institution acts as an “anchor” that helps draw together individuals who form trust relationships, both with each other, with the institution, and with the involved technology thus instantiating a “community of practice”.¹³² In effect, individuals and entities participating in NANOG and similar collectives drawn from the ranks of companies and organizations managing and governing the Internet, are embedded within the logical layer of the ICIRS model. As such, they possess a unique mix of agency and awareness that allows them to function both as a threat recognition and remediation agents. In order to better understand how such communities of practice function, the following section will focus on the individual level as a means to show how the interconnected topology of the Internet has bred a community of practice that is able to recognize and remediate issues related to BGP routing. It is necessary to keep in mind that parts of that same community overlap with a wide array of other security focused elements and communities of practice, parts of which were discussed in the case vignettes presented above in chapter three and will be discussed again later in this chapter.

¹³⁰ “The History of NANOG.” *North American Network Operators Group*, www.nanog.org/history.

¹³¹ Author interview

¹³² Matthews, Ashwin,. (2014). *Where in the World is the Internet? Locating Political Power in Internet Infrastructure*. pp 10.13140/RG.2.1.1243.2087

4.1.1- BGP Routing Errors

Threats born of malicious intent using malware, such as those previously detailed, are not the only vector of compromise on the Internet. Structural realities of how the Internet functions can leave the system open to adverse consequences due to misconfiguration, errant data, or exploitation. Border Gateway Protocol (BGP), introduced above, is a standard through which various autonomous networks can identify what servers belong to which disparate connected network. For example, Google servers know which ones belong within their own network, and collectively, that network is identified and recognized by other networks that reciprocate this awareness. This arrangement is necessarily transparent so that data is able to traverse the many collections of physical infrastructure, much of which is owned privately or held by universities and public entities and together make up the Internet. The traversal of that data is known by the technical term “routing.” The reciprocal recognition of networks relies on simple trust. We “trust” Google’s servers to identify themselves, just as we “trust” Netflix or the US Government to identify their own servers. These lists of self-identified networks are then propagated across the Internet, shared so that any connected terminal is able to ask for and receive the data it requests. That data may cross many third-party owned or controlled networks in order to arrive at the requesting terminal. This system of trust has not always functioned as envisioned. Examples of the transnational effects of such BGP errors abound. For example, in March 2015, an Indian broadband provider named Hathaway changed a technical prefix (the identifying marker of an individual network), accidentally directing traffic meant for Google’s servers to their own network. According to a news article detailing the incident, “Hathaway’s BGP error was accepted by its transit provider Bharti Airtel, which then broadcast the changes. The incorrect routes were

accepted by other network providers including Cogent, Level 3, Orange, Singapore Telecom and Pakistan Telecom...”¹³³

Private network operators provide a significant portion of worldwide bandwidth, acting as a middle-man between service providers that provide access to the wider public, these providers (like Cogent, Level 3 and others) make up the Internet’s “back-bone”. BGP errors manifest in the inaccessibility of affected servers, in this case the appearance of “Google” services being down. When BGP routing is utilized maliciously, an act known as “route hijacking”, which occurs when false mappings are propagated to intentionally reroute traffic to a third party. These sorts of incidents, malicious or unintentional, occur with surprising frequency on the modern Internet. Recognizing, diagnosing, and subsequently fixing such occurrences take place on small time-scales. Usually, when a major network, i.e. Google, experiences a BGP-related error, the problem is solved in a matter of hours. It is useful to briefly trace the manner in which such threat redress occurs. The following testimonial appeared as a blog post on the website of the California based computer security firm, CloudFlare:

“Today [6 Nov 2012], Google's services experienced a limited outage for about 27 minutes over some portions of the Internet. The reason this happened dives into the deep, dark corners of networking”¹³⁴.

¹³³ Kirk, Jeremy. “Google Services Disrupted by Routing Error.” *CSO Online*, IDG News Services, 13 Mar. 2015, www.csoonline.com/article/2896395/network-security/google-services-disrupted-by-routing-error.html.

¹³⁴ Paseka, T. Why Google Went Offline Today and a Bit About How the Internet Works. *CloudFlare* (November 6, 2012) <https://blog.cloudflare.com/why-google-went-offline-today-and-a-bit-about/>

The same individual goes on to explain the reason for the outage, and how he tracked the problem to an Indonesian ISP:

“I looked at the BGP Routes for a Google IP Address. The route traversed Moratel (23947), an Indonesian ISP. Given that I'm looking at the routing from California and Google is operating Data Centre's not far from our office, packets should never be routed via Indonesia. The most likely cause was that Moratel was announcing a network that wasn't actually behind them”¹³⁵.

The US-based engineer was able to help effect a solution by contacting Moratel. He writes:

“The solution was to get Moratel to stop announcing the routes they shouldn't be. A large part of being a network engineer, especially working at a large network like CloudFlare's, is having relationships with other network engineers around the world. When I figured out the problem, I contacted a colleague at Moratel to let him know what was going on. He was able to fix the problem at around 2:50 UTC 6:50pm PST. Around 3 minutes later, routing returned to normal and Google's services came back online. Looking at peering maps, I'd estimate the outage impacted around 3–5% of the Internet's population. The heaviest impact will have been felt in Hong Kong, where PCCW is the incumbent provider. If you were in the area and unable to reach Google's services around that time, now you know why”.¹³⁶

The preceding anecdote demonstrates the process by which involved entities were able to coordinate and redress a certain subset of routing problems and helps operationalize one such community of practice being discussed within this dissertation. The actors were able to coordinate across minor seams. The collaboration presented is somewhat ephemeral and takes place on a small time-scale. In this case, a third-party security firm noticed an outage of *Google's* service. An *individual* within that third-party firm decided to diagnose the issue, and was able to enact a solution that affected 3-5% of the *Internet's total user population*. That solution involved a US-based computer engineer leveraging a social connection with another individual located across the

¹³⁵ Paseka (2012)

¹³⁶ Ibid.

world. It is conceivable that “maintenance of relationships” referenced by the CloudFlare engineer references the types of relationships built and maintained at NOG meet-ups detailed earlier. All this happened *without* the involvement of Google, the company whose system was most affected by the routing error. According to the blog post, the problem was first observed around 6:24 PST in California and the solution was enacted in Indonesia at 6:50 PST.¹³⁷

This case illustrates the enabling effect of minor seams at the individual and for-profit levels of analysis. The leveraging of a social connection between two engineers in separate private firms located in different countries remediated an issue that affected a large portion of the Internet’s user community, even though major seams existed between the parties effected and involved. In fact, Google, the company most effected by the error was *not* involved in the diagnosis and remediation of the problem. If Google had been involved, they would have necessarily had to contact Moratel but may not have benefited from the social connection and thus minor tie these two engineers had. In fact, one can assume that Google’s internal process may have led to a slower response due to an entrenched bureaucracy characterized by many seams. The example helps operationalize the concept of a community of practice, as does the prior discussion of Morris Worm. Admittedly, the contexts of those two discussions are very different. However, the Morris Worm incident shows how the very structure of the early Internet begat a system of distributed agency brought to bear during crisis and problem solving, and the BGP routing case shows how continued evolution in scale and interconnectedness has bred entrenched and robust communities of practice centered on continued operation of the Internet while also having implications at various levels of analysis. There is significant overlap between the network engineering community of practice and the

¹³⁷ Ibid.

community surrounding security, and the next section will identify specific segments of that community and discuss various facets of identity and practice.

4.2 The Operational Security Community of Practice and the “Takedown”

The sections above sketched, in a broad sense, a community of practice that evolved around network engineering leveraging individuals and entities embedded within the logical layer of the ICIRS model and involved with the function and management of the Internet. Similarly, there exists an operational security community of practice that does overlap substantially with the network engineering community of practice as the individuals are often employees of various companies and institutions that help manage the Internet’s network infrastructure. This includes hardware, software, tier1, 2, and 3 network companies along with governance institutions such as ICANN and academics. In addition, that community also draws on specialty industry experience such as individuals involved in banking, defense, law enforcement, and others who have deep ties to information technology and Internet security due to niche experience as consequence of job function as well as for profit and non-profit information security focused companies and institutions.

The author attended a conference of the Internet Security and Operational Intelligence (ISOI) group, conducting the field work presented within this dissertation. ISOI is an event to which all new attendees have to be “vouched” for by an existing ISOI member or members before being invited. ISOI represents a “loose, grassroots collaboration of various security and Internet infrastructures stakeholders.”¹³⁸ The conference is held at least once and sometimes twice a year, at times on the periphery of another security conference or event so as to maximize the ability of

¹³⁸ Author interview

members to attend. This is a non-trivial issue as multiple ISOI attendees discussed the lack of institutionalized funding within their respective organizations to attend an event such as ISOI, this is despite of the utter centrality these same individuals placed on ISOI as an integral part of both their job and professional networking. There were representatives from all the above referenced categories present at the event attended by this author. The conference content is not published and all discussions at ISOI are held in general confidence (unless otherwise specified) amongst attendees in order to encourage openness and frank discussion amongst participants. This author spoke with multiple attendees to gather information and understand the community and types of practices that enable individuals and institutions to participate in security provisioning and threat recognition inherent to the modern Internet and information technology space. Individuals present at the conference represented a cohort containing one or multiple persons whom were active participants in most malware/take down operations covered within this dissertation spanning 2008 to 2017. Discussions with these individuals were mostly semi-structured or unstructured and all of them asked that specific attribution not be assigned due to operational security concerns. Thereby, specific insights generated are not attributed to individuals but are noted as derived from author interviews.

The ISOI community makes use of multiple channels of communication in order to exchange information and collaborate. In addition to the in-person conferences, members communicate via the online Ops-Trust portal (Ops-T). Ops-Trust is a heavily peer vetted online forum that has been purpose built to facilitate secure collaboration amongst the operational security constituency.¹³⁹ Their mission is to promote “...responsible action against malicious behavior beyond just

¹³⁹ Ops-Trust “Mission” ops-trust portal. <https://portal.ops-trust.net/>

observation, analysis, and research.”¹⁴⁰ Ops-T enables collaboration using various models of trust chosen and administered by constituencies who govern themselves and utilize the Ops-T platform. Thereby, an account on Ops-T only allows you to participate within a group if that group 1) invites you, and 2) you are affirmed within the trust model that group has instantiated. This could mean that at least one person already in the group has vouched for you and you have been approved by a group administrator or it could mean that all members of the group have to vouch for you before you are granted access to that group’s communications and materials. Conceptually, member groups on Ops-T follow a structure that distinguishes between a “sphere of trust,” a “sphere of action” and a “need to know”. The practice is fairly well institutionalized and translates the idea that information and interaction stays within “sphere of trust” which is vetted, that action is conducted amongst a group of trusted actors, and only those with a need can access relevant information. One of the most obvious indicators of practice observed across the Ops-T community both through interactions during ISOI and beyond within the more general information security community of practice, is usage of a highly institutionalized system of information classification. This system is referenced as traffic light protocol or “TLP.”

TLP is system that marks information shared amongst community members as belonging to either a “white,” “green,” “amber,” or “red,” category. Tracing the history of TLP is difficult as various individuals interviewed gave divergent accounts of when it was introduced, however it appears that individuals within various NOG communities developed and institutionalized it within the Forum of Incident Response and Security Teams (FIRST) organization.¹⁴¹ According to FIRST materials, the protocol has its roots in the United Kingdom amongst public and private

¹⁴⁰ Ops-Trust “Mission” ops-trust portal. <https://portal.ops-trust.net/> and author interviews

¹⁴¹ FIRST is an Umbrella organization of worldwide CERTS, both constructs are discussed in further detail later within this section

sector security professionals. Various ISACs, CERTs, and other important communities further adopted the protocols. Even US-CERT within DHS has adopted TLP and publishes guides on their website detailing definitions of the various categories that they derive from FIRST. The FIRST guide provided to the public contains some insight into the inherited nature of language and the way in which the community builds upon prior work. The version 1.0 document has a footnote which reads “This document uses ‘should’ and ‘must’ as defined by RFC-2119.”¹⁴² The term RFC references IETF “Requests for Comment,” which are memos that document technical and organizational notes about the Internet that help codify various technical standards and norms while also providing a vector of institutional knowledge retention. RFC-2119 published in March 1997 concerned “Key words for use in RFCs to Indicate Requirement Levels.”¹⁴³ The RFC codifies when and how to use the terms “MUST,” “MUST NOT,” “SHOULD,” “SHOULD NOT,” “MAY.” It also specifies how to use those terms with regarding “security consideration”:

“These terms are frequently used to specify behavior with security implications. The effects on security of not implementing a MUST or SHOULD, or doing something the specification says MUST NOT or SHOULD NOT be done may be very subtle. Document authors should take the time to elaborate the security implications of not following recommendations or requirements as most implementors will not have had the benefit of the experience and discussion that produced the specification.”¹⁴⁴

That language is used subsequently when defining the TLP system. FIRST specifies:

- “TLP RED - Not for disclosure, restricted to participants only. Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for

¹⁴² FIRST “Traffic Light Protocol (TLP).” <https://first.org/tlp>

¹⁴³ Bradner, Scott. “Key words for use in RFCs to Indicate Requirement Levels.” Internet Engineering Task Force (IETF). 1997. <https://tools.ietf.org/html/rfc2119>

¹⁴⁴ Bradner (1997)

example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.

- “TLP AMBER - Limited disclosure, restricted to participants’ organizations. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.
- “TLP GREEN - Limited disclosure, restricted to the community. Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
- “TLP WHITE - Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.”¹⁴⁵

TLP is now firmly ensconced among security professionals, and interestingly, the community has even established various sanctions for individuals that violate TLP. These vary depending on the severity of the disclosure, ranging from admonishment to full excommunication. One professional interviewed for this dissertation expressed excitement for the manner in which that sanctioning has changed, commenting that “...it used be that the community was too small and if someone violated TLP you had to balance the necessity of their presence within the community with the fact they leaked. However, now that the community is bigger, we have multiple resources and individuals who can step up”¹⁴⁶ Several individuals interviewed at ISOI expressed the

¹⁴⁵ FIRST “Traffic Light Protocol (TLP).” <https://first.org/tlp>

¹⁴⁶ Author interview

importance of TLP and discussed considerations when conveying information and collaboration. They spoke of various cases in which TLP was violated and the community took action to sanction guilty parties.

While TLP has been informally used for, at least, the past decade and a half, it wasn't until 2016 that a FIRST special interest group produced a common, standardized set of definitions for all TLP colors.¹⁴⁷ The manner that TLP has been adopted and relied upon within the community is a powerful indication of practice and community made obvious in no small part by the seriousness with which individuals adhere to the classification scheme. Emails and printed information passed among community members are designated with the "...TLP color of information in the subject line and in the body of the email, prior to the designated information itself. TLP color must be in capital letters..."¹⁴⁸ The fact that the system can lead to sanctions despite the lack of any formal legal mechanism underlying the system makes apparent the institutionalized culture present within the security community of practice.

The community of practice surrounding information security manifests that culture as shared concept of *identity*, and TLP along with the cultural norms surrounding its usage helps indicate and define it. TLP shows how the initial debates which took place on Phage during the Morris Worm that questioned who should be included and have access to the mailing list have evolved into the present. Those questions led to the creation of tools and mechanisms such as TLP. One of the reasons such a system is necessary is due the active operations the community of practice engages in. The next section will discuss the practice of a "takedown".

¹⁴⁷ FIRST. "Traffic Light Protocol (TLP-SIG)." <https://www.first.org/global/sigs/tlp/>

¹⁴⁸ FIRST "Traffic Light Protocol (TLP)." <https://first.org/tlp>

4.2.1 The “Takedown”

ISOI is but one trust group utilizing Ops-Trust. The site allows for mixed media collaboration and information sharing. It is an example of the multiple collaborative mechanisms that have sprung up around Internet security since the days of the Morris Worm. What once was just mailing lists has evolved into incorporated non-profits with purpose-built information infrastructures, conferences, public and private partnerships, social networking and communication mechanisms, and much more. These range from highly vetted platforms like Ops-Trust to easily accessed mailing lists, to large scale corporately backed Information Security Analysis Centers (ISACs) which often exist as both private partnerships and as private/public partnerships across various industry sectors and geographic groupings.

In the US, the National Council of ISACS serves as an umbrella organization of 24 “organizations designated by their sectors as their information sharing and operational arms.”¹⁴⁹ ISACS were introduced through Presidential Decision Directive-63 (PDD-63) in May of 1998 and began forming around individual critical infrastructures in 1999. The organizations exist to foster public/private information sharing and many have 24/7 warning and incident reporting capabilities.¹⁵⁰ The Nation Council describes its role as follows:

“The NCI is a true cross-sector partnership, providing a forum for sharing cyber and physical threats and mitigation strategies among ISACs and with government and private sector partners during both steady-state conditions and incidents requiring cross-sector response. Sharing and coordination is accomplished through daily and weekly calls between ISAC operations centers, daily reports, requests-for-information,

¹⁴⁹ Council of ISACs. “About ISACs.” *National Council of ISACs*, www.nationalisacs.org/about-isacs.

¹⁵⁰ *Ibid.*

monthly meetings, exercises, and other activities as situations require. The NCI also organizes its own drills and exercises and participates in national exercises.”¹⁵¹

The ISAC concept has spread to other regions of the world, for example in Europe the European Union Agency for Network and Information Security advocates for the establishment of European and National level ISACs and has published various reports detailing cooperative models being used along with incentives and barriers to information sharing within the European ISAC context.¹⁵² In addition to ISACs which operate as an interface between private critical infrastructure providers and national governments, the concepts of CERTS was alluded to above as an outcome of the Morris Worm incident.

CERTS act as another information sharing and central location on which countries and industries can turn to for information security expertise. In the US case, the original DARPA funded CERT at Carnegie Mellon was incorporated into the Department of Homeland Security as US-CERT and now publicizes cyber threats both to the technical community and public. However, all these organizations, ISACS, CERTS, and other information sharing infrastructures differ, conceptually, from the operational community represented by Ops-Trust and other organizing mailing lists, forums and communities. Perhaps the most obvious indicator of practice related to that community has become a persistent march of botnet takedowns which have continued from the time of Conficker to the present. The “takedown” is a term that is shorthand for an operation aimed at stopping malicious activities due to malware often associated with botnets or other widespread threats. Over time, takedowns have evolved into legitimate legal maneuvers including

¹⁵¹ Council of ISACs, 2019

¹⁵² <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing>

law enforcement and judicial constituencies but there have been historic examples which may have been within legal “gray space.”

Academic literature that arose in the wake of the Conficker incident served as early indications of practice that institutionalized the terminology of takedowns. Examples of early papers include the 2012 workshop presentation by Dave Dittrich entitled “So You Want to Take Over a Botnet.” The author begins by defining basic terminology like “bot” and “botnet” before defining various levels of response ranging from observation to takedown and eradication. He defines the “takedown” as identifying weaknesses in the C&C structures...” that “...can completely disrupt any new infections, any connections with the C&C infrastructure, and any means of the attacker countering your actions.”¹⁵³ Dittrich notes when discussing the takedown of the Storm botnet that remediation efforts which demonstrated one could remotely clean up some infected computers without interaction from those system owners fell into realm of “...some well-reasoned ethical debate.”¹⁵⁴

Dittrich briefly outlines some examples of takedowns which include the Totpig, Mega-D, Conficker, Waledac and Mariposa botnets. The Mariposa botnet will be further explored in the next section. Before doing so, it is important to note the myriad tools and organizations that have sprung up around the idea of operational security, information sharing, and security provisioning. As detailed above, portals such as Ops-Trust and others should be considered strong indicators of practice helping to show how the community of practice is engaging in collaborative discussion and problem solving. Mechanisms such as TLP also help illustrate an institutionalized culture

¹⁵³ Dittrich, David. "So You Want to Take Over a Botnet..." University of Washington (2012) <https://staff.washington.edu/dittrich/papers/dittrich-leet2012.pdf>

¹⁵⁴ Dittrich (2012), p2

unique to the community which has evolved since the time of the Morris Worm. Specific non-profit entities have been setup to facilitate take-down activities as well. Once such organization is the Shadowserver Foundation.

Founded in 2004, the Shadowserver Foundation is a non-profit entity which helps facilitate “sink-hole” operations. A “sink-hole” is the term of art for the act of redirecting illicit traffic away from the intended C&C infrastructure which is emanating from infected computers within a botnet to a third-party server controlled by “the good guys.” Part of Shadowserver’s utility is that the foundation helps provide server space for such operations, this can cost money and as detailed in several of the cases above, can be the cause of failure or limited success. Volunteers help run Shadowserver, one such individual interviewed commented that while it was a role he filled due to his interest, his Shadowserver activities often take up more time than his “day job.”¹⁵⁵

Shadowserver also lists the following goals on their website:

- “Investigate and contribute to new technologies in botnet control.
- “Develop and deploy new methods for harvesting malware and studying its behavior.
- “Develop and utilize additional techniques for gathering and analyzing botnet data and network flows.
- “Work more closely with ISPs, Hosting and DNS providers in the identification and mitigation of botnets and malware propagation.
- “Increase our collaboration with other key security organizations and researchers to share discoveries and analysis.
- “Develop and release whitepapers and reports based on our research.
- “Further develop our website to provide information and reports to the interested public.
- “Participate in future security conferences and workgroups.
- “Increase our communication with the public through irc, mailing lists, and the website”¹⁵⁶

¹⁵⁵ Author interview

¹⁵⁶ Shadowserver (1) “Mission.”

<https://www.shadowserver.org/wiki/pmwiki.php/Shadowserver/Mission>

It should be noted, that while Shadowserver's website appears to not have been updated in quite some time, the organization is still very much active as indicated by discussions with participants and representatives during various conferences and workshops attended by this author. For example, Shadowserver participated in the takedown of the Avalanche "fast flux" malware, during which sink-holing operations showed at least two million unique victim IP address from the world in just over a 48-hour period. Avalanche will be discussed further later in this chapter; the next section will explore the Mariposa Botnet to help understand the diverse set of actors and constituencies within the modern provisioning environment.

4.3 The Mariposa Botnet

Whereas Conficker represented an incident in which the perpetrators were never found, the Mariposa Botnet followed closely on the heels of that event and represents a more complete case study in that it involved a law enforcement investigatory phase and a prosecutorial phase that unfolded across international borders and involved several elements. It is used here as an introduction to the modern security community of practice that crosses many constituencies and highlights a more mature infrastructure than that of Conficker, though it hails from the same time period. It also represents the now common practice called a "takedown" that has evolved as a partnership across private and public constituencies to help identify emerging threats and threat actors, and then undertake actions to mitigate, investigate and prosecute those actors. In fact, various non-profits and mechanisms have sprung up to help facilitate such operations. After

discussing the Mariposa case, data gathered across a number of takedown/remediation events will be presented before drawing conclusions guided by the ICIRS model in chapter five.

In 2009, a Canadian information security company, Defence Intelligence, observed a piece of software being propagated that permitted a degree of remotely administered control over a wide range of computers. They named this network of compromised computers the “Mariposa botnet.” The Mariposa botnet infected more than “half of Fortune 1000 companies and more than 40 major banks.” The botnet was associated with over 11 million IP addresses between 23 December 2009 and 9 February 2010.¹⁵⁷ What transpired was a multi-national effort to eradicate the botnet, eventually leading to the arrest and prosecution of individuals in Slovenia and Spain. Tracing the evolution of the botnet’s discovery, the building of a constituency to address the botnet, and the linkages within and outside of the information security space which led to arrests, prosecutions and mitigation provides insight into how diverse information security provisioning communities connect and function, while also highlighting several organizational seams.

Defence Intelligence was not the first company to observe the coordinated command and control of Mariposa through Domain Name System (DNS) activity. The coordinated communication of globally dispersed computers to centralized servers that did not seem to have legitimate functions was noticed by several organizations.¹⁵⁸ The original C2 servers coordinating Mariposa were housed in Israel and Germany and activity was noticed by another security firm, Prevx.¹⁵⁹

¹⁵⁷ Sully, Matt, and Matt Thompson. "The deconstruction of the Mariposa botnet." *Defence Intelligence*. Retrieved September 16 (2010): 2012., p4

¹⁵⁸ Sully and Thompson (2010), p11

¹⁵⁹ Ibid. p11

The Mariposa botnet seemed to be based upon a set of pre-packaged malware tools known as the “Butterfly Exploit Kit.” The kit was available for between 400 and 700 euros on known websites being sold as a “security” tool.¹⁶⁰ In order to address the problem, Defence Intelligence, a relatively small company, forged a diverse set of partnerships. In a paper published by the company, they note there were few law enforcement institutions within their native Canada to which they were able to turn for help.¹⁶¹ They rejected a formal arrangement with the Technological Crime Branch of the Royal Canadian Mounted Police (RCMP), concluding that it was hostile to free information exchange. Instead, they forged a relationship with information security professionals at the Georgia Tech Research Institute and Panda Security, an information security focused firm based in Spain. When individuals associated with the effort were asked why they chose those partnerships, they answered that the team reflected professional connections built, in large part, through previous employment at a prior company in which a core group of participants were all coworkers.¹⁶² The three entities branded their collaboration the “Mariposa Working Group.” The working group tracked Mariposa activity in Latin America, South Korea, Europe, the United States, and the Middle East. Using technical means, they identified where the botnet was being administered, narrowing the location to Spain. Spanish authorities were contacted and the Spanish judicial system was leveraged to provide internet service provider records. This led to the arrest of a Spanish citizen and the identification of several individuals involved in the

¹⁶⁰ Ibid. p11

¹⁶¹ Sully and Thompson (2010), p7

¹⁶² Author interview

botnet's administration. In addition, the creator of the Butterfly Malware Kit was arrested in Slovenia.¹⁶³

The Mariposa case provides a detailed example of the networked structure of modern information security provisioning and the resulting organizational seams. A small Canadian firm sought to address widespread infection of malware across private and public computer networks dispersed globally. Perceived weakness within the Canadian information security response infrastructure led the firm to partner with a US educational/research entity and another private Spanish firm. The established "working group" captured and redirected internet traffic in order to investigate an identified threat. Upon completing its research, the response then drew upon law enforcement and judicial infrastructure in Spain, Slovenia, the United States and several other countries. The nature of that collaboration is revealing. The individuals arrested in Spain and Slovenia were also indicted in the United States and the indictments provide a lens into the nature of trans-national legal collaboration within and around the information security space.

According to the indictment *United States of American v. Matzaz Skorjanc, Florencio Carro Ruiz, and Mentor Leniqi*, the individuals involved engaged in violations of US law regarding racketeering, conspiracy to commit fraud, and conspiracy to commit computer crimes.¹⁶⁴ According to the indictment, the FBI conducted an investigation that benefited from collaboration with at least one informant (unnamed) and collaboration with Spanish and Slovenian law enforcement. This included sharing information obtained during searches by those entities. For example, "Chat logs obtained during the search of RUIZ's residence, and analyzed by the Spanish

¹⁶³ Sully and Thompson (2010), p8 and *United Sates v. Skorjanc* Case. 1:11-mj-00321-AK. *The United States District Court For the District of Colombia*, <https://www.justice.gov/opa/file/630811/download>

¹⁶⁴ *United States v. Skorjanc*

Guardia Civil, demonstrate that RUIZ and Ostiator intentionally executed a DDOS attack against several websites at the request of Torbe.”¹⁶⁵ Spanish authorities were able to zero in on the perpetrators due to information obtained by the Mariposa Working Group, one of the criminals “made a mistake” and tried to connect to a C&C server without anonymizing themselves. This information was turned over to Spanish investigators who were able to trace the individual’s identity.¹⁶⁶ The indictment also makes use of information obtained by Slovenian authorities specifically, “The digital evidence seized by the Slovenian National Police also contained saved online chat logs.”¹⁶⁷ Information in such evidence was used to establish the charges against the defendants.

When viewed through the lens of organizational seams, the Mariposa example has several minor and major seams. In this case, coordination occurred across the minor seams and the major seams actually constrained collaboration. For example, the decision by Defence Intelligence to reject collaboration with the RCMP shows how the existence of a major seam between a government agency and a private firm structures choice in that it constrained their willingness to coordinate. Rather, Defence Intelligence coordinated trans-nationally which paradoxically represents a minor seam consisting of information security professionals exploiting their social connections enabling an ad hoc yet effective working group that provided a public good ultimately leading to remediation and prosecution. The Mariposa case is also useful because it goes beyond the Conficker example to show how law enforcement and judicial elements have become equally important within the remediation effort with regard to large scale Internet based threats. The strategy that has emerged within both the operational security community of practice and the larger

¹⁶⁵ Ibid, p8

¹⁶⁶ Dittrich (2012), p4

¹⁶⁷ United States v. Skorjanc, p28

law enforcement community is an agreement that to stop these large-scale threats, the *people* behind them must be pursued and punished. Just such a strategy has been pursued by Microsoft which will be explored next.

4.4 Microsoft Botnet Takedowns

The history and chronology presented thus far has illustrated the ever widening and ever more complex emergence of cybersecurity concerns over the history of the Internet's evolution. Controlling the spread and effect of botnets, particularly, has become a central security issue for various private entities that have business interests dependent on the Internet's continued function and ease of access for the public. This has led to a strategy that closely links such private entities to public legal and law enforcement resources. Microsoft has pioneered pursuing civil action to "thwart and disable botnets"¹⁶⁸. One of the first of these actions was the takedown of the Waledac Botnet in 2010.

Waledac was a network of infected computers that were sold as a service to third parties who utilized the network to send out spam email and execute criminal activities.¹⁶⁹ Waledac used 277 unique addresses to execute command and control over several "tiers" of infrastructure, the lowest being the infected computers that sent out actual spam and the upper tiers being a complex C&C system of repeaters. From a technical point of view, this tiered system meant past remediation practices would be difficult to accomplish.

¹⁶⁸ Hiller, Janine S. "Civil cyberconflict: Microsoft, cybercrime, and botnets." *Santa Clara Computer & High Tech. LJ*31 (2014): 163.

¹⁶⁹ Hiller (2014), p. 177

As such the strategy Microsoft designed was to pursue *ex parte* civil action directly suing “John Doe” defendants while asking for preliminary injunction which required VeriSign, a domain register, to lock the domains while the ownership was verified. They pursued this action based not only on the Computer Fraud and Abuse Act and the more recent CAN-SPAM Act, but via trademark litigation. Microsoft employed the Lanham Act arguing the usage of Microsoft systems (Hotmail) and products to carry out the spam campaigns diluted their brand.¹⁷⁰ The Microsoft strategy built upon a nascent legal understanding emerging within the US Justice system and it leveraged the Chinese Justice system as well in order to block various IP addresses. Over the next several years, Microsoft executed a number of these take-down operations: Rustock, Kelihos, Zeus, Nitol, and Bamitol along with two subsequent operations, the Citadel and the ZeroAccess botnets collaboratively with the FBI.¹⁷¹ Before discussing the last two it is useful to understand the Rustock takedown from a community of practice point of view.

4.4.1 *Rustock*

In 2011 the Rustock botnet was responsible for sending an incredible amount of spam email, some 30 billion emails a day, and at various times in its operational life the network was responsible for over 50% of worldwide spam.¹⁷² Versions of the malware had been present since 2005 or 2006 and the botnet propagated and established itself by staying dormant for five days after infection making it harder to notice or track. Estimates of the botnet’s size range from

¹⁷⁰ Ibid., pp178-180

¹⁷¹ Ibid., p. 186

¹⁷² Lanstein, Alex and Julia Wolf *The Rustock Botnet Takedown: Operation B107* 2 Feb. 2015, www.youtube.com/watch?v=3laG_GxCuJ8.

850,000 to more than a two million infected computers.¹⁷³ On 16 March 2011 a coordinated effort between Microsoft, the US Marshall Service, FireEye, multiple state law enforcement, and several other entities executed Operation b107 aimed at taking the Rustock botnet offline. The legal standing for seizing Rustock's command and control servers and associated domains emanated from trademark infringement claims brought by Microsoft and Pfizer based on spam advertising of fake Viagra, a trademarked drug owned by Pfizer. Washington University and the Dutch High-Tech Crime Unit along with Chinese law enforcement all assisted in seizing equipment and blocking domains.¹⁷⁴

From a community of practice point of view, insights can be generated from a presentation given by Julia Wolf and Alex Lanstein at the Blackhat Security Conference in 2011. The duo spoke regarding their involvement with the effort. The talk was typical of such presentations which happen at many different conferences and workshops helping maintain information awareness amongst the community of practice. It is interesting to observe, they hold the Rustock takedown in contrast to a takedown which didn't work well, the Grum botnet. They pointed out, their effort to take down Grum failed due to the way the offense and defense evolve. An uncoordinated effort on the part of an individual at FireEye who attempted to stop the C&C infrastructure of Grum by imploring the upstream bandwidth provider for the malware's server provider (this is to say, the ISP's ISP so to speak) to block the C&C infrastructure.¹⁷⁵ This forced the Grum botnet controllers to adapt their methods and become far more sophisticated. This is an important point, not because of the technical nuances, but due to the inherent mistake being one of insufficient *social connection*

¹⁷³ Bright, Peter. "How Operation b107 Decapitated the Rustock Botnet." *Ars Technica*, 22 Mar. 2011, arstechnica.com/information-technology/2011/03/how-operation-b107-decapitated-the-rustock-botnet/.

¹⁷⁴ Bright (2011)

¹⁷⁵ Lanstein and Wolf, 2011. 3:58

to leverage resources across multiple communities...not just tier 2 and 3 ISPs, but also that of law enforcement, software providers, and security community elements allowing the adversary to regroup and evolve their strategy. Rustock, however, is presented as an example coordination with those constituencies to better perform a more successful takedown. The effort started when Microsoft went to FireEye and asked them for a recommendation on what malware that, if taken down, would provide the greatest benefit to their customers. Individuals within FireEye recommended the Rustock botnet. Microsoft, at this time, had a specific unit set up within the company whose mandate was to “bring the hurt” to the bad guys. Rustock was chosen because it was causing an “easily measurable harm.”¹⁷⁶ The presentation further points out, targets which are not easily measurable are not as desirable as potential takedowns. FireEye was engaged to provide an independent view apart from Microsoft’s during the takedown activities. Microsoft asked FireEye to file a legal “declaration of harm” against the Rustock botnet controllers (individuals that promulgated and controlled the botnet). However according to the FireEye employees, when the declaration was presented to a US Judge, the judge was confused and unsure of how to proceed or what was being asked of the court. The judge asked to be given a few weeks to re-read the declaration in order to understand, amongst other things, the relationship between the malicious actors and the third party servers from which they were operating.¹⁷⁷

This shows the complex nature of modern malware, in that often nefarious actors rent server space from legitimate vendors, thereby takedown operations must involve the seizing of and redirecting of data from physical hardware that is not owned by the bad actors directly, but may also host legitimate enterprises.¹⁷⁸ Relationships amongst the security community and various

¹⁷⁶ Ibid. 41:13

¹⁷⁷ Ibid.

¹⁷⁸ Ibid. 43:19

functional entities such as DNS providers is pointed out as being extremely beneficial. Lanstein says that by being friends with the DNS providers, they can provide technical information simply because “we asked” which is helpful.¹⁷⁹

Microsoft’s legal counsel was able to devise a new way to help show standing in US courts by employing provisions of the Lanham Act (parts not utilized in the earlier Waledac case) that allow a trademark holder to seize counterfeit goods that infringe upon their trademarks. By showing brand damage from spam marketing counterfeit drugs, companies like Pfizer, Microsoft and their partners successfully argued to sinkhole Internet traffic. Microsoft was also able to argue that the increased traffic brought about by spam had real world costs associated with the increased bandwidth they would have to support through their Hotmail email service, which was a major recipient of spam email. Temporary access was granted by both US courts and Dutch courts allowing Microsoft and their lawyers to access servers located in both countries in order to gain forensic evidence.¹⁸⁰ Contrasted against the experience of Grum, the Rustock botnet case was far more successful due to the multipronged approach, which stitched together Microsoft acting for the benefit of its brand and business interest, entities like FireEye that represented the now mature and professionalized security community, and judicial elements both in the US and abroad. Hiller surmises the importance of the Rustock takedown from a legal standpoint:

“...the Rustock case added legal specificity for court authority to order third parties to [do] botnet takedowns by purging IP addresses and domain names from the Internet, and preserving evidence. Furthermore, it established the Lanham Act as a viable vehicle for Microsoft to seize physical botnet property and increased the ability of Microsoft to pursue the eradication of botnets through the civil system.”¹⁸¹

¹⁷⁹ Ibid. 45:27

¹⁸⁰ Ibid. 45:58 – 49:44 and Hiller, 2014 pp 186-187

¹⁸¹ Hiller, 2014 p188

From the perspective of IR and Security studies, this represents a unique deputation of a private entity on behalf of the *State* acting in the interests of Internet users *worldwide*. The Rustock takedown is a useful milepost in the steady march of provisioning activities beginning at Morris Worm and evolving through Conficker before becoming institutionalized practice.

4.4.2 *Evolving Microsoft Strategy*

Subsequently, Microsoft began to execute takedown operations with a fair regularity. Later in 2011 they sued a limited liability company in the Czech Republic to cripple the Kelihos botnet. This was an interesting tactic as both defendants were outside of the US, but Microsoft was able to show standing in Virginia due to businesses being affected within that state.¹⁸² Microsoft further evolved their legal strategy in 2012 with the takedown of the Zeus malware. Microsoft utilized the Racketeer Influenced and Corrupt Organizations Act (RICO). The Zeus malware enabled this approach, as the malware stole banking credentials in furtherance of financial crime. By showing that the criminal enterprise was an interstate and international operation, which implicitly due the nature of the Internet it was, Microsoft successfully argued the defendant's actions were in furtherance of a criminal enterprise to move money across state and international lines.¹⁸³ Above, it was pointed out that during the Rustock takedown, a judge had displayed a relative lack of knowledge and comfort with the subject matter and implications of what was being presented to the court. However, during the Zeus takedown, the US government was closely involved, at an earlier stage and was a far more central instantiating actor. US courts issued findings and judgments, and the US Marshall Service was instrumental in seizing physical computing hardware

¹⁸² *Ibid.* pp. 189-190

¹⁸³ *Ibid.* p191

in wider fashion than during previous takedowns. The Financial Service ISAC (FS-ISAC) joined Microsoft as a plaintiff in the case.¹⁸⁴

It should be noted, the Kelihos take down was not entirely successful, which will be discussed in the next section below. These are all clear indicators that seams between public and private constituencies across the “cyber patchwork” were transitioning from major to minor as the practice of botnet takedowns had finally become routinized across many different collaborating entities including the law enforcement community. The next section will identify numerous security provisioning cases and consider them in aggregate alongside the reviewed provisioning activities in prior sections and chapters to generate observations and insights.

4.5 Take-down operations in Summary

So far this chapter has reviewed a number of various security provisioning activities summarizing some while robustly analyzing others. Table 4 below identifies distinct takedowns and security provisioning activities, representing varying degrees of collaboration amongst participants across the “cyber patchwork.” The dates indicate when the botnet/malware was first observed and the second date indicates when either there was an attempt to takedown the botnet or the last year that related law enforcement or other activity occurred. These could include judicial activity like indictments or sentencing. It includes many of the cases detailed in previous sections and chapters along with several other cases. The intent of the table isn’t to provide a detailed accounting of specifics related any one of the identified cases, but to present the fact such activities have occurred regularly over the past twelve years into the present. Each of the entries on the table represents a collection of primary, secondary, and tertiary material gathered in support

¹⁸⁴ Ibid. p193

of this dissertation. That material isn't presented exhaustively as both the specificity and quality of data collected varied greatly across all cases. However, a number of dynamics can be identified and will be discussed next.

Table 4: Summary of Takedown/Security Provisioning Activities

Botnet/Malware	Year Discovered	Takedown/Activity	Short Description
Zotob	2005	2006	Worm which took down CNN and other corporations worldwide. Moroccan virus writer sentenced in Morocco in 2006 ¹⁸⁵
Conficker	2008	2008	Botnet often presented as a canonical case study in networked security provisioning based on the activities of the Conficker Working Group ¹⁸⁶
McColo Srizbi	2007	2008	Takedown of large spam hosting service provider through private action of upstream providers. McColo servers hosted the Srizbi botnet, third party legitimate operations were also affected ¹⁸⁷
Storm	2007	2008	Large botnet that used a number of defensive techniques and one of the many which became commodity rented as a capability for criminal activity. The botnet was also notable as it became a "battleground" over which various factions fought for control. A team of German researchers attempted to disrupt the botnet's activities through a technique called "poisoning" which has ethical implications due to the act of changing/modifying information on victims' computers without explicit permission ¹⁸⁸
Mariposa	2008	2009	Botnet dismantled by the Mariposa Working Group led by Canadian firm Defence Intelligence. The effort was similar to the Conficker experience, even resulting in the identification, arrest, and prosecution of individuals behind the botnet in Spain and Slovenia. ¹⁸⁹
Mega-D	2008	2009	An operation in 2008 by both the US FTC and FBI along with agencies in New Zealand froze the financial assets of the operators of the Mega-D botnet, this preceded a FireEye takedown operation in 2009 which redirected C2 infrastructure in collaboration with the upstream ISP of the botnet ¹⁹⁰

¹⁸⁵ Richtel, Matt. "Virus Attacks Windows Computers at Companies." *The New York Times*, 17 Aug. 2005, www.nytimes.com/2005/08/17/technology/virus-attacks-windows-computers-at-companies.html. and BBC "Technology | Windows 2000 Worm Hits US Firms." *BBC News*, 17 Aug. 2005, news.bbc.co.uk/2/hi/technology/4159002.stm.

¹⁸⁶ Conficker Working Group (2011) and Mueller et al. (2013)

¹⁸⁷ Vijayan (2008)

¹⁸⁸ Hiller (2014)

¹⁸⁹ Sully and Thompson (2010)

¹⁹⁰ Stone, Brad. "Authorities Shut Down Major Spam Ring." *The New York Times*, 14 Oct. 2008, www.nytimes.com/2008/10/15/technology/internet/15spam.html.

Table 4 Continued			
Botnet/Malware	Year Discovered	Takedown/Activity	Short Description
Cutwail	2007	2010	Takedown involving UC Santa Barbara and Ruhr University Bochum ¹⁹¹
Waledac	2008	2010	One of the first of many Microsoft takedown operations. Microsoft was granted “ownership” of 277 domains that Waledac used in operation. ¹⁹²
Lethic	2008	2010	The company Neustar attempted a takedown of the Lethic botnet in 2010 though later that year the botnet’s originators (allegedly) were able to regain control of parts of the network. Neustar was able to convince the botnet’s ISP to redirect the C2 infrastructure which led to large and measurable decline in internet wide spam
DNSChanger	2006	2011	The DNS Changer Working Group (DCWG) created to help remediate via “Operation Ghost Click” included the FBI. An Estonian national was charged for its distribution ¹⁹³
Rustock	2006	2011	Botnet addressed as part of Microsoft campaign employed provisions of the Lanham act helping establish trademark-based seizing of physical servers for forensics ¹⁹⁴
Coreflood	2010	2011	In a 2011 operation, the FBI requested and was given permission by US Courts to delete Coreflood malware on infected computer if provided written consent from users of those computers. ¹⁹⁵
Nitol	2012	2012	Nitol was another takedown operation by Microsoft that led to unattended consequences. The dynamic DNS operator 3322.org was taken over by Microsoft in an effort to address the Nitol botnet which was using the service, Pen Yon 3322.org’s owner later settled with Microsoft over damages he claimed. ¹⁹⁶
Bredolab	2009	2012	Bredolab was dismantled by Dutch law enforcement and led to the arrest of an Armenian national who was sentenced in four years in jail in 2012 ¹⁹⁷

¹⁹¹ Stone-Gross, Brett, et al. "The Underground Economy of Spam: A Botmaster's Perspective of Coordinating Large-Scale Spam Campaigns." *LEET* 11 (2011): 4-4.

¹⁹² Hiller (2014)

¹⁹³ DCWG “DNS Changer Working Group” www.dcwg.org; FBI (2) “DNS Changer Malware.” <https://www.fbi.gov/DNS-changer-malware.pdf>; Zetter, Kim. “DNSChanger’ Malware Could Strand Thousands When Domains Go Dark on Monday.” *Wired*, Conde Nast, 3 June 2017, www.wired.com/2012/07/dns-changer-going-dark/.

¹⁹⁴ See Hiller (2014) and Lanstein et al. (2015)

¹⁹⁵ "US Government Takes over Coreflood Botnet." *Network Security* 2011.5 (2011): 1-2. Web.

¹⁹⁶ Leyden, John. “Chinese Nitol Botnet Host Back up after Microsoft Settles Lawsuit.” *The Register - Biting the Hand That Feeds IT*, The Register, 4 Oct. 2012, www.theregister.co.uk/2012/10/04/nitol_botnet_settlement/.

¹⁹⁷ “Russian Spam Mastermind Jailed for Creating Botnet.” *BBC News*, BBC, 24 May 2012, www.bbc.com/news/technology-18189987.

Table 4 Continued			
Botnet/Malware	Year Discovered	Takedown/Activity	Short Description
Grum	2009	2012	Partial success was found by FireEye in an operation to disable the Grum botnet, contact with the upstream ISP was not enough to disable the botnet due to a evolving sophistication of those who controlled it responding to FireEye's efforts. ¹⁹⁸
Citadel	2012	2013	Citadel is often thought of a derivative of the Zeus (original variant not the one referenced below) malware, its creator was a Russian National that was extradited from Norway to the US and prosecuted.
Bamital	2009	2013	Joint operation between Microsoft and Symantec (antivirus and security company). This temporarily broke some infected computers' ability to use some web search services. Technicians associated with the two companies "raided data centers" accompanied by US Marshals to pull servers offline. Bamital enabled "click fraud" in which search results were fraudulently manipulated to garner advertising income.
ZeroAccess	2011	2013	An operation led by Microsoft to dismantle the ZeroAccess botnet was seen, by some, as a failure due to the fact not all of the C&C infrastructure was taken offline
Simda	2010	2015	Microsoft partnered with INTERPOL, Kaspersky Lab, Trend Micro and Japan's Cyber Defense Institute to effect the Simda takedown. The operation also involved Dutch agencies, the FBI and law enforcement in Luxembourg and Russia ¹⁹⁹
Shylock	2011	2014	The European Cybercrime Centere (EC3) led a multinational effort with collaboration from the UK National Crime Agency, the FBI, the Netherlands, Turkey, Italy, Germany, Poland, and France. Shylock was named after pieces of its code that contained excerpts of Shakespeare. Shylock was also banking malware that steals credentials for financial fraud and abuse.
GameOver Zeus	2011	2014	GameOver Zeus was banking malware that stole credentials, the takedown was named "Operation Tovar" and involved the FBI, Europol, and the UK's National Crime Agency. In addition to these public entities, private firms were involved including: CrowdStrike, Dell SecureWorks, Symantec, Trend Micro and McAfee. Both the VU University Amsterdam and Saarland University in Germany were involved as well. The FBI also placed the malware's operator, Evgeniy Mikhailovich Bogachev on its "Most Wanted" list. ²⁰⁰

¹⁹⁸ See Lanstein et al. (2015)

¹⁹⁹ INTERPOL. "INTERPOL Coordinates Global Operation to Take down Simda Botnet." INTERPOL, 13 Apr. 2015, www.interpol.int/News-and-media/News/2015/N2015-038.

²⁰⁰ USDOJ "U.S. Leads Multi-National Action Against 'GameOver Zeus' Botnet and 'Cryptolocker' Ransomware, Charges Botnet Administrator." *The United States Department of Justice*, 16 Sept. 2014, www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware.

Table 4 Continued			
Botnet/Malware	Year Discovered	Takedown/Activity	Short Description
Blackshades	2012	2014	The FBI began operations in 2012 to arrests 24 hackers in eight countries and various operations carried on until 2014 when the FBI coordinated a worldwide effort which led to the arrest of nearly one hundred people in nineteen countries that were using Blackshades for cyber-crime. The software was available for sale through various “dark web” portals. ²⁰¹
Ramnit	2010	2015	Ramnit was dismantled by Europol and involved partner in Germany, Italy, the Netherlands and the UK along with Microsoft and Symantec
Dorkbot	2012	2015	Dorkbot was unique in that it spread through instant messaging and social networks by enticing victims to download a malicious zip file. The malware was subject to a takedown collaboration by Microsoft, ESET, Poland’s CERT, the FBI, DHS, INTERPOL, the RCMP, and the Canadian Radio-television and Telecommunications Commission (CRTC). Microsoft reportedly provided “telemetry” to law enforcement agencies around the world to assist in the effort. Newer versions of Dorkbot are reported to have resurfaced in 2018 used to steal banking credentials. ²⁰²
Kelihos	2010	2017	Kelihos represents a number of takedown attempts stretching from 2012 to 2017 of various variants. The operators of Kelihos were allegedly behind Waledac as well ²⁰³
Avalanche	2009	2017	Shadowserver along with European and International law enforcement executed this takedown operation. The Avalanche malware made use of a “fast-flux” hosting method that helped it defend against being dismantled. The operation was hailed as a new template for collaborative security involving private and public constituents. ²⁰⁴

²⁰¹ Kerr, Dara. *BlackShades Malware Bust Ends in Nearly 100 Arrests Worldwide*. CNET, 20 May 2014, www.cnet.com/news/blackshades-malware-takedown-ends-in-100-arrests-worldwide/.

²⁰² Brooks, Chris. “Microsoft, Law Enforcement Collaborate in Dorkbot Takedown.” *The First Stop for Security News | Threatpost*, Threatpost, 8 Dec. 2015, threatpost.com/microsoft-law-enforcement-collaborate-in-dorkbot-takedown/115589/.

²⁰³ USDOJ “Justice Department Announces Actions to Dismantle Kelihos Botnet.” United States Department of Justice, 28 June 2017, www.justice.gov/opa/pr/justice-department-announces-actions-dismantle-kelihos-botnet-0.

²⁰⁴ Shadowserver. “Avalanche Botnet.” Shadowserver. 4 December 2017. <https://avalanche.shadowserver.org/>

Table 4 Continued			
Botnet/Malware	Year Discovered	Takedown/Activity	Short Description
Dridex	2014	2016	Dridex was another botnet that specialized in harvesting banking credentials for engaging in financial crime. In 2016 the UK National Crime Agency working with the FBI arrested 14 individuals accused of using Dridex and variants to steal money. ²⁰⁵
Mirai	2016	2018	While Mirai was never subject to a “takedown” operation, the FBI did trace and question two individuals that ended up confessing to its creation, they avoided jail time by agreeing to robust cooperation with the government on cybercrime investigations. The botnet is considered the first “internet of things” malware and can be utilized for massive DDOS campaigns enabled through poorly secured Internet of Things (IoT) devices such as cameras, DVRs and other internet aware technology. Mirai also demonstrates that when ‘new’ threats emerge, individuals within the information security community embedded within the functional structure of the Internet are the first to become aware of the threat and begin problem solving. ²⁰⁶

When analyzing the breadth of data, it becomes apparent that simple observation of the emergence of a hitherto unseen botnet or piece of malware does not necessarily lead to an organized takedown with any immediacy. Often months to years can pass before an attempt is made by elements of the community of practice to take action and address a threat. As observed during the discussion of the Rustock botnet, this may be because certain targets are more desirable than others in terms of observable metrics and impact. Also, often elements of the community are engaging in information exchange, discussions, observations, and coordination to understand and decide if a threat should be addressed. In the case of Kehilos, the time gap on the table represents a series of failed take down events across successive versions of the malware in 2012 and again in

²⁰⁵Trendmicro. “FBI, Security Vendors Partner for DRIDEX Takedown.” *TrendLabs Security Intelligence Blog*, 14 Oct. 2015, blog.trendmicro.com/trendlabs-security-intelligence/us-law-enforcement-takedown-dridex-botnet/.

²⁰⁶ Burzstein, Elie. “Inside the infamous Mirai IoT Botnet: A Retrospective Analysis.” *CloudFlare Blog*. (14 Dec 2017). <https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/>

2013. Finally, in 2017 a joint operation between Shadowserver, the FBI, and a security company named CrowdStrike took over the peer to peer C2 infrastructure through redirection to sinkholes. This resulted in a “100%” takedown of the C2 infrastructure, and also included collaboration with Spanish authorities to arrest Pyotr Levahov, a Russian reported to be behind a massive empire of spam-based malware.²⁰⁷ Kehilos also helps show how variants of the same piece of malware and non-codified naming conventions may lead to confusion and repeated work across the provisioning patchwork.

In 2012 another security nonprofit named the HoneyPot Project attempted a sinkhole operation of the the Kehilos .B/Hux malware. They were joined by the private company actors, Dell SecureWorks, CrowdStrike, and Kaspersky. This is one of the “failed” attempts to disable Kehilos referenced above. However, if the information provided by HoneyNet regarding the effort on their website and, published contemporaneously with the 2012 effort, is to be believed the takedown was quite successful. That stands in contrast Shadowserver’s analysis and published after the 2017 takedown of subsequent Kehilos variants working with the FBI.²⁰⁸ Why? As an indication of practice, that question points to an inherent problem of networked provisioning mechanisms, often coordination does not breed standardization in terms of what success or failure consist of and in terms of distinguishing amongst malware, variants of that malware, and new or wholly different malware. An analysis of a small set of malware naming and identification across various industry entities/products by cybersecurity firm OPSWAT concluded “...we can infer that the naming conventions seem to lack consistency across different anti-malware vendors - there

²⁰⁷ Shadowserver (2) . “Kelihos.E.” <http://blog.shadowserver.org/2017/04/12/kelihos-e> and Reuters. “Russian computer programmer arrested in Spain: embassy.” *Reuters*. 9 April 2017. <https://www.reuters.com/article/us-spain-russia-idUSKBN17B002>

²⁰⁸ See Shadowserver, 2017 and HoneyNet, 2012

isn't even consistency in the inconsistency...”²⁰⁹ As early as 2012 analysts such as Dittrich identified the confusion surrounding naming as a factor that hinders greater collaboration and awareness.²¹⁰

The Kehilos experience preceded an effort by the HoneyNet Project to promote a “code of conduct” for takedown operations. As mentioned previously, these operations had sometimes existed in legal “gray space” when undertaken by private actors either without or with little public legal support and the involvement of law enforcement. Additionally, in 2007 the takedown of the McColo/Szrizbi servers proved that such operations can have unintended consequences. That takedown effort stemmed from journalistic sources providing information to the ISP which hosted the McColo Corporation’s webhosting services. The ISP made the decision to “pull the plug” which affected not only the bad actors using McColo’s services to send out spam and malware, but also legitimate users of the service.²¹¹ In another incident in 2008, German researchers attempted to disrupt the operations of the Storm botnet by using a technique called “poisoning,” which is an active technique of changing the destination of the botnet’s C2 requests and requires

²⁰⁹ Mo, Jianpeng. “What Can We Learn from Anti-Malware Naming Conventions?” *Cyber Security and Malware Protection*, OPSWAT, 5 Nov. 2015, www.opswat.com/blog/what-can-we-learn-anti-malware-naming-conventions.

²¹⁰ Dittrich (2012), p2

²¹¹ The saga of the McColo takedown is well worth exploring in further depth, the cybersecurity blogger and former Washington Post journalist, Brian Krebs, chronicles a great deal of the story in his 2014 book: Krebs, Brian. *Spam nation: The inside story of organized cybercrime-from global epidemic to your front door*. Sourcebooks, Inc., 2014. The reason Krebs’ work isn’t leaned on more heavily within this dissertation is the circular referencing that often puts Mr. Krebs at the center of the narrative while citing his own articles. That being said, Krebs himself is a useful indicator of practice, he has become a central nexus that helps spread awareness beyond the information security community of practice to the general public and remains well read amongst both practitioners and laymen alike. Often his blog articles lean on information he is able to cull from sources within the community of practice. See also, Vijayan, Jaikumar. “McColo Takedown: Internet Vigilantism or Online Neighborhood Watch?” *Computerworld*, Computerworld, 17 Nov. 2008, www.computerworld.com/article/2529316/malware-vulnerabilities/mccolo-takedown--internet-vigilantism-or-online-neighborhood-watch-.html.

making changes on victim's computer, which may occur without their permission or knowledge.²¹² The Honeynet Project's code of conduct was further supported by Shadowserver, they; based their code of conduct on a DHS effort that resulted in the *Menlo Report: Ethical Principles Guiding Information and Communication Technology Research*²¹³. The Menlo Report tried to offer a set of guiding principles on which to base ethical execution of research within the information sciences and computing fields. The report was used as the basis to then generate a code of conduct for takedown efforts within the information security community. The code of conduct's overall effect and penetration beyond discussion generated from its release in 2012 is debatable, however it offers a clear indication of practice and identifies an important seam that has been referenced throughout this work. That seam is between the academic/research community of practice and the security community of practice. In many cases that seam is obviously minor, in that the two communities overlap and often help enable security provisioning. In the case of the code of conduct, a specific individual can be identified as the (or, perhaps a) node connecting the two communities, that being Dave Dittrich whom is both an academic researcher and security practitioner as he is also part of the Honeynet Project non-profit.²¹⁴

In general, coordination efforts have increased in complexity and occupied longer timelines as various legal instruments, tactics and techniques have been developed, institutionalized and evolved.²¹⁵ As a general statement, reviewing the data and debates surrounding the presented

²¹² Broersma, Matthew. "Researchers 'Poison' Storm Botnet." *PCWorld*, 26 Apr. 2008, www.pcworld.com/article/145171/article.html.

²¹³ Dittrich, Dave and E. Kenneally, "The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research", Tech. rep., U.S. Department of Homeland Security, Aug 2012. https://www.caida.org/publications/papers/2012/menlo_report_actual_formatted/

²¹⁴ Dittrich and Kenneally, 2012 and Dittrich, Dave. "FAQ on Kelihos.B/Hlux.B sinkholing." The Honeynet Project. 2012. <https://www.honeynet.org/node/836>

²¹⁵ A similar conclusion regarding the time lag representing coordinative effort is reached by Dittrich (2012) p7

takedown/ provisioning activities seems to confirm the most successful efforts involve broad based constituencies and partnership between public and private entities and across international lines. This would make sense if thought about not as criminal activity confined to a technological space, but as criminal activity that has *people* at the root. Successful security provisioning across these cases involves technical solutions to interdict and shut down C2 of the malware and botnets, but it also requires that law enforcement arrest individuals and courts sanction and sentence those individuals to stop the issue at its root. The manner in which those various elements have mixed and the stage of the process in which various elements begin their involvement has changed. Generally, it can be stated that while public elements such a law enforcement have always been present, there is a general shift toward involving public constituencies earlier as the operations have matured and evolved to become more and more complex. Clear indicators of practice have emerged subsequent to the Conficker experience. Efforts such as the code of conduct that sought to codify behavior across the community is evidence of the evolving *practice* of takedowns. Clearly, agencies such as the US DOJ, and equivalents in countries such as the UK, the Netherlands, and many others have become ever more sophisticated and proactive within the area of takedowns as well. This is another clear indicator of an evolving community of practice that has grown to include constituencies outside of computational security professionals embedded within Internet relevant companies and academia.

In 2016 Shadowserver took part in a multinational effort to mitigate the Avalanche malware. Avalanche was not a botnet, but a “content delivery service” that allowed multiple botnets and malware to be controlled and sold for a number of criminal purposes. Members of Shadowserver worked as part of a technical subgroup within the collaborative effort to build an infrastructure to sinkhole traffic emanating from multiple malware families that utilized Avalanche

C&C functions over an 18 month period.²¹⁶ A blog entry on Shadowserver’s website described “a mammoth effort involving complex international coordination, with the final operational take down being conducted from Europol/EC3’s Headquarters over the 3 days.”²¹⁷ The operation affected more than 20 malware families operating in 30 countries and US states while impacting over 60 domain name registries worldwide. The blog entry specifies that the Avalanche takedown “required unprecedented levels of international partnership.”²¹⁸ Five individuals were arrested, 37 different premises were searched in a coordinated worldwide effort, 39 servers were seized while 221 were taken offline. IP addresses representing over 180 countries were reportedly victimized, and Shadowserver blocked or redirected over 800,000 domains falling within over 60 top level domains (.com, .biz, .us, etc.).²¹⁹ Comparing the Avalanche takedown to the Conficker takedown is useful, in that one can easily see the complexity that such operations have taken on, but at same time, basic elements of collaboration have remained surprisingly similar. Indications of practice include the sheer *scale* of coordination, which clearly incorporated multiple entities working transnationally, and unlike Conficker, substantial State support across a number of countries’ law enforcement and judicial elements. This is a clear substantiation of one of this dissertation’s central claims: Security provisioning related to large-scale problems on /for the Internet is carried out by a community of practice that has evolved through significant events and represents a unique culture of social practice.

²¹⁶ Shadowserver(3). “Avalanche.” Shadowserver. (2016)
<http://blog.shadowserver.org/2016/12/01/avalanche/> 2016

²¹⁷ Shadowserver (3), 2016

²¹⁸ Shadowserver (3), 2016

²¹⁹ See the statistics on the table posted on Shadowserver, 2016 Avalanche Blog Entry

CHAPTER 5. CONCLUSION

This dissertation began with an effort to help define the domain of analysis in a manner that could facilitate investigation from the perspective of IR Security Studies. The ICIRS model draws upon understandings of security as conceived by computing and information security disciplines that it combines with an understanding of levels of analysis drawn from IR theory. Using the ICIRS model as a heuristic, the foundational ideas of agency, structure, identity, and power across the modern information security space can all be systematically explored.

Chapter two of this dissertation establishes the idea that social practice characterizes the manner that networks of individuals and entities, organize collaborate, and coordinate to address large-scale security concerns on and for the Internet. These networks form within and around an information security community of practice that has arisen as consequence of the early Internet's structure and due to the social connections maintained amongst individuals and entities. In order to substantiate this claim, this dissertation reviews the historical context within which security provisioning on and for the Internet has evolved, bookended by two canonical cases, the Morris Worm incident and the Conficker botnet. It was shown that the types of collaboration enabled through early mailing lists helped establish a culture and mechanism of security provisioning that has remained remarkably similar through time. Early incidents made use of security aware individuals that had tremendous operational responsibility across the nascent and growing Internet. As time went on, the scale of threat, and the pace with which emergent threats spread increased, a community of practice evolved as a necessary response.

Chapter four led the reader through two separate types of security provisioning to help understand the modern provisioning environment that has grown complex due the Internet's explosive growth, the professionalization across the security community, and the proliferation of seams across the security patchwork. In the BGP routing case, evidence showed how network engineers embedded within the logical layer of the Internet maintain social connections to help recognize and remediate routing errors born of either mistake or malfeasance. The chapter then turned to an understanding of the post-Conficker world of botnet remediation. The Mariposa botnet shows how minor seams enable takedown operations and major seams, like that between Defence Intelligence and the RCMP can hinder collaboration. Additionally, chapter four discussed the relative frequency of takedown efforts across 12 years, and the evolution of various dynamics involved in the effort.

The reader was introduced to the Internet OPSEC community of practice, the organization ISOI provides an example of the closely knitted and highly vetted trust groups that have arisen around the issue of security substantiating a concept of identity amongst that constituency. The chapter ended by detailing the Avalanche takedown that involved public and private constituents coordinating and collaborating across 60 countries helping show the maturation of a community of practice that has evolved from adhoc problem solving on the nascent Internet since the Morris Worm and into an institutionalized and robust community. The following sections will offer some concluding thoughts considering the breadth of this dissertation.

5.1 Security as Practice *and* Power

In November 2014 Sony Pictures Entertainment (SPE) experienced a “wiper” attack that disrupted the company's operations and caused significant financial damage. The attack was

reportedly attributed to the DPRK, which was confirmed by the US Government when the Justice Department issued indictments of North Korean citizens for, amongst other things, the Sony incident.²²⁰ However, before the 2018 indictment, various non-governmental entities conducted their own investigations. One was Novetta Threat Research. On a website set up to distribute their report findings, the following appears.

“Operation Blockbuster was spearheaded by Novetta’s Threat Research and Interdiction Group (TRIG), working in close partnership with a group of trusted experts from cybersecurity, antivirus and malware protection, intelligence and research firms. The cross-industry partnership and the scope of the operation’s reach signify a new security role and posture for private industry. The Lazarus Group activity shows the cyber landscape has evolved. The Novetta-led team demonstrates industry can be a highly agile, capable and effective force in tracking and interdicting global cyber crime.”²²¹

The release of private reports such as the one detailing Operation Blockbuster help shape the larger public debates surrounding response and responsibility for incidents such as the hacking of SPE. They also provide insight into seams important to the analysis of such incidents. Outside of the public/private seam, identified above throughout several cases, there exists important seams within the private cybersecurity patchwork. Authors of Novetta’s report write, “Novetta believes that these efforts can help cause significant disruption and raise operating costs for adversaries...” and goes on to say, “It is our hope private industry will not only continue to illuminate various threat actors’ toolsets and operations, but also work with other industry partners and law enforcement agencies as able to affect positive change on the safe of network environments

²²⁰ DOJ. “North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions.” The United States Department of Justice, 6 Sept. 2018, www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

²²¹ Novetta. “Operation Blockbuster.” Novetta Threat Research & Interdiction Group, operationblockbuster.com/.

worldwide.”²²² The invocation of language that echoes traditional concepts of international deterrence and dissuasion (i.e. “raise the costs”) within the context of private actor investigation and mitigation of state sponsored cyber malware raises important questions of command, control, and communication not only across public/private seams, but also between private entities.

The authors of the Novetta report appropriately caveat their work as being valid only within the scope represented in the malware samples they have collected from public sources and private partners, but also forcefully argue that their attribution to North Korea as the perpetrator is correct and confirmed by the US Government’s own findings as evidenced by the indictments issues. Novetta’s work is a clear acknowledgement, on their part, that they believe as private actors, they possess a dimension of power to effect security change on/for the Internet. In fact, many of the cases studied within this dissertation, beginning with the Morris Worm through various botnet takedowns and BGP routing errors confirms that private actors embedded within the functional portions of the Internet’s structure are uniquely situated to recognize emergent threats. Microsoft’s leveraging of the legal system to seize control of domains proved, they too, believed they possess a dimension of power and sought to use it. Admittedly Microsoft has a sound business case for securing the Internet for its own products, but in doing so it is also acting as a de facto deputy on behalf of all Internet users.

Without a doubt, governments and law enforcement play a role as well, but just as *agency* within this space is described as distributed, so must *power* be thought of as spread across a larger constituency than IR Security theory has traditionally considered. One might observe, however, that as traversing the summary table of takedown operations in chapter four, there does seem to be

²²² Novetta (2017)

an increasing presence of law enforcement partners within the cohort of collaborators on any given provisioning activity. In fact, previous authors and analysts have asserted that hierarchies are being established over the previously networked nature of security provisioning present on the Internet.²²³ This dissertation doesn't deny that observation, but it does temper the idea that hierarchies are replacing networked provisioning or that hybrids of the two systems are becoming prevalent. Going back to the Morris Worm, government participation both through law enforcement action and judicial court proceedings have been a regular feature and outcome of many of these cases. Certainly, as evidenced by Conficker and several "gray space" botnet takedowns, exclusive private networked actor coordination is featured. But rather than making a sweeping statement that hierarchies are replacing networked provisioning, it is more accurate to speak of a *routinization* of the law enforcement and court proceedings woven into and coming after various types of provisioning activities. Botnet takedowns, particularly, seem to have found an institutionalized pattern of activity that begins with the security community of practice deciding that a specific piece of malware or botnet had become large and problematic enough to be addressed forming public/private partnerships to address the issue. Many times, these operations take months or even, as discussed in previous chapters, years to form, evolve, and then be executed.

5.1.1 *Its networks all the way down...*

The debate of networks vs hierarchies is at its heart, one of abstraction. However as the above alludes, the debate is perhaps less about a hard divide between the two and more about defining the terms of what consists of hierarchy and what is networked. Without a doubt, public agencies and national governments are becoming increasingly involved in phases of the Internet

²²³ Schmidt (2014) and Mueller et al. (2013)

security process, but instead of seeing this as a creeping hierarchy happening at the expense of once networked activity, it may be more useful to understand how public constituencies fit into the security provisioning network and cause rearrangement of the nodes and relationships while still remaining ‘networked’. Stated simply, its “networks all the way down.” It was noted earlier in this dissertation that networks are a metaphor *du jour*. This is especially true when analyzing social relations. The Internet security space is, perhaps surprisingly, no exception. This dissertation has shown that the Internet’s early structure has had lasting effects on the way security must be pursued, this is not just a technical or exclusively a technological issue. It’s a *social* one.

This has been true since the Morris Worm, an incident that was only recognized and remediated due to collaboration between individuals via electronic mail, phone, and in-person communication and information exchange to align goals and intentions while coming to common conceptions of what the problem was. This general process has been continually repeated again and again in the emergence of larger and faster spreading threats. Security within a space characterized as ‘networked’ ultimately involves social connection between increasingly specialized human actors which breeds a community of practice. That community is an important constituency that should factor into analysis of the space, in no small part, because their ability to recognize emerging threats and act first to remediate them, making them powerful within this evermore important segment of the modern world.

One insight that can be highlighted from this dissertation is the importance in recognizing that each node within a provisioning network is embedded within a context of its own. Individuals may be part of a “provisioning network” but they are also embedded within other networks, whether it is the company they work for or groups they associate with. Those connections matter for their ability to participate within the networked provisioning that may be instantiated around

any given problem as it arises. Put another way, members of the CWG represented a network passing information and coordinating with each other, but their ability to be useful is derived from the context they are already embedded within. While botnets, as a threat vector, have now become a routine target of law enforcement and international collaboration, the unforeseen, advanced, and wholly new threat, when it debuts, will first be recognized by elements of the Internet's security focused community of practice.

5.2 Lessons for Policy Makers

Communities of practice literature originated, partially, to understand living curriculum environments in which apprentices learned their trade. The *practice* of such trades encompasses much more than rote knowledge, and includes subtle worldviews and understanding of how to access resources and participate as a member of a community. Similarly, the community of practice arising around the need to recognize and remediate threats on/for the Internet represents a pool of specialized knowledge, talent, and resources drawn from individuals and entities embedded within functional pieces of the Internet's structure. This includes the functional pieces encompassed within the logical layer of the ICIRS model, and increasingly, within specialized security focused companies like Novetta and nonprofit entities like Shadowserver, ISOI, and many others. Pockets of that community are also represented within large companies like Microsoft and Cisco, each with their own business reasons necessitating a functional and stable Internet.

Security, once an afterthought, now represents a central concern, which in and of itself should come as no surprise. However, what is the proper role of the State? Are there trade-offs in allowing networked methods to be replaced with centralized hierarchies directed by State institutions? On one hand, the history of takedowns shows an agile problem-solving culture that

comes up with solutions to spreading criminal activity such as researchers developing “sinkholing” techniques, but on the other hand bereft of strong law enforcement and judicial action, those attempts proved less effective in the long term and carried with them unintended consequences. Consider, for example, the McColo, Grum, and Bamital takedowns. When broad constituencies were built around the operations, better success was had. The lesson for policy makers is that the security community of practice needs to be engaged early in the threat recognition phase in order to incorporate their agile problem-solving against emergent threats into established legal understandings *in situ*, not after the fact. The community of practice acts as “sensors” embedded within the Internet that can recognize threats as they emerge, often they too are “first movers” helping initiate security provisioning activities that can often become templates for future activity.

Previous analysis that identified a central tension between secrecy and openness within the security community is correct.²²⁴ This tension is obvious when researching close knit trust groups like ISOI and others that operate, in part, utilizing Ops-Trust among other ways of collaboration and coordination such as conferences. On one hand, the community has an innate need for security but the networked nature of security provisioning across the community benefits from open coordination, collaboration, and information exchange. This is an issue across all levels of analysis within the ICIRS model, information sharing is often discussed as ideal, but hindered by the economic disincentives (in terms of stock share price, reputational harm, and legal recourse of victims affected) guaranteed by open disclosure of security breaches. Participants at ISOI explained when asked, the various companies and institutions they represented have misgivings about the frank and open dialogue taking place at ISOI conferences. Some theorized if their upper management knew the extent of the information exchange that they engage in across the vetted

²²⁴ Schmidt (2014)

and trusted community, their upper management would be furious.²²⁵ Those same individuals are, adamant that such interaction is wholly necessary for them to be effective in their security focused positions.²²⁶ For policymakers, this presents a unique institutional design problem, one that encompasses questions of political economy, public interest, legal liability among various other dimensions — as well as security.

Some direction can be taken from the community of practice perspective, which points to the fact that information sharing in and of itself won't necessarily lead to the formation of robust and functional remediation mechanisms. Communities of practice are born of shared experience that forces coordination through problem solving. Thereby, top down mandates to share information may fall flat if those efforts aren't augmented by opportunities for practitioners to interface and build working multi-dimensional relationships such those engendered by FIRST, ISOI, and other institutions. The BGP routing case alludes to this issue, which highlighted the fact that maintaining personal connections across the industry is an important way to remediate problems. Multiple cases of botnet and malware remediation highlighted within this work show how *individuals* reached out through various mechanisms to coordinate and collaborate with others within what was once a burgeoning but is now a robust community of security practitioners. Additionally, history of botnet takedowns highlights the way formal state mechanisms need time to evolve in response to emerging areas of threats. How does law enforcement learn about a new threat? How do entities like the FBI go from being a reactive element engaged later in the process of remediation (not involved in great measure with Conficker during the CWG's most active

²²⁵ Author interview

²²⁶ These observations are synthesized from author interviews and collected information across the breadth of conversations, conferences, and professional engagements undertaken for this dissertation.

phases) to being a proactive investigatory entity directing takedown activities (Avalanche, Khelios, GameOver Zeus, etc.) and being involved in all phases of the process? The answer is that the practice of takedowns had to be socialized and elements of the Internet's security community of practice had to first interact with, and become embedded within, entities such as the FBI. That process happens bit by bit as that community itself grapples with understanding, problematizing, and responding to the evolving threat-scape.

Within this work, when two constituencies come into contact and must exchange information for the purpose of coordination and cooperation, the interface is deemed a "seam". From the perspective of policy makers and regarding the fostering of a community of practice, *seams matter*. While only two types of seams are identified within this work, minor or major, the former that enables action and the latter that inhibits it, seams themselves are dynamic and help identify an important facet/mechanism for consideration by policymakers. How should connections between groups be architected in order to reap the benefits of a minor seam arrangement and mitigate against the detriments of a major seam arrangement? Both the Conficker and Mariposa cases show how the ad-hoc nature of coordination in place since the days of Morris Worm has matured into the establishment of formalized "Working Groups" stood up around a specific threat or problem, in both cases membership largely followed from prior relationships amongst participants. Similarly, as both scale and pace of future threats increase, such working groups will need to be stood up around wholly different problems that may go far beyond botnets in terms of impact.

While numerous efforts across the ICIRS levels of analysis have manifested to address coordination, cooperation, and information sharing, the evidence presented seems to indicate relationships must be instantiated and developed prior to an event in order to be the most effective.

As such, there may be utility in national level exercises that mobilize a larger segment of public, private, and academic resources than current initiatives that often take place within narrow industry and trade segments (Energy, Banking, etc.) among public and/or private constituencies. Doing so may help establish working relationships necessary for best navigating seams and reducing major ones to minor ones.

5.3 Future Work

The lens of practice has further potential to help IR theorists interrogate and make sense of the unique mixture of structure and agency presented by the Internet as a conceptual space. Describing what “cyberspace” consists is problematic for IR security scholars. The ICIRS model combined with the lens of practice shows a way out of the morass, allowing for a more systematic exploration that integrates an understanding of information security with levels of analysis meant to segment analysis of social dynamics. This holds promise for further exploration of the space using social science theories and methodologies at each level of analysis. There are several areas that this dissertation did not address, but should be pursued in future work. The first is, clearly, that transnational provisioning of security by the information security community of practice needs to be explored from the perspective of political economy.

Internet Security is a tremendous growth field and industry. The economic dimension is required to think about the practice of security. The discussion in chapter four of the Rustock takedown hints at various implications of this. On one hand, the threat itself often has economic incentives that explain criminal pursuit of such activities. Spam email that advertises any number of products, many of which are fraudulent or illicit, is a canonical example. Indeed, as mentioned in chapter three, spam led to the monetization of Internet worms, viruses, and eventually botnets,

giving rise to a large criminal enterprise. But on the defensive side of the equation, money plays a role as well. Companies like FireEye exist to market their security solutions, and as evidenced by their own employees' presentation, they may pick targets based on how easily they can measure the outcome and on visibility of their work. That means there are economic incentives and disincentives for companies like FireEye when deciding which targets to pursue and when.

More work needs to be done to integrate analysis of international security provisioning on/for the Internet through the lens of political economy as conceived by IR scholars. Not only at the firm level, but at the State level of analysis. Take for example the case of *allofmp3.com*. In 2006, the US based part of its protest over Russia's desire to join the WTO on the continued operation of *allofmp3.com* from Russian servers.²²⁷ The website sold illegal copies of music, including many songs and whole albums with copyrights held in the US, for cut-rate prices far below market value and without paid royalties to content creators. The dispute may have forced Russia to pass newer copyright protections that forced *allofmp3* to shut down, likely as a condition to their accession into the WTO. While that anecdote is centered on intellectual property rights, it highlights the centrality of the Internet within global commerce and its importance at the highest levels of State to State economic diplomacy. Similarly, issues of security will become increasingly tied to the political economy of international machinations.

Currently, the US and China are locked in a standoff centered on the Chinese company Huawei's access to American and Western markets for their enterprise level switching equipment and next generation cellular technology. The US contends Huawei is an instrument of China's

²²⁷ Reuters. "U.S. Pushes Russia in WTO Talks to Close MP3 Site." *CNET*, 4 Nov. 2006, www.cnet.com/news/u-s-pushes-russia-in-wto-talks-to-close-mp3-site/; and Doorn, Jerooen. "US and Russia Strike Deal to Close AllofMP3.Com Site." *Computerworld*, 30 Nov. 2006, www.computerworld.com.au/article/169238/us_russia_strike_deal_close_allofmp3_com_site/.

military and intelligence apparatus and as such cannot be trusted to provide foundational Internet infrastructure to the US government, their allies, and important adjacent defense industries.²²⁸ While that is, in and of itself, worthy of study, the question for the subject matter of this dissertation is how such high-level debates affect the transnational peer groups such as those among network engineers and information security professionals that traditionally have to coordinate in the face of largescale threats? Multiple cases detailed above highlight coordination by US private and public actors and China's domain name registrar to redirect illicit traffic toward sinkholes crippling the C&C infrastructure of malware and botnets. Can such coordination survive antagonistic relationships mediated through not only State actors, firms such as Cisco (a US based Huawei competitor), Huawei itself, academic, and private members of the cybersecurity patchwork along with market derived incentives and disincentives? Answering those questions necessitates bringing the theoretical lens of political economy and associated methodologies to bear on the Internet security provisioning space.

5.4 Complex Things Fail in Complex Ways

The Internet is a system of systems. It is a complex architecture inexorably entwined with social systems, creating a sum of parts that is complicated. The thing about complex systems is—they can fail in complex ways. The Internet isn't the first complex system of connectivity built by humankind that diffuses knowledge and ideas, spreads commerce and creates wealth, all while ushering in new risks. Take, for example, the largest contiguous land empire in human history, the Mongol Empire. At its largest, the Mongol Empire encompassed approximately 9,300,000 square miles stretching from Eastern Europe to the Sea of Japan while also encompassing parts of

²²⁸ Chan, Kelvin. "As US Pushes to Ban Huawei, UK Considers Softer Approach." *AP News*, Associated Press, 21 Feb. 2019, www.apnews.com/f373e15671884f35bbe085a131c59262.

Siberia, the Middle East, and southward into the Indian subcontinent. The Empire became the administrative authority securing trade connections between the Western and the Eastern World.

The period subsequent to Genghis Khan's death, but before the Empire began its decline, is known as *Pax Mongolica*. The known world was surprisingly interconnected and economically interdependent.²²⁹ The Mongol method of rule was pragmatic and often took local culture and tradition seriously striving to adapt to local conditions, albeit initial rule was established through military conquest. The Mongols reined in corruption, controlled bribes and lawlessness, which allowed trade and business to flourish. This system of trade routes called the Silk Road, was like the Internet, a complex system of interconnection. News could spread wider and faster than ever before and the Empire was administered due, in no small part, to the system of garrisons the Mongols created. An insatiable appetite to continuously grow the Empire meant the Horde was always riding, bringing with them technologies absorbed through conquest, new ideas, spices, cultural goods –and even disease. Even after Genghis Khan's death, the Mongol empire grew, and though his descendants eventually split the Empire into four administrative regions controlled by separate Khans –all descendants of the Great Khan himself through his sons- the Empire thrived due to this interconnected system of systems.²³⁰

²²⁹ This view is synthesized from Weatherford, Jack. *Genghis Khan and the Making of the Modern World*. Three Rivers Press, 2012. See, especially, pp. 241 -265 regarding the decline of the Mongol Empire, Weatherford doesn't use the term *Pax Mongolica*, but other academics do although there are debates regarding how to bound the period and what the defining characteristics of it are. See for example: Tabak, Faruk. "Ars Longa, Vita Brevis? A Geohistorical Perspective on Pax Mongolica." *Review (Fernand Braudel Center)* (1996): 23-48. And Di Cosmo, Nicola. "Black Sea emporia and the Mongol empire: A reassessment of the pax mongolica." *Journal of the Economic and Social History of the Orient* 53.1-2 (2009): 83-108.

²³⁰ This also is, essentially, the view laid by Weatherford (2012), though the characterization of the Silk Road as a "system of systems" is an interpretation of the history and context presented by Weatherford by this dissertation's author.

The Mongol Empire did not, however, last into perpetuity. Infighting and competing spheres of power helped weaken the Empire's cohesiveness, but beyond that and according to modern historians, there was another reason the Empire was lost to time: The Black Plague. The Plague originated in central Asia and spread via the fleas present on the backs of rats on ships, horses, and camels as they moved through the Empire and beyond. Like the evolving computer-based viruses of modernity, the Plague was ever faster spreading and unstoppable.²³¹ Regions of the world were decimated. But why did the Plague contribute to the decline of the Mongol Empire? The answer lies with how locales responded. It varied across regions, but local laws began to regulate all manner of activity thought to contribute to the spread of the disease. Whole ethnicities faced condemnation and death, not due to the plague, but due to panic that they were responsible for the plague due their affiliation with trade. Jewish peoples were put to death in various parts of the world including Italy and other European countries, Muslims were killed as it was thought they brought the plague with them from the East. Laws were enacted to ban the importation of cloth thought to carry the plague, outlaw the trade of meat not due to any understood direct connection, but because it was associated with "smell of death".²³² According to some sources, whole houses were condemned to be burned with the occupants inside once plague was identified. If a foreign visitor fell ill, those they visited might be burned to death in order to stop the disease from spreading despite no symptoms being identified amongst the incidentally condemned. The result of these local responses was for parts of the Empire to turn inward. The plague response cut off communication, shut down trade, and halted the cultural diffusion through travel all of which characterized *Pax Mongolica*. The secondary and tertiary effects of plague induced madness were

²³¹ Ibid. pp. 242-246

²³² Ibid. p244

overwhelming. The great system of systems known as the Silk Road faltered and could not recover.²³³ The *response* to the black plague helped doom the Mongol Empire. Local responses to systemic problems can generate negative systemic effects, especially in the absence of coordination amongst localities. Threat recognition and threat response is important within a complex system of systems. Complex things fail in complex ways.

This dissertation, similarly, seeks to understand the manner that large-scale threats are recognized and remediated on and for another system of systems, the Internet. The application of the ICIRS model helps understand the issue of security as it intersects with various levels of social order across the systems that underlie the Internet and allows it to function, bounding the concept and helping clarify the confusing terminology of cybersecurity. Further, this dissertation shows that a community of practice has arisen due to the way the Internet was initially structured, and that community has grown robust as security has become professionalized and seams have multiplied as the Internet has grown. As new threats have emerged, ever larger in scale and ever faster in propagation, the community of practice has engaged in the process of threat recognition and problem-solving. That community will become ever more central in maintaining the Internet's stability and is thereby a powerful constituency deserving of study and explication.

²³³ Weatherford (2012) bases his account on several other works concerning the Black Plague, his chapter ten endnotes on p284 are useful for placing his interpretation into context

REFERENCES

- Adler, Emanuel, and Patricia Greve. "When security community meets balance of power: overlapping regional mechanisms of security governance." *Review of international studies* 35.S1 (2009): 59-84.
- Adler, Emanuel. "The spread of security communities: communities of practice, self-restraint, and NATO's Post—Cold War Transformation." *European journal of international relations* 14.2 (2008): 195-230.
- Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2016* issued by the US Office of the Secretary of Defense available at: <https://www.defense.gov>
- Anonymous. "(TCP-IP Distribution List for November 1988)." *Comp.protocols.tcp-ip*. 3 November 1988. Mailing List. <http://securitydigest.org/tcp-ip/archive/1988/11>
- AP Archived Data 2016 Summary Report available at: <https://research.collegeboard.org/programs/ap/data/archived/ap-2016>
- Bacq, Sophie, et al. "Bricolage in social entrepreneurship: How creative resource mobilization fosters greater social impact." *The International Journal of Entrepreneurship and Innovation* 16.4 (2015): 283-289.
- Baker, Ted, and Reed E. Nelson. "Creating something from nothing: Resource construction through entrepreneurial bricolage." *Administrative science quarterly* 50.3 (2005): 329-366.
- Baskerville, Richard, Paolo Spagnoletti, and Jongwoo Kim. "Incident-centered information security: Managing a strategic balance between prevention and response." *Information & management* 51.1 (2014): 138-151.
- Bauer, Johannes M., and Michel JG Van Eeten. "Cybersecurity: Stakeholder incentives, externalities, and policy options." *Telecommunications Policy* 33.10 (2009): 706-719.
- BBC "Technology: Windows 2000 Worm Hits US Firms." *BBC News*, 17 Aug. 2005, news.bbc.co.uk/2/hi/technology/4159002.stm.
- Benkler, Yochai. *The wealth of networks: How social production transforms markets and freedom*. Yale University Press, 2006.
- Bijker, Wiebe E., et al. *The social construction of technological systems: New directions in the sociology and history of technology*. MIT press, 2012.

- Bowden, Mark. *Worm: The first digital world war*. Grove/Atlantic, Inc., 2011.
- Bradner, Scott. "Key words for use in RFCs to Indicate Requirement Levels." Internet Engineering Task Force (IETF). 1997. <https://tools.ietf.org/html/rfc2119>
- Brand, Russell. "CERT" Message to phage. 12 February 1988. Mailing List. <http://securitydigest.org/phage/archive/320>
- Bright, Peter. "How Operation b107 Decapitated the Rustock Botnet." *Ars Technica*, 22 Mar. 2011, arstechnica.com/information-technology/2011/03/how-operation-b107-decapitated-the-rustock-botnet/.
- Brown, John Seely, and Paul Duguid. "Organizational learning and communities-of-practice: Toward a unified view of working, learning, and innovation." *Organization science* 2.1 (1991): 40-57.
- Buchanan, David A., et al. "Nobody in charge: Distributed change agency in healthcare." *Human Relations* 60.7 (2007): 1065-1090.
- Butler, Alan. "When cyberweapons end up on private networks: third amendment implications for cybersecurity policy." *American University Law Review* 62 (2013): 1203.
- CAIDA "A Historical View of the AS Core." CAIDA. https://www.caida.org/research/topology/as_core_network/historical.xml
- Cavelty, Myriam Dunn. "Cybersecurity Research Meets Science and Technology Studies." *Politics and Governance* 6.2 (2018): 22-30.
- Cavusoglu, Huseyin, Birendra Mishra, and Srinivasan Raghunathan. "The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers." *International Journal of Electronic Commerce* 9.1 (2004): 70-104.
- CCDOE. <https://ccdcoe.org/cyber-security-strategy-documents.html>; and specific strategic documents such as the 2015 National Security Strategy of the US available at <http://nssarchive.us/wp-content/uploads/2015/02/2015.pdf>.
- Cercine, John and Michael Salomone. *A Theory of Organizational Seams*. Unpublished Manuscript, 1991
- Choucri, Nazli, and David D. Clark. "Integrating cyberspace and international relations: The co-evolution dilemma." (2012), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2178586
- Choucri, Nazli, Stuart Madnick, and Jeremy Ferwerda. "Institutions for cyber security: International responses and global imperatives." *Information Technology for Development*.20.2 (2014): 96-121.
- Cluley, Graham. "Memories of the Love Bug Worm." *Naked Security*, Sophos, 4 May 2012, nakedsecurity.sophos.com/2009/05/04/memories-love-bug-worm/.

- Cluley, Graham. "Memories of the Melissa Virus." *Naked Security*, Sophos, 10 Nov. 2013, nakedsecurity.sophos.com/2009/03/26/memories-melissa-virus/
- Conficker Working Group. "Conficker working group: Lessons learned." *Conficker-Working-Group-Lessons-Learned-17-June-2010-final. pdf*, published Jan (2011), p17
- Cyert, R, March, J. *A Behavioral Theory of the Firm*. Wiley-Blackwell, 1963
- Czosseck, Christian, and Karlis Podins. "An Usage-Centric Botnet Taxonomy." *European Conference on Information Warfare and Security*. Academic Conferences International Limited, 2011.
- DCWG "DNS Changer Working Group" www.dcwg.org
- DDN MGT. "DDN MGT Bulletin #43." Phage. 3 November 1988. Mailing List. <http://securitydigest.org/phage/archive/383>
- De Graaf, Daan F., Ahmed F. Shosha, and Pavel Gladyshev. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST 114* (2013): 302-13
- Degenne, Alain, and Michel Forsé. *Introducing social networks*. Sage, 1999.
- DeNardis, Laura. *The global war for internet governance*. Yale University Press, 2014.
- Di Cosmo, Nicola. "Black Sea emporia and the Mongol empire: A reassessment of the pax mongolica." *Journal of the Economic and Social History of the Orient* 53.1-2 (2009): 83-108.
- Dittrich, David. "So You Want to Take Over a Botnet..." *Presented as part of the 5th USENIX Workshop on Large-Scale Exploits and Emergent Threats*. 2012.
- DOJ. "Creator of Melissa Computer Virus Sentenced to 20 Months in Federal Prison." *FBI Press Releases*, The United States Department of Justice, 1 May 2002
- DOJ (2) "Justice Department Announces Court Authorized Efforts Map and Disrupt Botnet." US Department of Justice. <https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-efforts-map-and-disrupt-botnet-used-north>
- DOJ (3). "North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions." The United States Department of Justice, 6 Sept. 2018, www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.
- Eckert, Penelope. "Communities of practice." *Encyclopedia of language and linguistics* 2 (2006): 683-685.
- Eeten, Michel van, et al. "The role of internet service providers in botnet mitigation an empirical analysis based on spam data." OECD Working Paper, 2010

- Eeten, Michel van "Patching Security Governance: an Empirical View of Emergent Governance Mechanisms for Cybersecurity." *Digital Policy, Regulation and Governance*, 19.6 (201): 429-448.
- ENISA. <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing>
- Feldman, Martha and Wanda Orlinkowski "Theorizing Practice and Practicing Theory." *Organization Science* 22.5 (2011): 1240-253
- FBI "Catching a Cyber Saboteur.", FBI, 19 Sept. 2005, archives.fbi.gov/archives/news/stories/2005/september/global_partner091905.
- FBI (2) "DNS Changer Malware." <https://www.fbi.gov/DNS-changer-malware.pdf>
- FIRST "Traffic Light Protocol (TLP)." <https://first.org/tlp>
- FIRST. "Traffic Light Protocol (TLP-SIG)." <https://www.first.org/global/sigs/tlp/>
- Fox, Stephen. "Communities Of Practice, Foucault And Actor-Network Theory." *Journal of management studies* 37.6 (2000): 853-868.
- Freeman, Richard. "Epistemological bricolage: How practitioners make sense of learning." *Administration & society* 39.4 (2007): 476-496.
- Frickel, Scott, and Kelly Moore, eds. *The new political sociology of science: Institutions, networks, and power*. Univ of Wisconsin Press, 2006.
- Friedrichs, Jörg, and Friedrich Kratochwil. "On acting and knowing: how pragmatism can advance international relations research and methodology." *International Organization* 63.04 (2009): 701-731.
- Garud, Raghu, and Peter Karnøe. "Bricolage versus breakthrough: distributed and embedded agency in technology entrepreneurship." *Research policy* 32.2 (2003): 277-300.
- Geigner, T. "If Most Crime Involves A 'Cyber' Element, Can't We Just Call It Crime Instead Of Cybercrime?" *Techdirt.*, 5 Mar. 2013, www.techdirt.com/articles/20130304/06541422191/if-most-crime-involves-cyber-element-cant-we-just-call-it-crime-instead-cybercrime.shtml
- Gerspacher, Nadia, and Benoît Dupont. "The nodal structure of international police cooperation: An exploration of transnational security networks." *Global Governance: A Review of Multilateralism and International Organizations* 13.3 (2007): 347-364.
- Giere, Ronald N. "The problem of agency in scientific distributed cognitive systems." *Journal of Cognition and Culture* 4.3 (2004): 759-774.
- Haftendorn, Helga. "The security puzzle: theory-building and discipline-building in international security." *International studies quarterly* 35.1 (1991): 3-17.
- Hand, V. "Operationalizing Culture and Identity in Ways to Capture the Negotiation of Participation across Communities." *Human Development*, 49.1 (2006) 36.

- Hansen, Lene, and Helen Nissenbaum. "Digital disaster, cyber security, and the Copenhagen School." *International Studies Quarterly* 53.4 (2009): 1155-1175.
- Healey, Jason, ed. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. The Atlantic Council, 2013.
- Héritier, Adrienne, and Sandra Eckert. "New modes of governance in the shadow of hierarchy: self-regulation by industry in Europe." *Journal of Public Policy* 28.01 (2008): 113-138.
- Hiller, Janine S. "Civil cyber conflict: Microsoft, cybercrime, and botnets." *Santa Clara Computer & High Tech. LJ* 31 (2014): 163.
- Hofmann, Stephanie C. "Overlapping institutions in the realm of international security: The case of NATO and ESDP." *Perspectives on politics* 7.1 (2009): 45-52.
- Hosmer, Larue Tone. "Trust: The connecting link between organizational theory and philosophical ethics." *Academy of management Review* 20.2 (1995): 379-403.
- IBM "Michelangelo Madness" IBM Research Report. 1992.
<https://web.archive.org/web/20080309235614/http://www.research.ibm.com/antivirus/SciPapers/White/VB95/vb95.distrib-node7.html>
- Jackson, Jonathan, Nick Allum, and George Gaskell. *Perceptions of risk in cyberspace*. Edward Elgar, 2005.
- Johnson, Eric S. "Re: initial portion of virus and how to catch the rest." Phage. 4 November 1998. Mailing List. <http://securitydigest.org/phage/archive/033>
- Jones, Candace, William S. Hesterly, and Stephen P. Borgatti. "A general theory of network governance: Exchange conditions and social mechanisms." *Academy of management review*. 22.4 (1997): 911-945.
- Kahler, Miles, ed. *Networked politics: agency, power, and governance*. Cornell University Press, 2015.
- Kerr, Dara. *BlackShades Malware Bust Ends in Nearly 100 Arrests Worldwide*. CNET, 20 May 2014, www.cnet.com/news/blackshades-malware-takedown-ends-in-100-arrests-worldwide/.
- Kirk, Jeremy. "Google Services Disrupted by Routing Error." *CSO Online*, IDG News Services, 13 Mar. 2015, www.csoonline.com/article/2896395/network-security/google-services-disrupted-by-routing-error.html.
- Kotulic, Andrew G., and Jan Guynes Clark. "Why there aren't more information security research studies." *Information & Management* 41.5 (2004): 597-607.
- Kubicek, Herbert, Robin Williams, and William H. Dutton. *The social shaping of information superhighways: European and American roads to the information society*. St. Martin's Press, Inc., 1997.

- Kuerbis, Brenden and Farzaneh Badiei "Mapping the cybersecurity institutional landscape." *Digital Policy, Regulation, and Governance*. 19, no. 6, 2017, pp. 429–448
- Lanstein, Alex and Julia Wolf *The Rustock Botnet Takedown: Operation B107* 2 Feb. 2015, www.youtube.com/watch?v=3laG_GxCuJ8.
- Libicki, Martin C. "Why Cyber War Will Not and Should Not Have Its Grand Strategist." 8.1 (2014): 23-39..
- Litchfield, David. "The Inside Story of SQL Slammer." *Threatpost*, 20 Oct. 2010, 14:30, threatpost.com/inside-story-sql-slammer-102010/74589/.
- Litfin, Karen T. "The status of the statistical state: Satellites and the diffusion of epistemic sovereignty 1." *Global Society: Journal of Interdisciplinary International Relations* 13.1 (1999): 95-116.
- LoVerso, John Robert. "source of the worm." Phage. 4 November 1998. Mailing List. <http://securitydigest.org/phage/archive/030>
- Leyden, John. "Chinese Nitel Botnet Host Back up after Microsoft Settles Lawsuit." *The Register - Biting the Hand That Feeds IT*, The Register, 4 Oct. 2012, www.theregister.co.uk/2012/10/04/nitel_botnet_settlement/.
- MacKenzie, Donald, and Judy Wajcman. *The social shaping of technology*. Open University Press, 1999.
- Mamakos, Louis A. "initial portion of virus and how to catch the rest." Phage. 4 November 1998. Mailing List. <http://securitydigest.org/phage/archive/029>
- Markoff, John. "Digital Fingerprints Leave Clues to Creator of Internet Virus." *The New York Times*, 30 Mar. 1999, p. A00017, www.nytimes.com/1999/03/30/us/digital-fingerprints-leave-clues-to-creator-of-internet-virus.html.
- Mathew, Ashwin Jacob. "Where in the World Is the Internet? Locating Political Power in Internet Infrastructure." (2014): 274
- Mathew, Ashwin & Cheshire, Coye. (2018). A Fragmented Whole: Cooperation and Learning in the Practice of Information Security. <https://www.ischool.berkeley.edu/research/publications/2018/fragmented-whole-cooperation-and-learning-practice-information-security>
- Mayer, Maximilian, Mariana Carpes, and Ruth Knoblich. "A Toolbox for Studying the Global Politics of Science and Technology." *The Global Politics of Science and Technology-Vol. 2*. Springer Berlin Heidelberg, 2014. 1-17.
- McElhaney, Lyle. "Security Mail List, #1." Unix Security Mailing List. 18 December 1984. Mailing List. <http://securitydigest.org/unix/archive/001>

- Mérand, Frédéric, Stéphanie C. Hofmann, and Bastien Irondelle. "Governance and state power: a network analysis of European security." *JCMS: Journal of Common Market Studies* 49.1 (2011): 121-147.
- Moore, David, et al. "Inside the slammer worm." *IEEE Security & Privacy* 99.4 (2003): 33-39
- Morgenthau, Hans J. *Politics among the nations: the struggle for power and peace*. Alfred A. Knopf, 1972.
- Mueller, Milton L. *Ruling the root: Internet Governance and the Taming of Cyberspace*. MIT press, 2002
- Mueller, Milton L. *Networks and states: The global politics of Internet governance*. Mit Press, 2010.
- Mueller, Milton, Andreas Schmidt, and Brenden Kuerbis. "Internet security and networked governance in international relations." *International Studies Review* 15.1 (2013): 86-104.
- Nadji, Yacin, et al. "Beheading hydras: performing effective botnet takedowns." *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 2013.
- NANOG "The History of NANOG." *North American Network Operators Group*, www.nanog.org/history
- NCI "About ISACs." *National Council of ISACs*, www.nationalisacs.org/about-isacs.
- NIST FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems available at: <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>
- Nye Jr, Joseph S. *Cyber power*. Harvard University Cambridge MA, Belfer Center for Science and International Affairs, 2010
- NYT "Creator of Melissa Virus Gets 20 Months in Jail." *The New York Times*, The New York Times, 2 May 2002, www.nytimes.com/2002/05/02/nyregion/creator-of-melissa-virus-gets-20-months-in-jail.html.
- OECD "Proactive Policy Measures by Internet Service Providers against Botnets", OECD Digital Economy Papers, No. 199, OECD Publishing. 2012.
- Ops-Trust "About Ops-trust." <https://portal.ops-trust.net/>
- Orsini, Amandine, Jean-Frédéric Morin, and Oran Young. "Regime complexes: A buzz, a boom, or a boost for global governance?." *Global Governance: A Review of Multilateralism and International Organizations* 19.1 (2013): 27-39.
- Overuse of prefix sparks a backlash, but alternatives are few; 'computery'" *The Wall Street Journal* 5 March 2015 available at: <https://www.wsj.com/articles/is-the-prefix-cyber-overused-1425427767>

- Paseka, T. Why Google Went Offline Today and a Bit About How the Internet Works. *CloudFlare* (November 6, 2012) <https://blog.cloudflare.com/why-google-went-offline-today-and-a-bit-about/>
- Paul McFedries. "The (Pre) Fix Is In." *IEEE Spectrum: Technology, Engineering, and Science News*, 1 Aug. 2004, spectrum.ieee.org/at-work/education/the-pre-fix-is-in.
- Pelline, Jeff. "MyDoom Downs SCO Site." *CNET*, CNET, 2 Feb. 2004, www.cnet.com/news/mydoom-downs-sco-site/?i10c.ua=1&i10c.encReferrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&i10c.dv=7.
- Phage List. "Security Digest Archives. 1 March 2005. <http://securitydigest.org/phage/>
- Podolny, Joel M., and Karen L. Page. "Network forms of organization." *Annual review of sociology* (1998): 57-76.
- Pouliot, Vincent. "The logic of practicality: A theory of practice of security communities." *International organization* 62.2 (2008): 257.
- Quack, Sigrid. "Legal professionals and transnational law-making: A case of distributed agency." *Organization* 14.5 (2007): 643-666.
- Rammert, Werner. "Distributed agency and advanced technology." *Agency Without Actors? New Approaches to Collective Action* (2012): 98-112.
- Raymond, M. Managing decentralized cyber governance: The responsibility to troubleshoot. *Strategic Studies Quarterly* 2016; 10:4 (Winter): 124.
- Reuters. "Russian computer programmer arrested in Spain: embassy." Reuters. 9 April 2017. <https://www.reuters.com/article/us-spain-russia-idUSKBN17B002>
- Rhinesmith, Colin. "The social shaping of cloud computing: An ethnography of infrastructure in east St. Louis, Illinois." *Proceedings of the American Society for Information Science and Technology* 51.1 (2014): 1-10.
- Roberts, Paul F. "MyDoom One Year Later: More Zombies, More Spam." *InfoWorld*, InfoWorld, 26 Jan. 2005, www.infoworld.com/article/2669026/security/mydoom-one-year-later--more-zombies--more-spam.html.
- Rosenblum, Gary J. "What is everyone doing?" phage. 4 November 1988. Mailing List. <http://securitydigest.org/phage/archive/034>
- Rowan, Miek. "Re. What is everyone doing?" Message to phage. 4 November 1988. Mailing List. <http://securitydigest.org/phage/archive/032>
- Rowe, Brent, Douglas Reeves, and Mike Gallaher. *The role of internet service providers in cyber security*. Institute for Homeland Security Solutions, 2009.
- Rowley, Timothy J. "Moving beyond dyadic ties: A network theory of stakeholder influences." *Academy of management Review*. 22.4 (1997): 887-910.

- Symantec. "VGS.LoveLetter.Var." Symantec. <https://www.symantec.com/security-center/writeup/2000-121815-2258-99>
- Schmidt, Andreas in Kremer, Jan-Frederik, and Benedikt Müller. *Cyberspace And International Relations : Theory, Prospects And Challenges* / Jan-Frederik Kremer, Benedikt Müller, Editors. n.p.: Heidelberg : Springer, (2014.):. 181-202.
- Schmidt, Andreas. "Hierarchies in networks: emerging hybrids of networks and hierarchies for producing internet security." *Cyberspace and International Relations*. Springer Berlin Heidelberg, 2014. 181-202.
- Schmidt, Andreas. "Open security. Contributions of networked approaches to the challenge of democratic internet security governance." *The Evolution of Global Internet Governance*. Springer Berlin Heidelberg, (2014): 169-187.
- SEI "1992 CERT Advisories" SEI Carnegie Mellon University. 1992.
https://resources.sei.cmu.edu/asset_files/WhitePaper/1992_019_001_496266.pdf
- SEI (2) "History of Innovation at the SEI". Software Engineering Institute.
https://www.sei.cmu.edu/about/history-of-innovation-at-the-sei/display.cfm?customel_datapageid_40842=41019
- Seidel, Robert J., et al. *Computer literacy: issues and directions for 1985*. Academic Press, 1985.
- Shadowserver (1) "Mission." (2017)
<https://www.shadowserver.org/wiki/pmwiki.php/Shadowserver/Mission>
- Shadowserver (2) . "Kelihos.E." (2017) <http://blog.shadowserver.org/2017/04/12/kelihos-e>
- Shadowserver(3). "Avalanche." Shadowserver. (2016)
<http://blog.shadowserver.org/2016/12/01/avalanche/> 2016
- Shaver, Dave. "Re: Sendmail hacking." Phage. 4 November 1988. Mailing List.
<http://securitydigest.org/phage/archive/031>
- Shirazi, Reza. "Botnet Takedown Initiatives: A Taxonomy and Performance Model." *Technology Innovation Management Review* 5.1 (2015).
- Sil, Rudra, and Peter J. Katzenstein. *Beyond paradigms: analytic eclecticism in the study of world politics*. Palgrave Macmillan, 2010
- Simmons, Beth A. "Preface: International relationships in the information age." *International Studies Review*. 15.1 (2013): 1-4.
- Singh, J. P. "Information technologies, meta-power, and transformations in global politics." *International Studies Review* 15.1 (2013): 5-29.
- Slaughter, Anne-Marie. *A New World Order*, Princeton University Press, 2004.
- Spafford, Eugene H. "Crisis and aftermath." *Communications of the ACM* 32.6 (1989): 678-687.

- Spafford, Eugene. Testimony to the House Armed Services Committee. 24 July 2003.
<https://spaf.cerias.purdue.edu/usgov/hasc.pdf>
- Spafford, Gene. "A worm 'condom' enclosed." Phage. 3 November 1988. Mailing List.
<http://securitydigest.org/phage/archive/013>
- Spafford, Gene. "Addition to the list." Phage. 8 November 1988. Mailing List.
<http://securitydigest.org/phage/archive/169>
- Spafford, Gene. "This Group." Message to phage. 26 November 1998. Mailing List.
<http://securitydigest.org/phage/archive/301>
- Sprafford, Eugene H. "A Failure to Learn from the Past." *Computer Security Applications Conference, 2003. Proceedings. 19th Annual*. IEEE, 2003.
- Stevens, Tim. *Cyber Security and the Politics of Time*. Cambridge University Press, 2015.
- Stone, Brad. "Authorities Shut Down Major Spam Ring." *The New York Times*, 14 Oct. 2008,
www.nytimes.com/2008/10/15/technology/internet/15spam.html.
- Stone-Gross, Brett, et al. "The Underground Economy of Spam: A Botmaster's Perspective of Coordinating Large-Scale Spam Campaigns." *LEET* 11 (2011): 4-4.
- Sully, Matt, and Matt Thompson. "The deconstruction of the Mariposa botnet." *Defence Intelligence*. Retrieved September 16 (2010): 2012.
- Tabak, Faruk. "Ars Longa, Vita Brevis? A Geohistorical Perspective on Pax Mongolica." *Review (Fernand Braudel Center)* (1996): 23-48.
- Takahashi, Dean. "Hackers and Virtual Perps: Beware of ICESA.net Sleuths." *The Wall Street Journal*, Dow Jones & Company, 30 Sept. 1999,
www.wsj.com/articles/SB938637421701976364.
- United States v. Skorjanc* Case. 1:11-mj-00321-AK. *The United States District Court For the District of Columbia*, <https://www.justice.gov/opa/file/630811/download>
- United States, Congress, Brock, Jack L. "Critical Infrastructure Protection: 'ILOVEYOU' Computer Virus Highlights Need for Improved Alert and Coordination Capabilities: Statement of Jack L. Brock, Jr., Director, Government wide and Defense Information Systems, Accounting and Information Management Division, before the Subcommittee on Financial Institutions, Committee on Banking, Housing and Urban Affairs, U.S. Senate", GAO, 2000.
www.gao.gov/new.items/ai00181t.pdf.
- United States, Congress, Rhodes, Keith A. "Information Security: the Melissa Computer Virus Demonstrates Urgent Need for Stronger Protection over Systems and Sensitive Data." *Information Security: the Melissa Computer Virus Demonstrates Urgent Need for Stronger Protection over Systems and Sensitive Data*, General Accounting Office, 1999.
- United States, Congress. "Virus Highlights Need for Improved Internet Management.", General Accounting Office. 1989 .<https://www.gao.gov/assets/150/147892.pdf>, p2

- Valeriano, Brandon and Maness, Ryan C. *International Relations Theory and Cybersecurity: Threats, Conflicts, and Ethics in an Emergent Domain* in The Oxford Handbook of International Political Theory. Oxford (2018)
- Vihul, Liis, et al. "Legal Implications of Countering Botnets." *Joint report from the NATO Cooperative Cyber Defence Centre of Excellence and the European Network and Information Security Agency (ENISA)* (2012).
- Vijayan, Jaikumar. "McColo Takedown: Internet Vigilantism or Online Neighborhood Watch?" *Computerworld*, 17 Nov. 2008, www.computerworld.com/article/2529316/malware-vulnerabilities/mccolo-takedown--internet-vigilantism-or-online-neighborhood-watch-.html.
- Vijayan, Jaikumar. "McColo Takedown: Internet Vigilantism or Online Neighborhood Watch?" *Computerworld*, Computerworld, 17 Nov. 2008, www.computerworld.com/article/2529316/malware-vulnerabilities/mccolo-takedown--internet-vigilantism-or-online-neighborhood-watch-.html.
- Von Solms, Basie. "Information security—the fourth wave." *Computers & security* 25.3 (2006): 165-168.
- Ward, Mark. "A Decade on from the ILOVEYOU Bug." *BBC News*, BBC, 4 May 2010, www.bbc.com/news/10095957.
- Weatherford, Jack. *Genghis Khan and the Making of the Modern World*. Three Rivers Press, 2012.
- Wenger, Etienne. "Communities of practice: A brief introduction." (2011).
- Whittle, Andrea, Olga Suhomlinova, and Frank Mueller. "Dialogue and distributed agency in institutional transmission." *Journal of Management & Organization* 17.04 (2011): 548-569.
- Wilson, Clay. "Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress." Library of Congress Washington DC Congressional Research Service, 2008.
- Woodcock, Bill, and Marco Fingino. *2016 Survey of Internet Carrier Interconnection Agreements*. Packet Clearing House, 2016. <https://www.pch.net/resources/Papers/>
- Weinberger, Sharon. "Top Ten Most-Destructive Computer Viruses." *Smithsonian.com*. 19 March 2012. <https://www.smithsonianmag.com/science-nature/top-ten-most-destructive-computer-viruses-159542266/?c=y&page=2>
- Yadron, Danny and Jennifer Valentino-DeVries. "This Article Was Written With the Help of a 'Cyber' Machine
- Zeitlin, Sam. "Botnet Takedowns and the Fourth Amendment." *NYUL Rev.*90 (2015): 746.
- Zetter, Kim. "DNSChanger' Malware Could Strand Thousands When Domains Go Dark on Monday." *Wired*, Conde Nast, 3 June 2017, www.wired.com/2012/07/dns-changer-going-dark/.